Kaseya®

2026 REPORT

Cybersecurity outlook: Trends, threats and readiness

Table of contents

Introduction

For MSPs, keeping clients secure in a rapidly evolving threat landscape is a high-stakes, 24/7 mission. However, a critical question remains: Are your services truly meeting clients' needs, or does a costly gap persist between what's delivered and what's expected?

The 2026 Kaseya Cybersecurity Outlook Report is designed to bridge that gap. We surveyed both SMBs and MSPs to get their views on cybersecurity challenges, shifting budgets and rising expectations.

While the data presented primarily reflects SMB responses, it also includes a few key insights from MSPs. Together, this analysis is designed to help MSPs understand their clients' evolving priorities — from where SMBs feel most vulnerable to where they are focusing their cybersecurity investments.

By understanding these perspectives, MSPs can better align their services, deliver measurable value and strengthen long-term partnerships. The findings in this report will equip you with the clarity and direction needed to guide clients confidently through 2026 and beyond.

Key findings

The 2026 Kaseya Cybersecurity Outlook Report reveals crucial insights shaping today's cybersecurity landscape. Here are the top findings.

The human factor: Cybersecurity's weakest link

Humans continue to be the weakest link in cybersecurity. The No. 1 vulnerability is human error, driven by poor user practices and inadequate training, making it the most feared threat vector for the next 12 months.

Penetration testing: Critical, yet costly

While 76% of businesses conduct annual penetration tests, nearly one in four remain inconsistent or skip testing entirely. Cost remains the leading barrier. For MSPs, however, pentesting is a profitable opportunity, with almost half reporting margins above 20%.

Downtime: The cost of cyber failure

Cyber incidents are more than just technical hiccups — they bring business operations to a grinding halt. A staggering 37% of businesses reported losing a full day or more to downtime following an incident. Additionally, 18% of businesses suffered financial losses of $100,000 or more after a security breach.

The AI paradox: Trust vs. potential

While AI adoption is accelerating, trust barriers are holding it back. Only 12% of businesses fully trust AI to act autonomously. Today, AI is most widely applied in email security (48%), enhanced endpoint protection (34%), and threat detection and anomaly identification (32%).

Phishing: The relentless threat

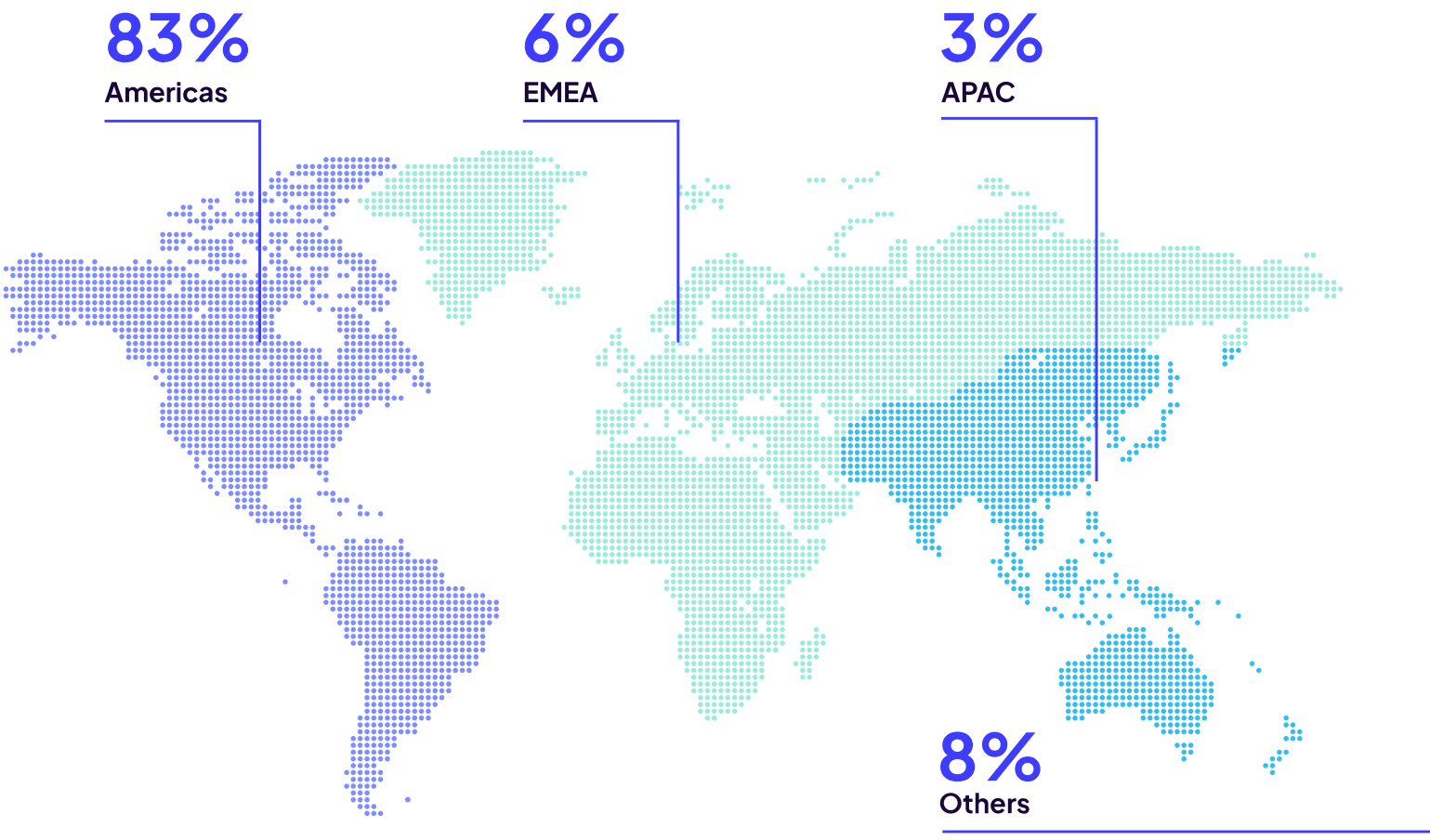
Phishing remains the most damaging and persistent cybersecurity challenge. It has affected more businesses than any other type of attack, with 56% impacted to date and nearly half (49%) within the past year alone.

Participant demographics

This year's report draws on insights from more than 700 SMBs and 370 MSPs worldwide, offering a truly global perspective on cybersecurity. The majority of participants (83%) came from the Americas, with additional representation from EMEA (6%), APAC (3%) and other regions (8%).

Most respondents (65%) work at SMBs with more than 100 employees, providing a strong view into the priorities and challenges faced by more established organizations. Collectively, the responses from all participants paint a comprehensive picture of how businesses are confronting today's cyberthreats, and where opportunities exist for MSPs to step in and lead.

Respondents by region



Where cybersecurity stands now

Although organizations are strengthening baseline defenses, gaps in proactive security create opportunities for MSPs to deliver greater value.

A mixed approach to IT management

While a clear majority of respondents (59%) rely on a dedicated internal IT team to handle their IT needs, a significant portion has chosen a collaborative approach. About 30% of businesses have a co-managed relationship with an MSP or MSSP, while 6% opt to outsource their entire IT function. This data highlights a market where there is no one-size-fits-all solution. Businesses are seeking the right balance of internal control and external expertise.

Which of the following best describes how your organization's IT needs are currently managed?

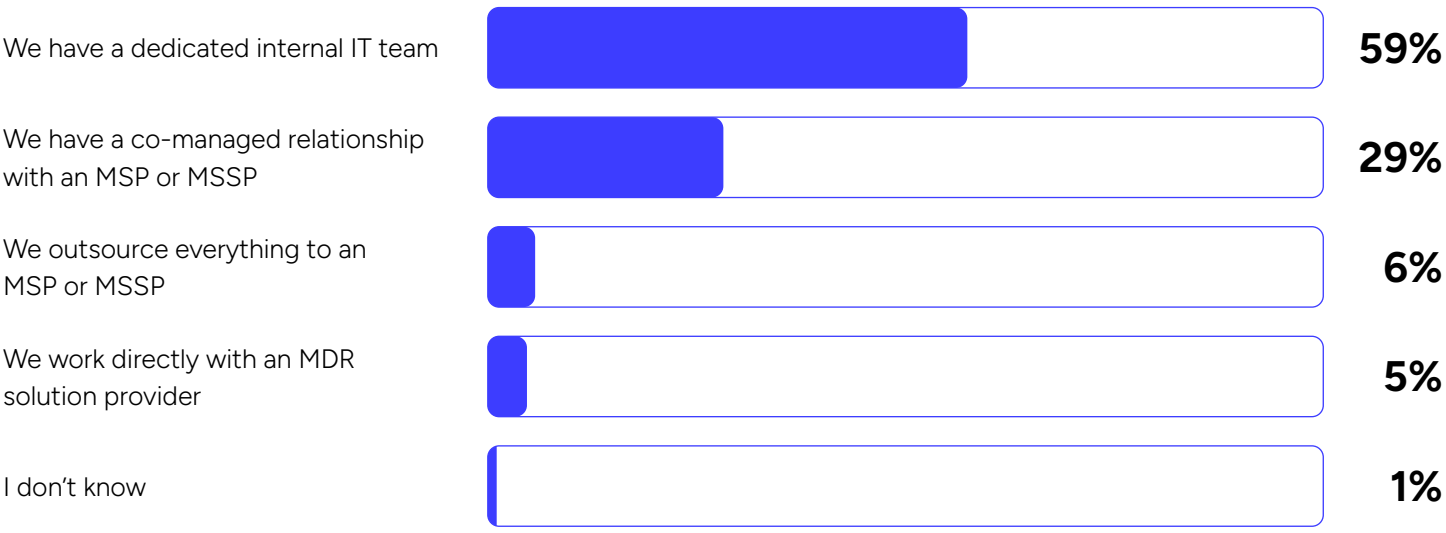


Figure 1. How IT needs are managed

Cybersecurity framework adoption signals maturity

Cybersecurity is no longer just about tools; it's about strategy. The adoption of formal cybersecurity frameworks demonstrates a growing maturity in how businesses approach risk. The most widely adopted frameworks are Zero Trust and ISO 27001 (36%), followed closely by NIST (35%), reflecting a strong push toward more structured security strategies.

However, with fewer than half of organizations embracing any single framework — and many adopting multiple frameworks simultaneously — MSPs are perfectly positioned to guide clients in adopting and operationalizing these models more consistently.

Which of the following cybersecurity frameworks (CSFs) do you currently utilize? (Select all that apply)

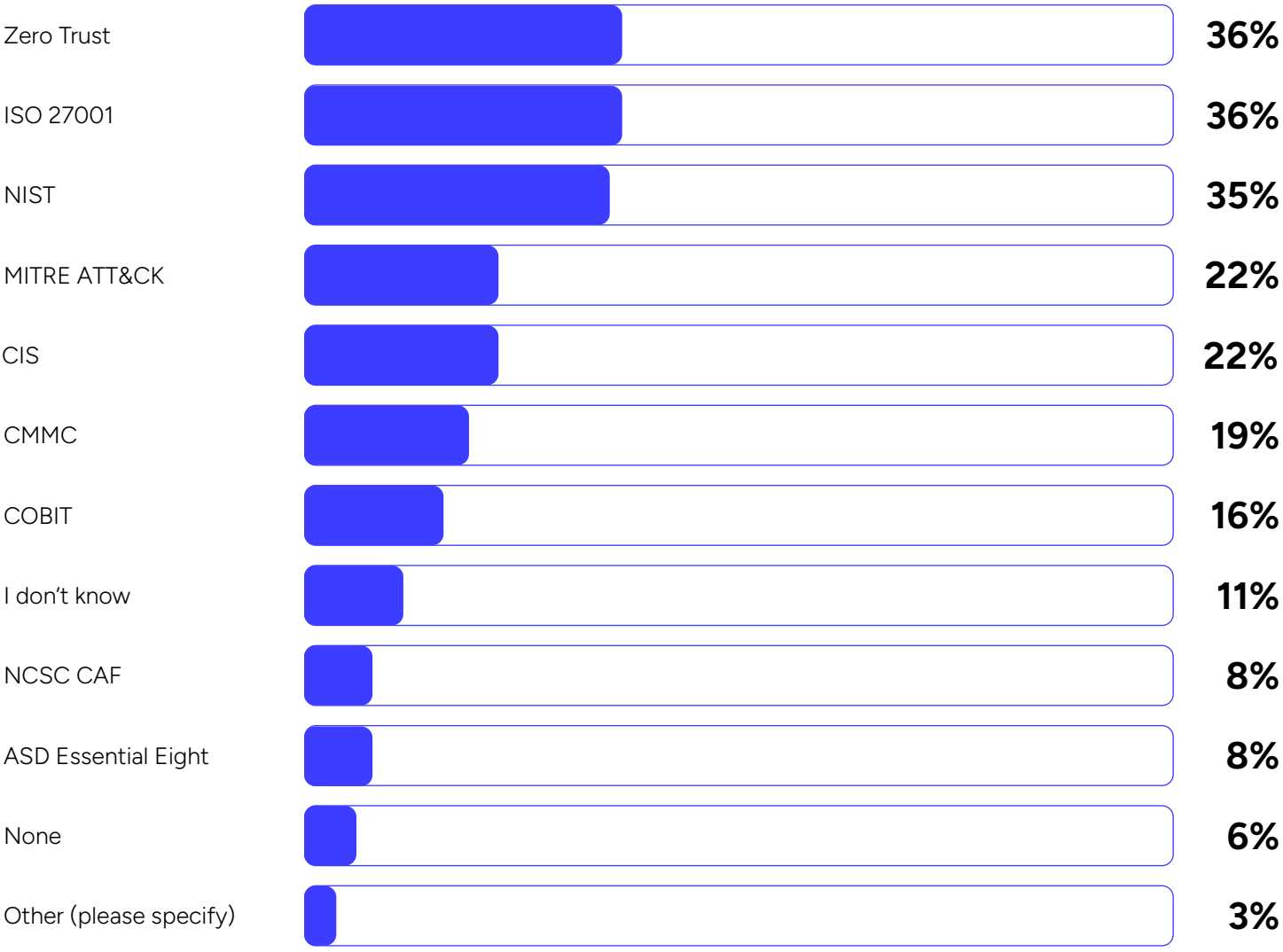


Figure 2. Cybersecurity frameworks in used

Defenses are strong, but proactivity is lagging

Organizations have built a strong foundation of core defenses. Essential tools, such as antivirus (76%), firewalls (71%) and email/phishing protection (68%), are widely used. More advanced measures like network security (61%) and EDR (59%) are also well adopted.

However, a clear gap exists in proactive measures that actively hunt for threats and neutralize them before they escalate. Only 37% of businesses conduct penetration testing, and less than 40% have implemented solutions like Managed SOC, MDR or SIEM. This creates a critical blind spot for many organizations, leaving them vulnerable to sophisticated attacks. For MSPs, this is a great opportunity to step in with proactive, layered solutions.

Which of the following security solutions have you implemented?
(Select all that apply)

Antivirus software	76%
Firewall	71%
Email/phishing protection	68%
Network security	61%
File backup	56%
Automated software patching	53%
Business continuity and disaster recovery (BCDR)	53%
Security awareness training	49%
Cloud detection and response/ SaaS security	47%
Endpoint detection and response (EDR)	45%
Identity and access management	44%
Vulnerability management and detection	39%
Penetrating testing	37%
Dark web monitoring	31%
Managed SOC	29%
Secure remote access (SASE)	29%
MDR	26%
SIEM	25%
Other	0.5%

Figure 3. Security solutions implemented

Future investment priorities

As organizations look to strengthen resilience, they are moving beyond baseline defenses and investing in more advanced capabilities. The top areas of planned investment for the next 12 months include penetration testing (17%), cloud detection and response/SaaS security (17%), dark web monitoring (16%) and BCDR (15%).

A notable 14% of respondents report no plans to add new security solutions in the coming year, which could indicate a false sense of security or a critical lapse in future-proofing their defenses. For MSPs, this presents both a challenge and an opportunity to educate clients, demonstrate value and position proactive security as non-negotiable.

Which of the following cybersecurity solutions do you anticipate implementing in the next 12 months? (Select all that apply)

Cloud detection and response /SaaS security	17%
Penetrating testing	17%
Dark web monitoring	16%
Business continuity and disaster recovery (BCDR)	15%
Security awareness training	14%
Automated software patching	14%
We do not anticipate investing in additional cybersecurity solutions	14%
Vulnerability management and detection	13%
Secure remote access (SASE)	13%
Identity and access management	12%
Managed SOC	11%
SIEM	11%
EDR	11%
MDR	10%
Email/phishing protection	9%
File backup	9%
Network security	8%
Firewall	6%
Other	5%
Antivirus software	4%

Figure 4. Planned security investments over the next 12 months

AI in cybersecurity

AI is redefining cybersecurity, but trust gaps, cost barriers and human oversight demands limit its full potential.

Current adoption and perceptions

AI's presence in cybersecurity is growing, but it is far from a universally embraced solution. A notable 18% of businesses still don't use AI to enhance their security posture. The core issue isn't a lack of interest, but a lack of trust. Just 12% of businesses fully trust AI to act autonomously. For the overwhelming majority (nearly 81%), human oversight is necessary. Among businesses that leverage AI, it's seen as an assistive tool and not an independent agent.

Where AI delivers the most value

AI's strongest value today lies in email security (49%), endpoint protection (34%), and threat detection and anomaly identification (32%). Looking ahead, businesses plan to expand AI's role into improving overall visibility through better threat and vulnerability detection (32%) and automating response or remediation (30%). The future of AI is about moving from detection to proactive action. To stay competitive, MSPs must combine efficiency with oversight while using AI for predictive and automated defense.

How is your organization currently leveraging AI to enhance your security posture? (Select all that apply)

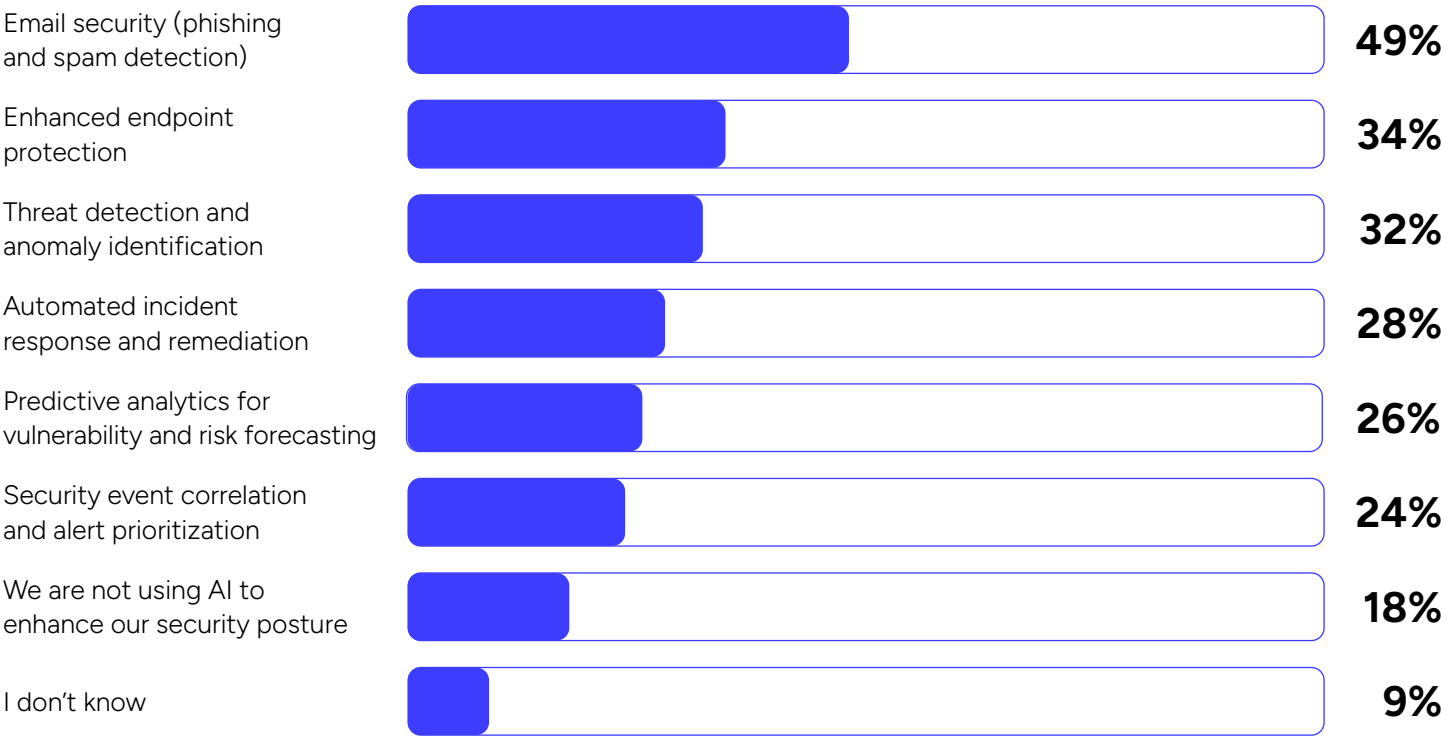


Figure 5. Current use of AI in security

Key concerns and barriers to adoption

Trust remains the biggest barrier to AI adoption. More than 80% of respondents said that human oversight is required, while just over 10% of businesses report that they fully trust AI to act autonomously. The key concerns cited by respondents are accuracy (29%), which includes the fear of false positives or negatives, followed by data privacy (27%) and cost (19%).

These barriers create a significant opportunity for MSPs to position themselves as trusted advisors, helping businesses navigate the complexities of AI implementation, ensure data integrity and prove a clear return on investment.

What is your biggest concern about using AI in cybersecurity?

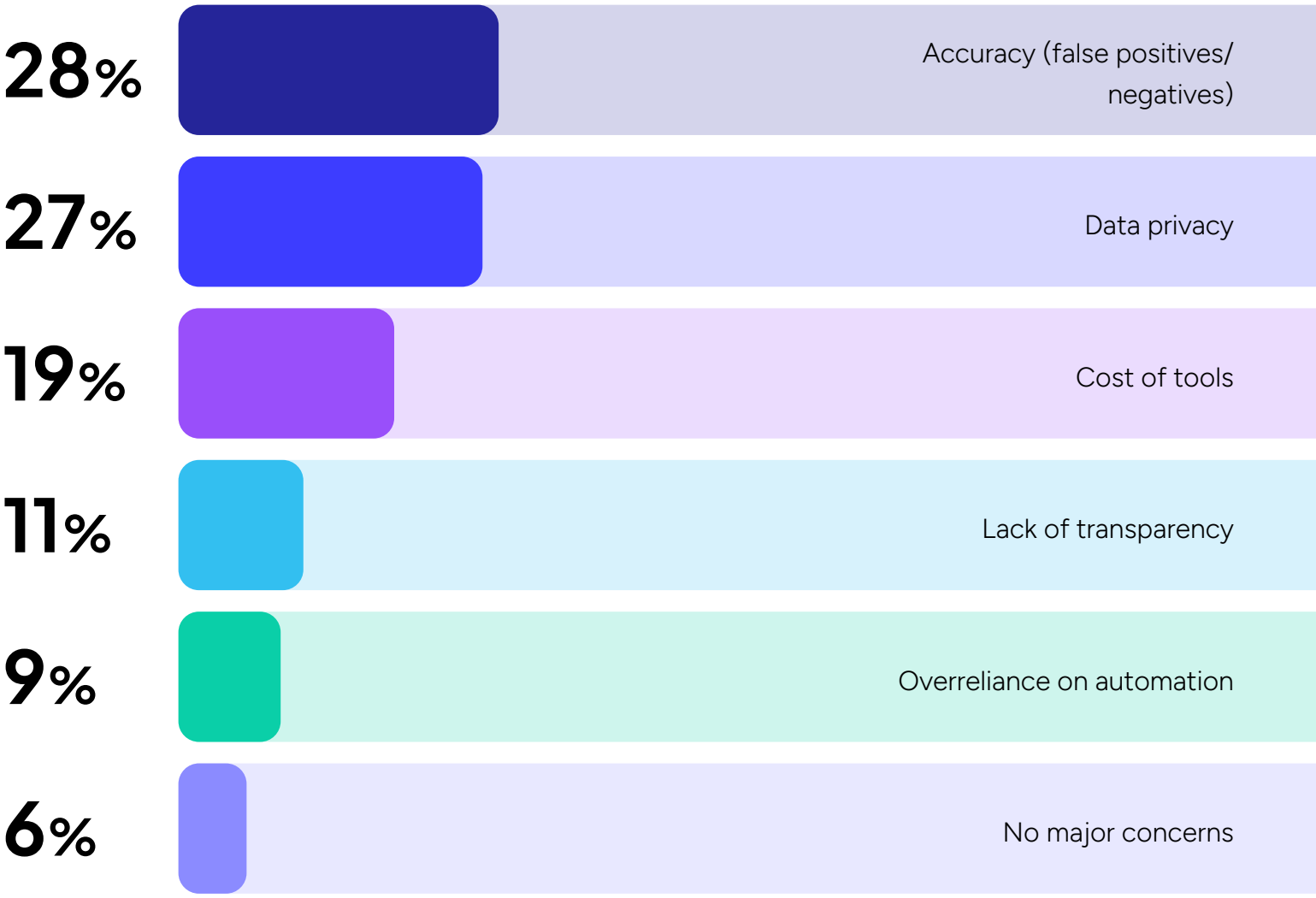


Figure 6. Biggest concerns about using AI in cybersecurity

Security operations and training needs

To build stronger defenses, businesses need mature operations, continuous training and MSP guidance to close the gaps that leave clients exposed to risks.

Threat monitoring

When it comes to threat monitoring, organizations are adopting a variety of approaches. While 44% of organizations maintain an internal SOC and 37% rely on a managed SOC, about 15% of businesses report having no real-time threat monitoring in place at all. Another 4% don't even know how threats are monitored. This lack of visibility creates dangerous blind spots. Many organizations still need help establishing continuous monitoring and leveraging outsourced SOC services for around-the-clock protection, which is a clear opportunity for MSPs.

How do you monitor for active threats across your IT environment?

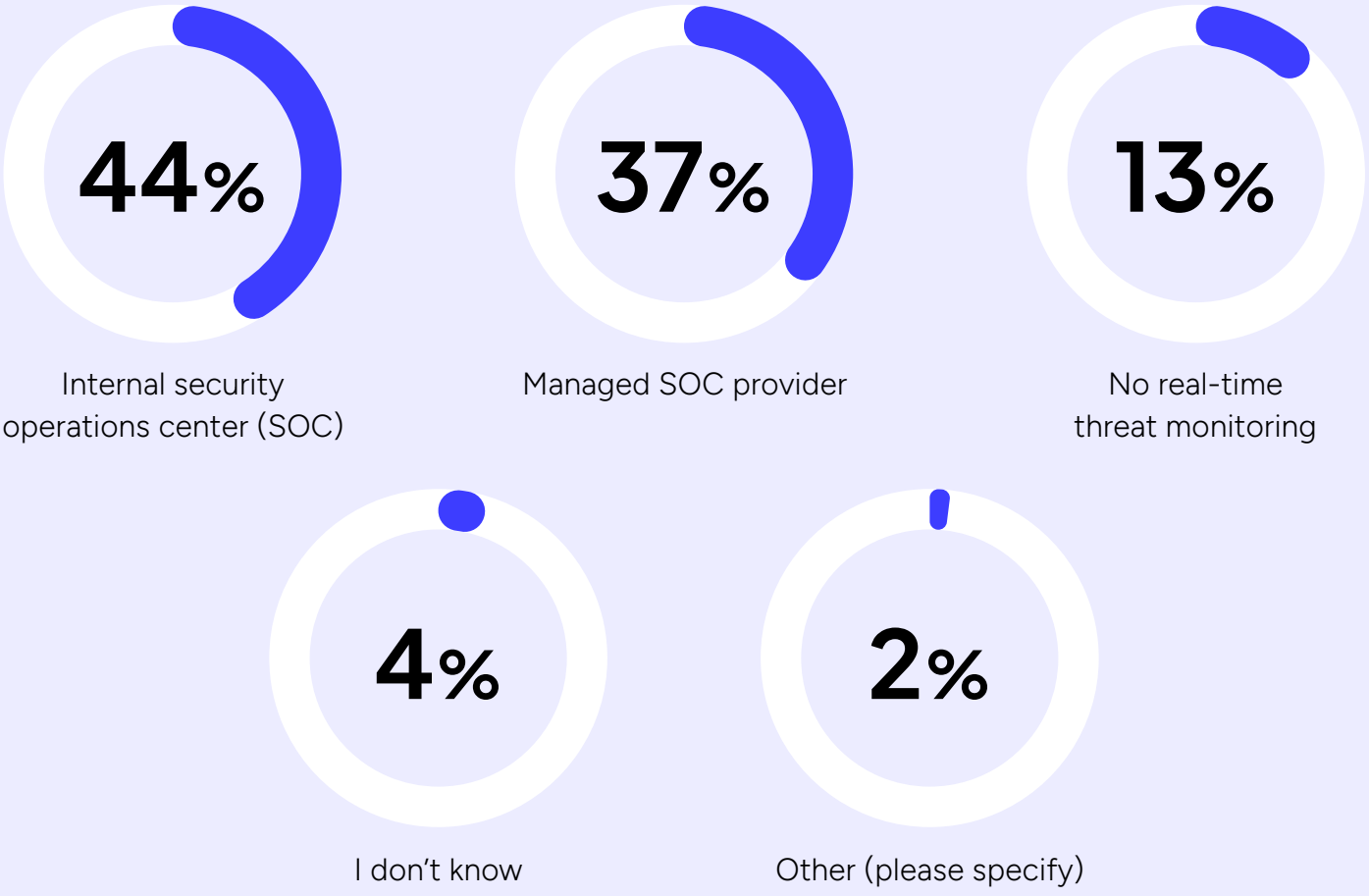


Figure 7. How organizations monitor threats

Security awareness: A fragmented culture

Human error remains the biggest weakness, and training practices reveal why. Security awareness culture is fragmented, with one-third of businesses providing training only once a year or less. The good news is that most organizations are at least engaging in proactive exercises, with 86% reporting that their training programs include phishing simulations. Still, the infrequency of these efforts shows that strong security habits are still missing across the workforce. MSPs that can deliver engaging, continuous training programs and reinforce a true culture of security will stand apart from competitors.

Which of the following best describes your employee security awareness culture?

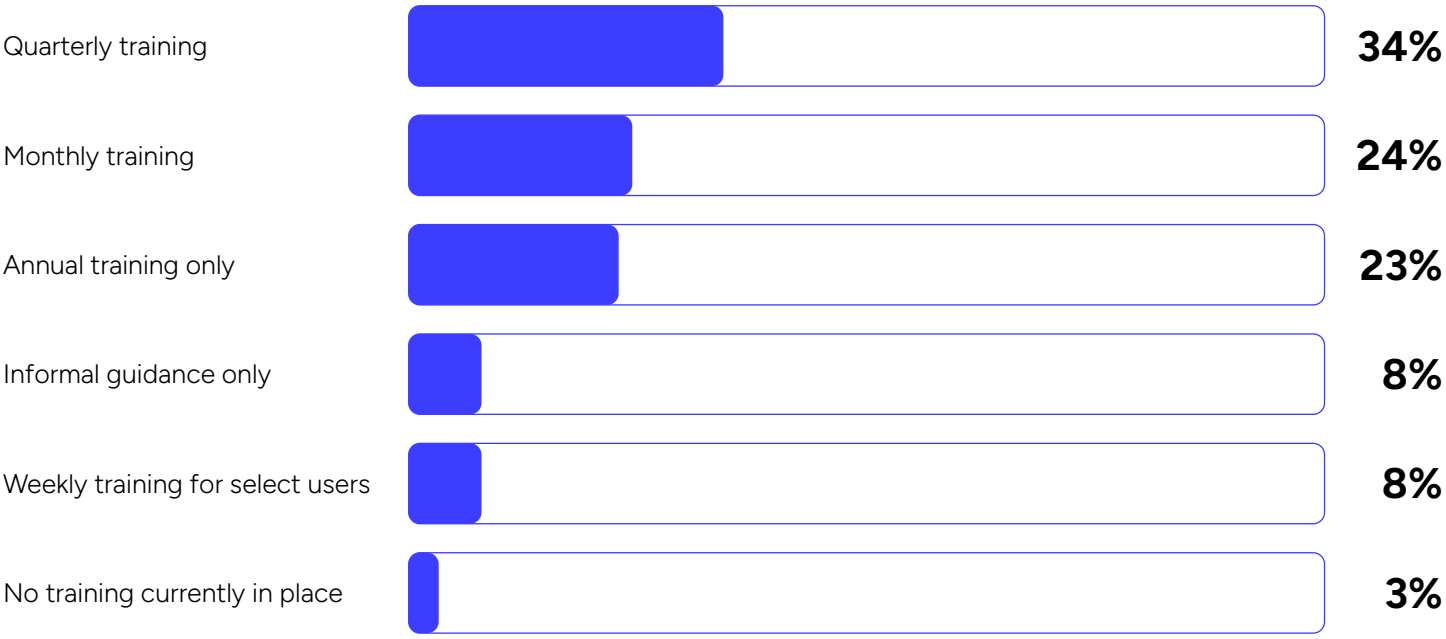


Figure 8. Security awareness training cadence

Does your training include phishing simulations?

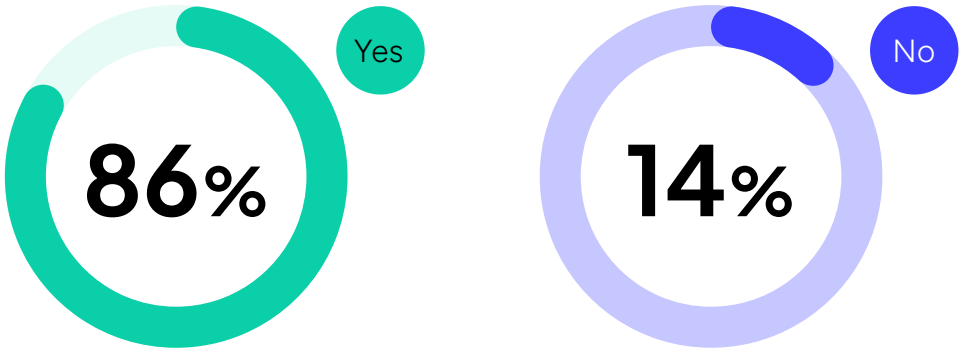


Figure 9. Phishing simulations included in training

Vulnerability assessments

A large majority of organizations (84%) conduct vulnerability assessments at least annually, and 63% run them quarterly. However, nearly 30% of businesses are inconsistent or do not conduct assessments at all. This inconsistency leaves exploitable gaps. MSPs can step in with managed assessment services that provide regular, standardized reporting to ensure no blind spots remain.

Approximately how frequently do you conduct IT security vulnerability assessments?

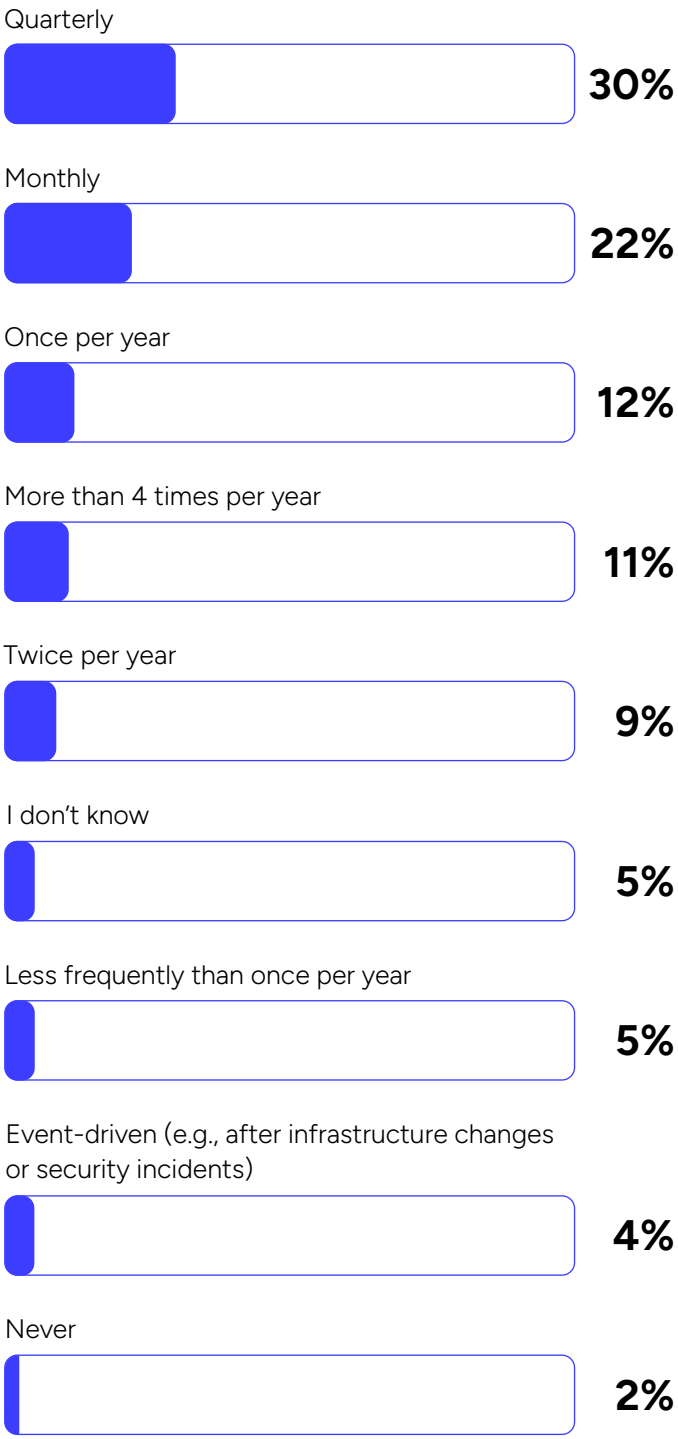


Figure 10. Security vulnerability assessments frequency

Penetration testing: Essential, yet underutilized

The situation for IT penetration testing is similar to vulnerability assessments. While a strong 76% perform pentesting annually, nearly a quarter are inconsistent or do not test. The primary barrier to adoption remains cost, cited by 47% of respondents.

Organizations use pentesting primarily to validate controls (34%), assess damage potential (20%) and prioritize investments (17%).

Approximately how frequently does your organization conduct IT penetration testing?

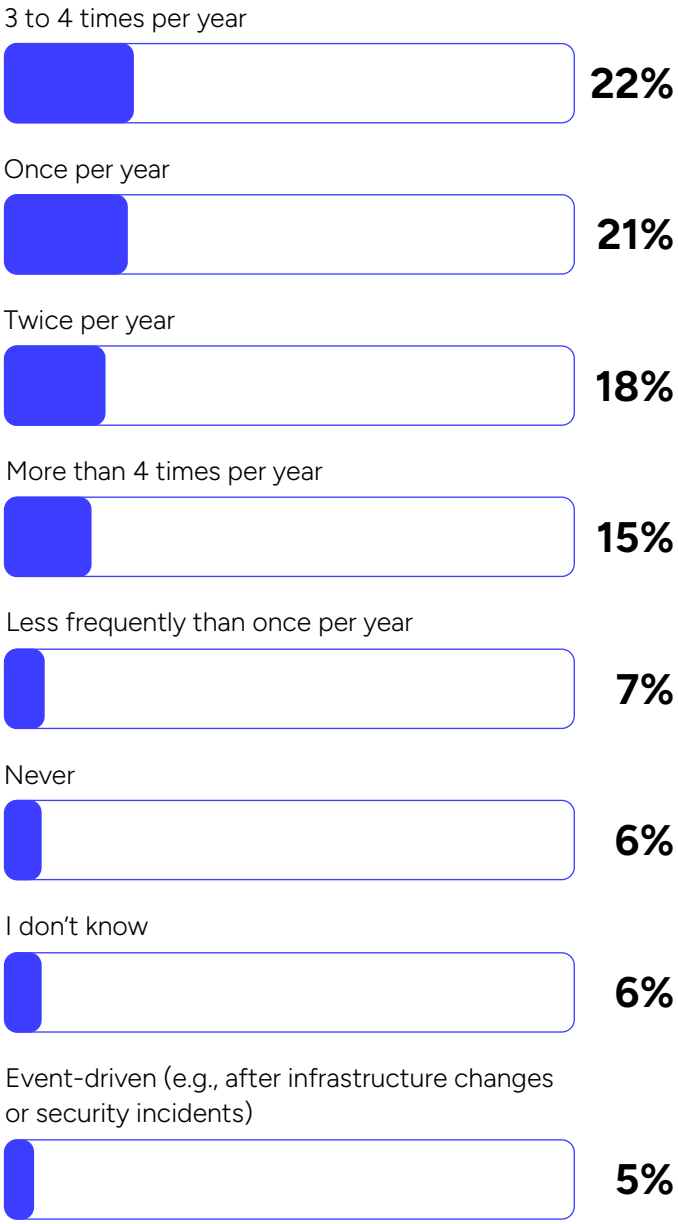


Figure 11. Penetration testing frequency

The data also reveals a significant opportunity for MSPs. Close to 40% of MSPs report profit margins of 21–40% from pentesting, especially when offered as part of bundled services. However, a third of MSPs don't offer the service at all, suggesting a sizeable untapped market.

What is your profit margin on offering penetration testing to your customers?

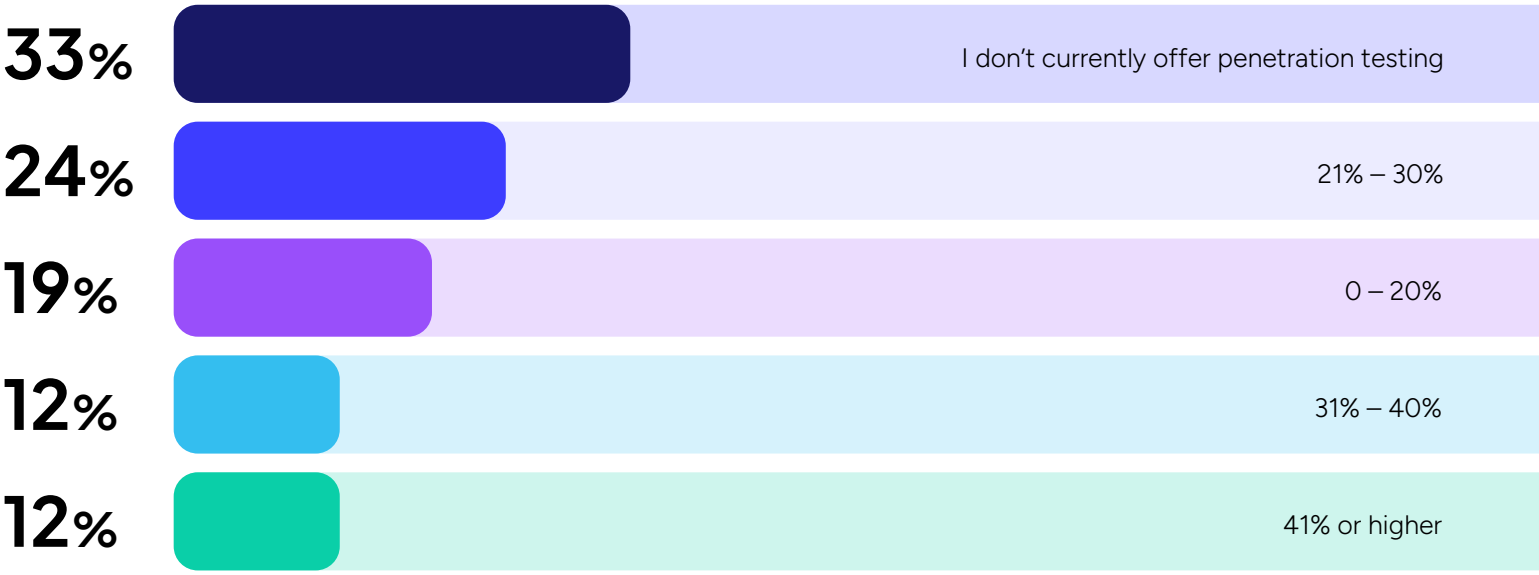


Figure 12. Pentesting profit margins

Cyber insurance is a growing priority

Cyber insurance adoption is growing — two-thirds (66%) of organizations already have coverage, and nearly half of the remainder plan to purchase insurance in the next 12 months. On the flip side, 19% lack coverage and 15% don't even know their organization's status. MSPs have a clear role in preparing clients for insurance requirements, ensuring compliance and guiding them through readiness assessments.

Does your organization have cyber insurance?

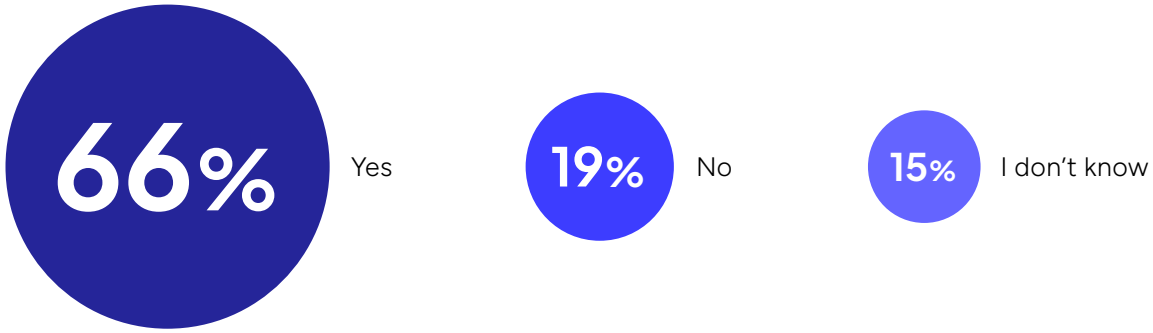


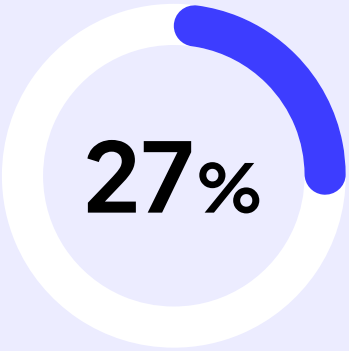
Figure 13. Cyber insurance coverage

Incident response

When a breach occurs, a robust IR plan is the most critical tool for minimizing damage. However, the readiness of businesses is concerning. While 40% of organizations have a formal IR plan and test it regularly, a significant 27% have a plan in place but have never tested it. Even more troubling, 24% have no formal plan at all, and an additional 10% are unsure of their organization's IR plan. This gap presents a critical opportunity for MSPs to help clients formalize, test and refine incident response processes.

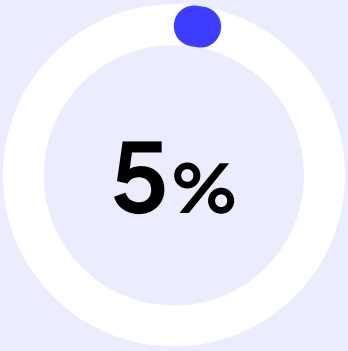
Which of the following best describes your organization when it comes to having a cybersecurity incident response (IR) plan?

We have a formal IR plan in place and we perform periodic drills and tabletop exercises to test it

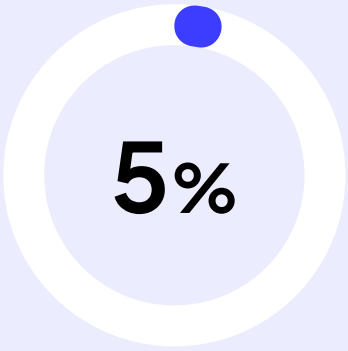


We have a formal IR plan in place but we haven't tested it

We have some security solutions to protect us but we do not have a formal IR plan in place



I believe our IT service provider (MSP) has a plan in place for us



I don't know

Figure 14. Incident response plan status

Cybersecurity threats and incidents

Cybersecurity incidents are a near-universal reality — over 75% of businesses reported having experienced a cybersecurity incident in their lifetime. Phishing, malware, business email compromise (BEC) and human error continue to dominate the threat landscape, driving costly downtime and losses for businesses worldwide.

Phishing dominates the threat landscape

Phishing remains the most significant cybersecurity threat facing businesses today, with 56% reporting they've been impacted at least once and nearly half (49%) targeted in the past year alone. It continues to outpace other threats, ahead of viruses/malware (32%) and BEC (27%). This data shows that attackers are successfully targeting the most complex and difficult-to-patch vulnerability: the human element.

The survey clearly identifies the primary causes of these incidents, pointing directly back to people and processes: poor user practices (30%), lack of end-user training (29%) and limited cybersecurity expertise (27%). These findings highlight the need for both better internal training and external expertise to close these vital security gaps.

Which of the following cybersecurity issues have ever impacted your business (including your clients, if applicable)? (Select all that apply)

Phishing messages	56%	Account takeover	16%
Computer viruses or malware	45%	Supply chain attack	11%
Business email compromise	40%	None	10%
Ransomware	26%	Zero-day exploit	9%
Personal information or credential theft	23%	Other cybersecurity issue	2%

Figure 15. Cybersecurity issues experienced (all time)

Business impact: Downtime and financial losses

The consequences of a security incident are immediate and expensive. Roughly 40% of businesses report suffering at least one full day of downtime after an incident. Only 21% avoided downtime, a slight drop from 27% in 2024. Additionally, close to 20% of businesses report financial losses of $100,000 or more.

The impact isn't limited to businesses alone; it extends to providers as well, with 40% of MSPs reporting their clients experienced downtime due to breaches in the past year. Unfortunately, 12% lost clients, primarily due to ransomware, account takeover and BEC attacks.

If you've experienced a cybersecurity incident, what was your total downtime?

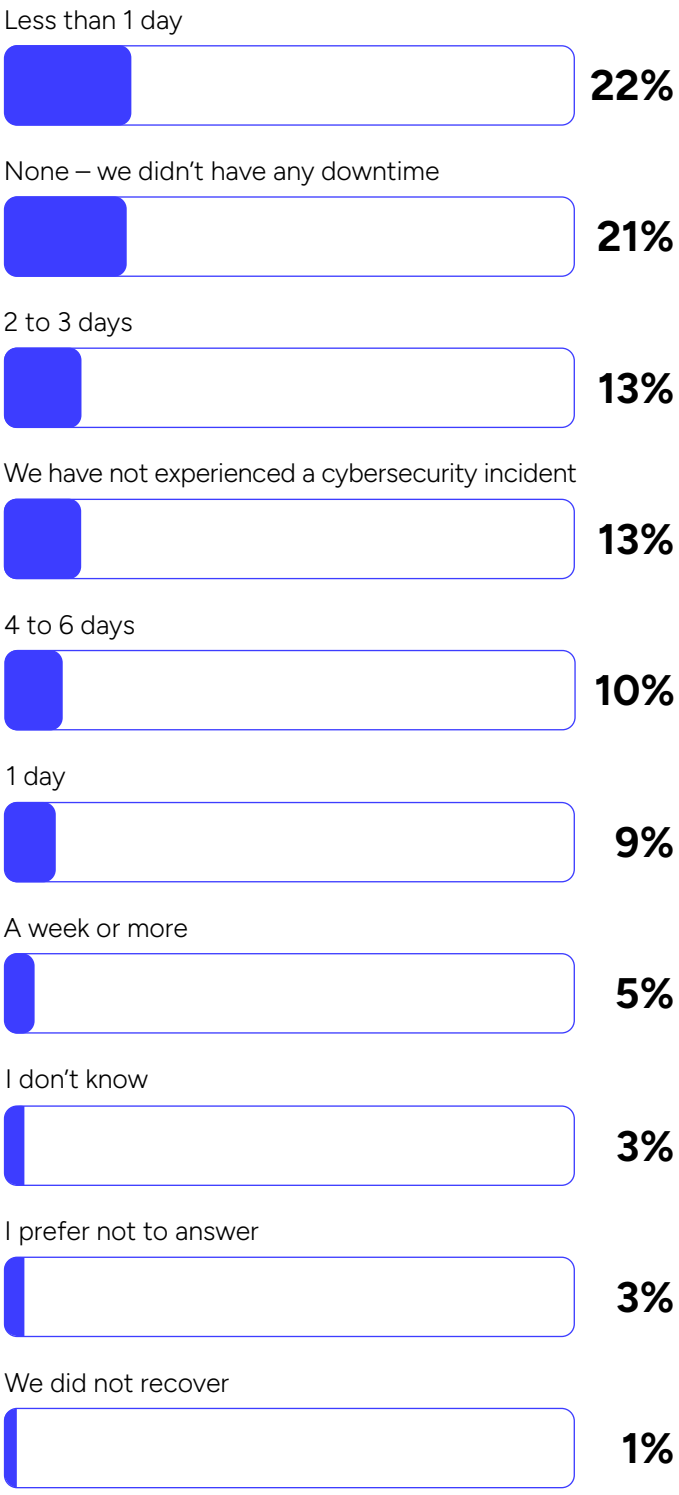


Figure 16. Total downtime

In the past 12 months, have any of your clients experienced downtime due to a breach?

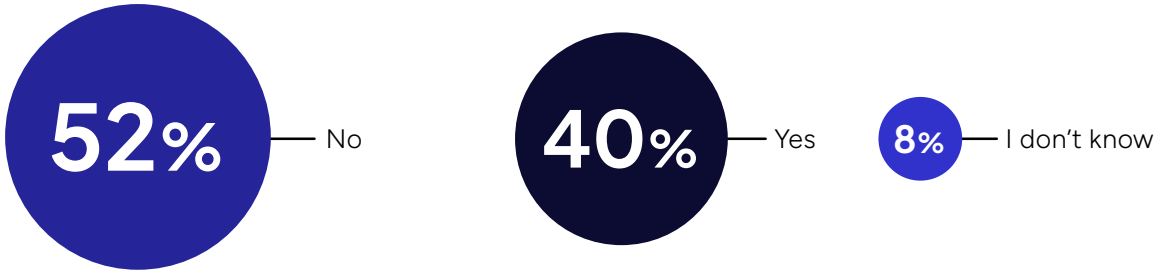


Figure 17. Clients experienced downtime

Ransomware: Less frequent, still devastating

Ransomware attacks appear to be declining — from 34% lifetime exposure to 18% in the past 12 months — suggesting either improved resilience or underreporting. While the frequency has reduced, the pressure to pay the ransom has increased. About 20% of victims paid the ransom in 2025, nearly double the 11% who paid in 2024.

If you were a victim of a ransomware attack, did you pay the ransom?

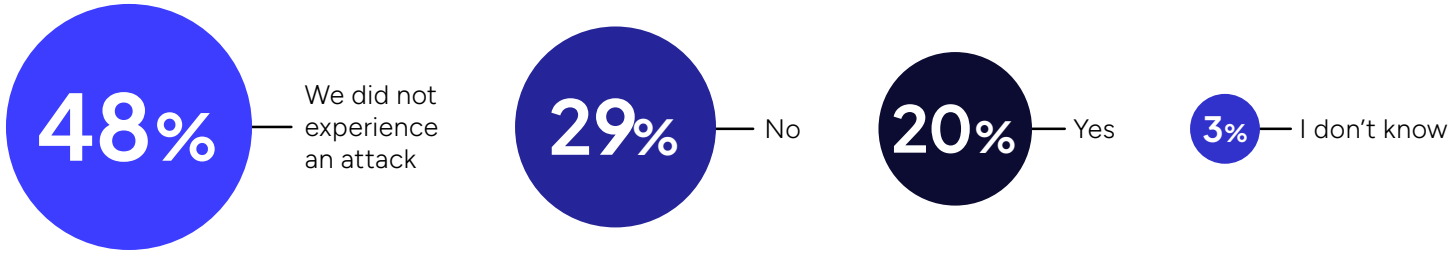


Figure 18. Ransom payment

Of those who paid, 56% successfully decrypted all data. However, a significant 41% could recover only partial data and 2% lost data completely. Of those who refused to pay, 47% were able to perform disaster recovery and restore everything from backups (up slightly from 44% in 2024). Others relied on system reinstallation or partial restores to recover data.

Clearly, paying the ransom is not a guaranteed solution. MSPs have a major role to play in helping clients harden defenses and strengthen backup and disaster recovery strategies.

Anticipated threats and risk perception

Both businesses and MSPs anticipate more frequent, damaging attacks in the next 12 months, with human error and phishing leading the list of risks.

Human error and email: The most feared threat vectors

Looking ahead to the next 12 months, human error and social engineering (29%) stand out as the single most feared threats businesses face. Following closely is email (27%), the primary delivery method for the majority of social engineering attacks. The human factor is a critical area that demands special attention from both organizations and MSPs.

Which of the following threat vectors are you most concerned will be the gateway to a successful attack in the next 12 months?

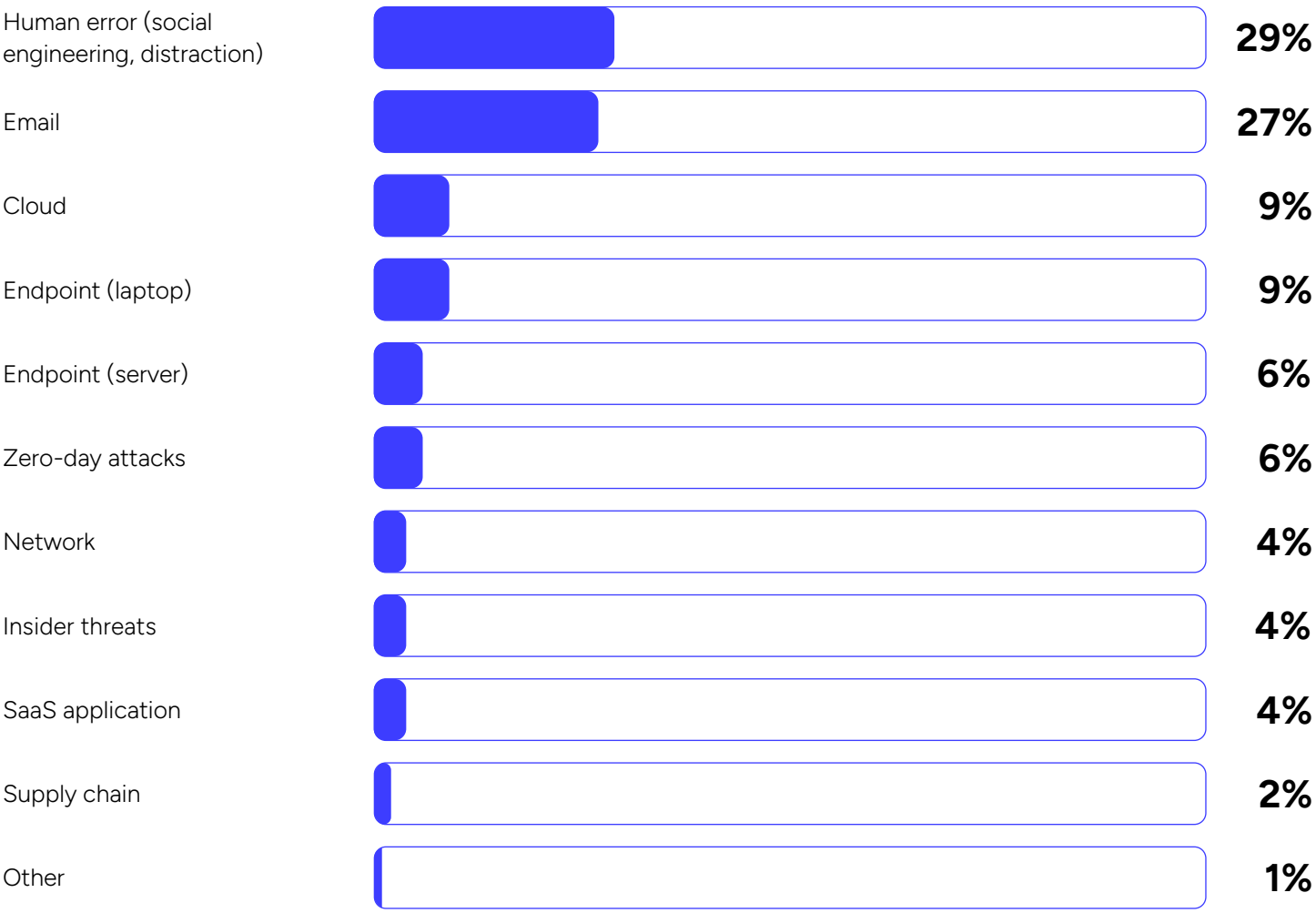


Figure 19. The most feared threat vectors in the next 12 months

Phishing and ransomware loom large

Organizations expect the onslaught of attacks to continue. Almost 70% of businesses surveyed believe they will fall victim to a successful phishing attack in the next 12 months, while more than half anticipate a ransomware breach. These figures suggest that most organizations view successful cyberattacks not as a matter of "if," but "when."

What do you believe is the likelihood that your organization will experience a successful phishing attack in the next 12 months?

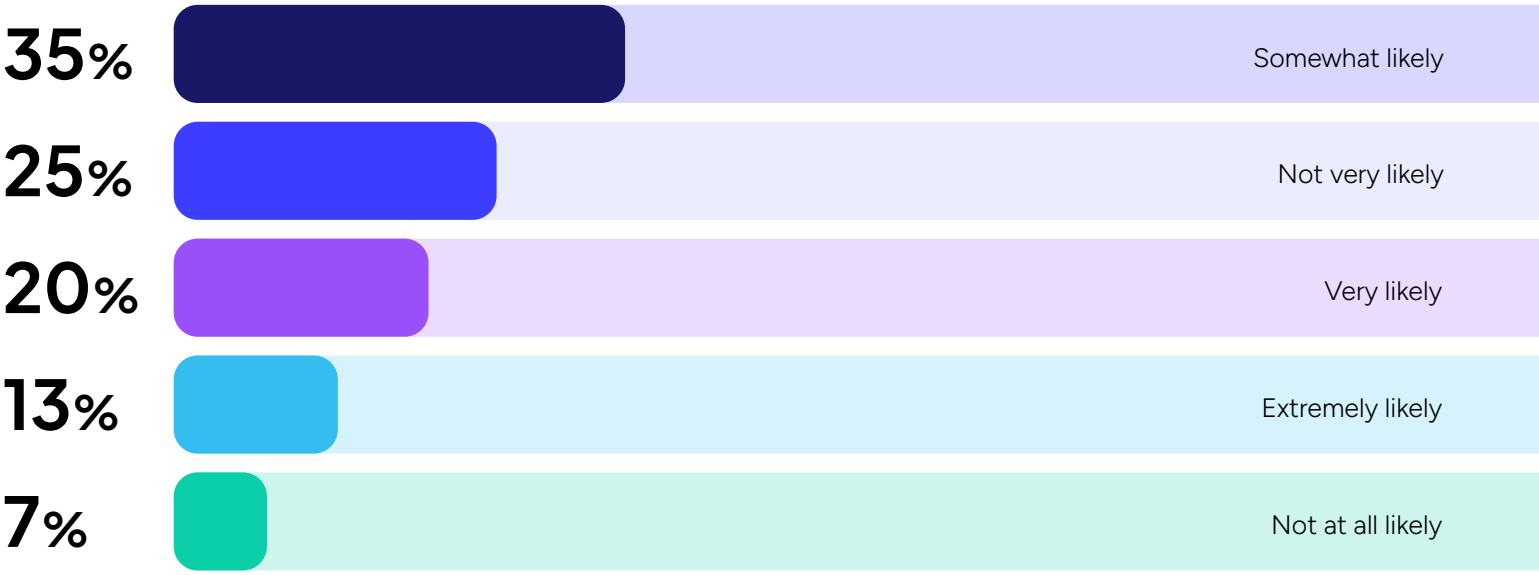


Figure 20. Likelihood of a successful phishing attack in the next 12 months

What do you believe is the likelihood that your organization will experience a successful ransomware attack in the next 12 months?

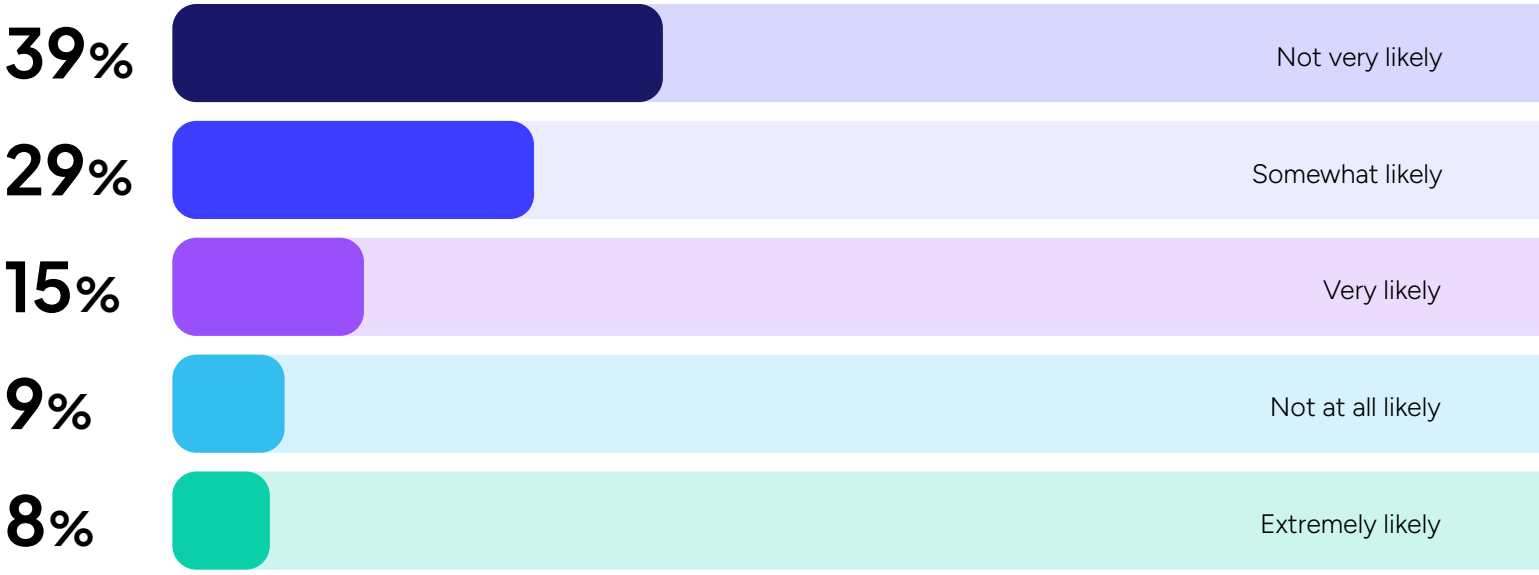


Figure 21. Likelihood of a successful ransomware attack in the next 12 months

MSPs share this pessimism, with 76% believing one of their clients will experience a successful phishing attack in the next 12 months. The top threats they anticipate during that period are phishing (74%), BEC (66%) and malware (44%). Alarmingly, only 2% of MSPs are confident their clients will avoid a successful attack.

Which types of cyberattacks are you anticipating over the next 12 months? (Select all that apply)

Figure 22. Anticipated attack types in the next 12 months

Anticipated impact

When it comes to the impact of future attacks, perceptions diverge. A majority of MSPs (around 60%) believe cyberattacks will cause serious disruption, but not complete collapse, for their clients. Businesses, however, are more pessimistic. Close to 70% of organizations expect extreme or significant impact — a jump from around 60% last year.

This gap highlights the urgency for MSPs to align more closely with client risk perceptions. To close the perception gap and meet client expectations, MSPs must focus on prevention and incident response, recovery testing and employee training.

As an MSP, if a successful cyberattack on your business were to occur, how much impact do you think it would have?

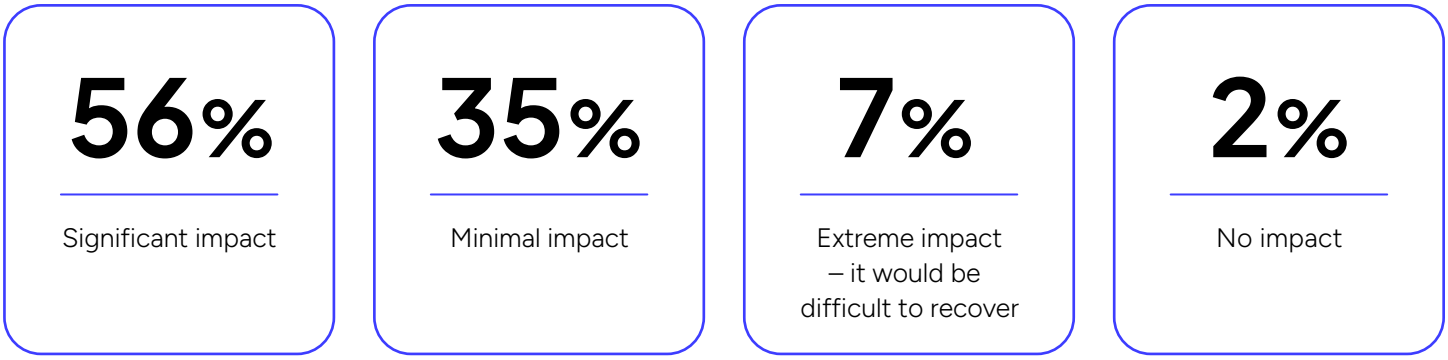


Figure 23. Anticipated impact (MSPs)

As an SMB, if a successful cyberattack on your business were to occur, how much impact do you think it would have?

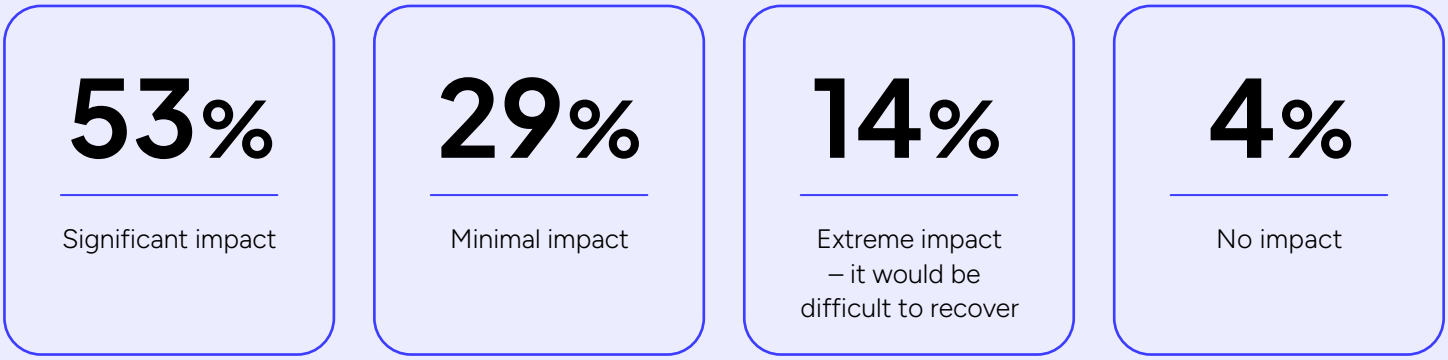


Figure 24. Anticipated impact (SMBs)

Security budgets and service expansion

Cybersecurity budgets are modest but rising, and MSPs are expanding services, which indicates that security is one of the top priorities.

Security spending: Growth amid constraint

Cybersecurity budgets are increasing, but growth remains measured. Most businesses allocate between 10% and 50% of their IT budgets to security, with spending concentrated at the lower end. This suggests that although security is a top concern, it must compete with other IT priorities.

In the past year, 44% of businesses increased their security spend. Confidence in continued budget growth over the next 12 months is strong. Nearly half of all respondents (48%) expect to see budget increases, with 68% of those projecting modest growth of 5%–25%.

This consistent, predictable growth shows that organizations are willing to invest in security. It also sends a strong signal to service providers that the market is expanding reliably, and will favor those providers who can scale their services incrementally to meet these measured budget increases.

Approximately what percentage of your overall IT budget is dedicated to security?

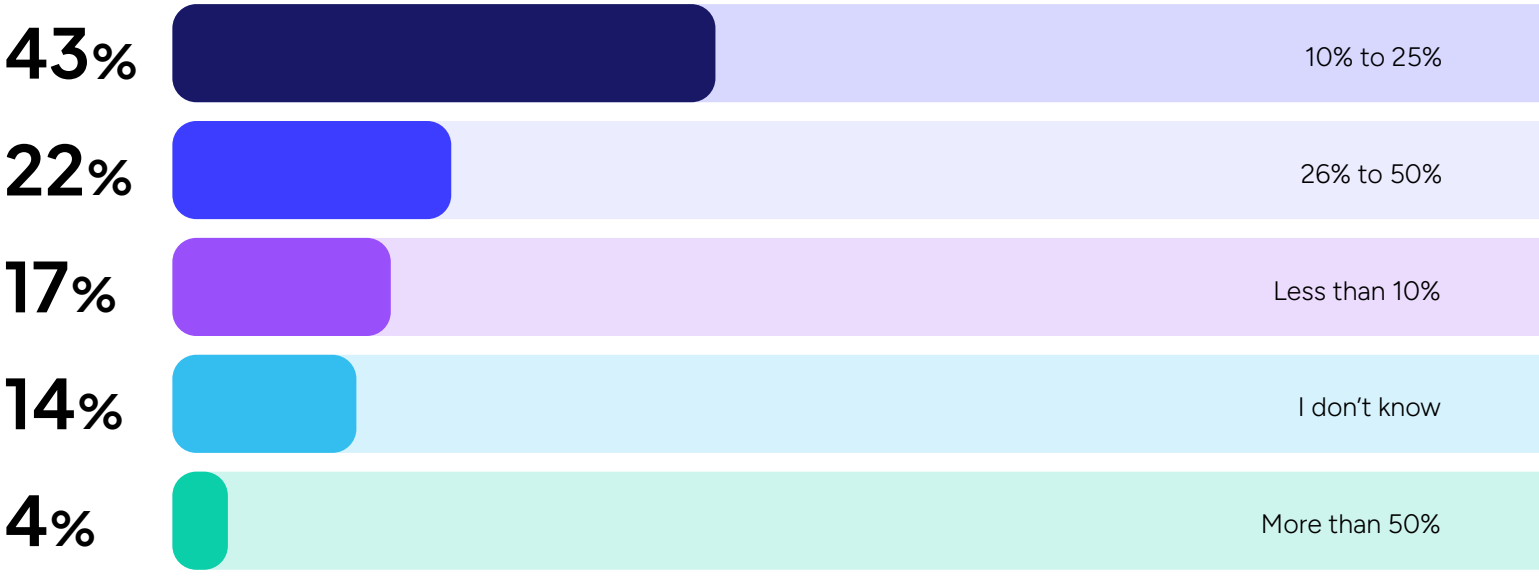


Figure 25. IT budget allocation

Security service expansion: The MSP growth driver

MSPs are clearly taking notice of this steady client investment and the pervasive threat landscape. They view security as the key engine for their own service portfolio growth. A massive 74% of MSPs plan to increase their cybersecurity service offerings over the next year. This high percentage reflects both strong market demand and recognition of the revenue potential in this space.

On one hand, businesses are planning to invest more in security, and on the other, MSPs are preparing to deliver more robust, comprehensive solutions. The winners in this market will be the providers who can balance cost efficiency with layered, proactive defense strategies that match evolving client needs.

What are your plans for your security service offerings?

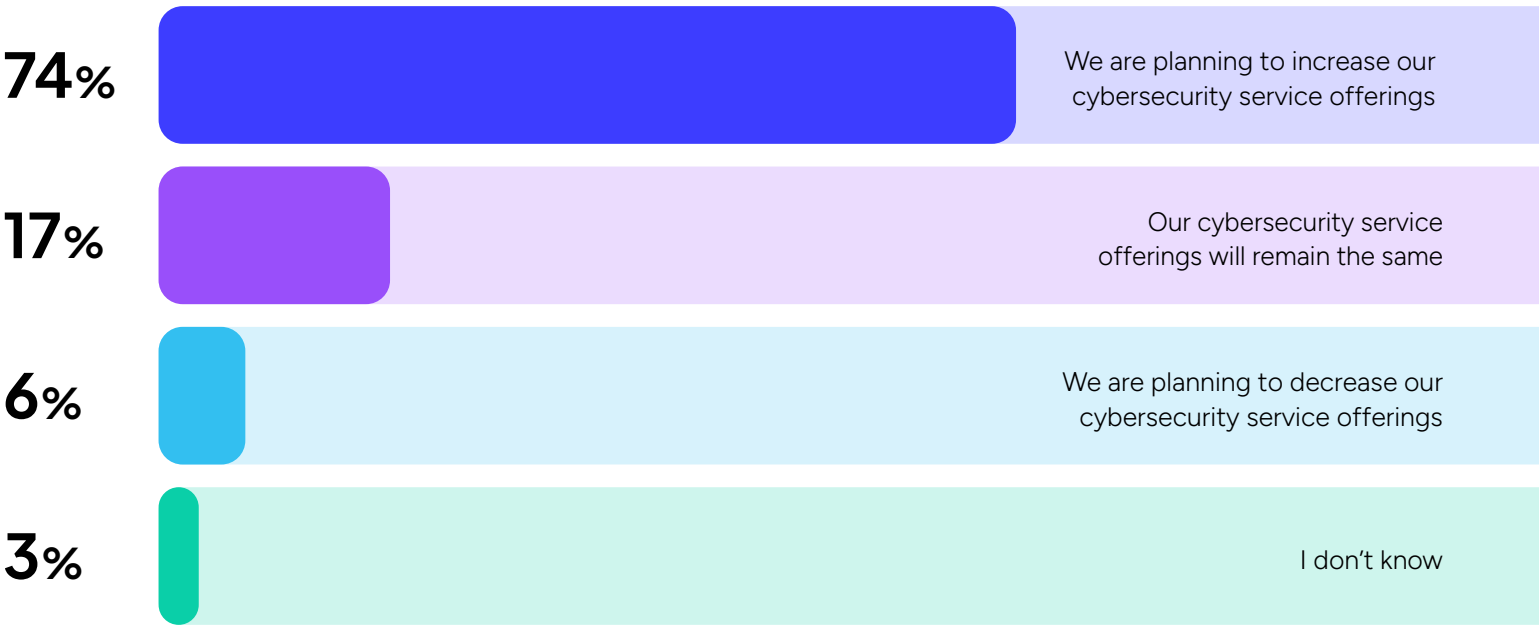


Figure 26. MSP future plans

Challenges shaping tomorrow's security landscape

Tomorrow's biggest security challenges aren't technical alone; they're human, skills, budgets and vulnerabilities MSPs must address.

Preparing for the next wave of challenges

Looking ahead, organizations see their biggest cybersecurity challenges coming more from people and resources rather than from technology. Human error (22%) tops the list, followed closely by shortages in IT and security skills (20%). The top two anticipated challenges both center on the human element, which indicates that the biggest obstacles to a resilient security posture are internal. For 16% of respondents, budgets remain a challenge, while 14% cite exploitable vulnerabilities as a major concern.

Technology alone isn't enough to tackle tomorrow's security management challenges. MSPs must evolve their offerings to solve people and process gaps, not just product gaps. By focusing their innovation on addressing the staffing and human behavioral challenges that clients anticipate most, MSPs can transition from being mere technology vendors to indispensable strategic partners.

What do you anticipate will be your top security management challenge in the next 12 months?

Human error	22%
IT and security skills	20%
Budget	16%
Governance (e.g., NIST framework)	14%
Antivirus software	9%
Security awareness training	7%
Zero-day attacks	4%
Insider risk	3%
Supply chain risk	2%
Hiring	2%
Other	1%

Figure 27. Anticipated security management challenges for the next 12 months

Key takeaways and next steps

The cybersecurity landscape is shifting quickly. To stay relevant and competitive, MSPs must align with client needs, bridge the gap between human error and skills shortage, and expand services.

Key takeaways

Here's a quick summary of key security insights:

- While core defenses are common, proactive measures remain inconsistent.
- Human error and phishing continue to dominate as the top risks.
- Trust in AI and preparedness for incident response remain limited.
- Organizations recognize that their biggest security challenges aren't technology failure but human error and a shortage of skilled IT and security talent.
- Cyberattacks are viewed as inevitable, making reliable, comprehensive protection a necessity.
- Steady but consistent investments in security create a great growth opportunity for strategic MSPs.

Practical recommendations

- Prioritize people-first security. Address human error with continuous security awareness training, phishing simulations and security culture development.
- Expand proactive defenses. Offer penetration testing, vulnerability management, MDR and SOC services to fill critical client gaps.
- Focus on integration, not tools. Look for a unified platform to simplify management and reduce the complexity that overwhelms in-house teams.
- Leverage AI responsibly. Deploy AI-powered solutions for email, endpoint and threat detection while reassuring clients with human oversight.
- Bundle services for value. Package security offerings to make advanced tools affordable and predictable, even for budget-constrained clients.
- Help clients meet requirements for cyber insurance coverage and prepare for audits with clear documentation.
- Strengthen resilience. Drive adoption of incident response planning, tabletop exercises and disaster recovery to minimize downtime and losses.

The path forward

Cybersecurity is here to stay, and MSPs who act now will lead tomorrow's market.

To expand your service offerings and close client security gaps, explore the full Kaseya security suite. Equip your MSP business with the right tools, intelligence and support you need to deliver unmatched value.

Explore the Kaseya security suite today.

Respondent overview

This year's cybersecurity outlook survey gathered insights from 713 SMBs and 375 MSPs worldwide, providing a comprehensive perspective on industry trends, challenges and opportunities.

Survey methodology

Kaseya conducted its "2025 cybersecurity outlook survey" in July 2025 using a structured questionnaire. Participants identified whether they were employed in IT operations with cybersecurity responsibilities or worked at/owned an MSP. The final analysis reflects responses from 1,193 qualified participants who completed the survey. The study focused on IT security trends, emerging threats and cyber readiness at small and midsize organizations.

Kaseya®

Kaseya is the leading global provider of AI-powered IT management and cybersecurity software. Kaseya delivers a unified technology platform to manage infrastructure, secure endpoints, back up critical data, and streamline operations for more than 40,000 MSP and SMB customers around the globe. To learn more, visit www.kaseya.com.

kaseya.com