July 2025

Market report

The MSP Customer Insight Report 2025

What organizations worldwide need from their cybersecurity managed service providers

Barracuda®
Your business, secured.

Contents

Introduction 3

Key findings 4

The customer base for MSPs 5

Customers need MSPs to help them manage security as they grow 6

Customers will need more support with AI and network security in the future 8

Customers are willing to pay more for the services they want 9

MSPs risk losing customers if they can't prove expertise 11

Organizations hit with a breach invest more in security and outsourcing 12

Conclusion 13

Introduction

This report explores what organizations worldwide need and expect from their managed service providers (MSPs) when it comes to cybersecurity services. It draws on the findings of a new international survey of MSP customers commissioned from Vanson Bourne.

MSPs have become business critical. Most of the organizations surveyed are already outsourcing some or all of their cybersecurity needs to MSPs, and others are exploring opportunities.

This report aims to help MSPs understand what their existing customers need from them now and in the future, what their potential customers look like and where to find them, and what drives customers away to a competitor.

Overall, the findings show that:

- Customers need MSPs to help them manage their security as they grow.
- Over the next few years, customers will particularly need help with the implementation of AI/machine learning applications and network security — and they're willing to pay more for it.
- Most MSP customers will consider switching providers, and the reasons include concerns about the MSP's ability to help them remediate and recover from a cyberattack.

We hope this report will help MSPs shape their future strategies, identify new opportunities and address any gaps. Barracuda is here to help every step of the way. Together, we can ensure more organizations are cyber resilient and protected as we face the headwinds of ever-evolving threats.

Methodology

Barracuda commissioned independent market research company Vanson Bourne to conduct a global survey of 2,000 senior security decision-makers in IT and business roles in organizations with between 50 and 2,000 employees from a broad range of industries in the U.S., UK, France, DACH (Germany, Austria, Switzerland), Benelux (Belgium, the Netherlands, Luxembourg), the Nordics (Denmark, Finland, Norway, Sweden), Australia, India, and Japan. The survey was fielded in April and May 2025.

Key findings

85%

of organizations with 1,000 to 2,000 employees rely on MSPs for security support, compared to 61% of those with 50 to 100 staff

48%

of organizations turn to MSPs for 24-hour security support

52%

of organizations turn to MSPs for help when the number of security tools becomes unmanageable — the top reason cited

51%

of organizations turn to MSPs to help them evolve their security strategies as they grow — the second most cited

39%

of organizations expect to need MSP support with AI and machine learning tools and applications in the next few years — the top reason cited

92%

of organizations are prepared to pay more for support with security tool integration

45%

will switch MSPs if they can't see evidence of skills, expertise and the ability to support them with 24/7 security — the top reason cited

The customer base for MSPs

Cyberthreats continue to evolve as attackers take advantage of artificial intelligence tools and criminal services-for-hire to launch increasingly sophisticated attacks — and to do so faster, in higher volumes and with greater precision.

IT and security professionals face a constant bombardment of such threats. To keep the organization and its assets protected, they need advanced security solutions as well as around-the-clock monitoring, management and mitigation capabilities, and a deep understanding of the threat landscape. Few organizations can meet all those needs in-house.

Key finding: 73% of the organizations surveyed outsource security services to an MSP

96% of the organizations surveyed are either already engaged with or considering working with an MSP: 73% say they already outsource security services to an MSP, with a further 18% currently evaluating providers, and another 5% considering the possibility of using an MSP.

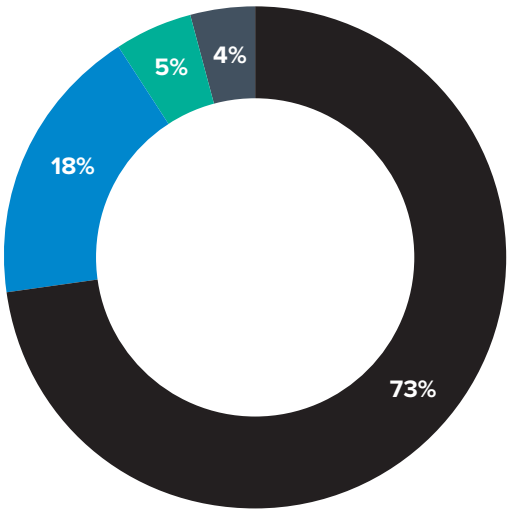

FIGURE 1

Does your organization outsource any IT security activities to a managed service provider (MSP)?

n=2,000

- Yes
- We're currently evaluating providers
- We're considering the possibility
- No

There are some interesting variations behind these numbers.

For example, the largest organizations surveyed are more likely to use MSPs than the smaller ones.

Key finding: 85% of respondents with 1,000 to 2,000 employees rely on MSPs for security support, compared to 61% of those with 50 to 100 staff

This higher level of MSP engagement may reflect the fact that larger organizations have greater security complexity and a broader range of tools to manage.

For example, the larger organizations surveyed tend to worry more than smaller ones about the growing complexity of their security environment (42%) and the growing complexity of cyberattacks (46%). For the smallest companies surveyed, the corresponding numbers are 32% and 34%.

A slightly worrying 10% of the smaller organizations surveyed have no plans to engage an MSP to help them with cybersecurity. Smaller companies generally have fewer in-house resources available for protection, so this approach could leave them vulnerable to attack.

The industries most likely to outsource cybersecurity to MSPs are local government (84%) and education (78%). There is a lower level of engagement in recreation and entertainment (60%), retail (65%) and manufacturing (57%).

Among the countries surveyed, organizations in the UK and Benelux are the most likely to work with an MSP (with 79% and 81% respectively doing so). The lowest levels of collaboration are seen in the Nordics (54%) and Japan (59%).

Customers need MSPs to help them manage security as they grow

The research shows that from the customers' perspective, the ideal MSP partner offers both practical, product- and technology-focused support and more strategic help in terms of security plans and compliance.

Looking at the top two results suggests that MSPs play a key role in helping organizations to manage the security implications of business growth.

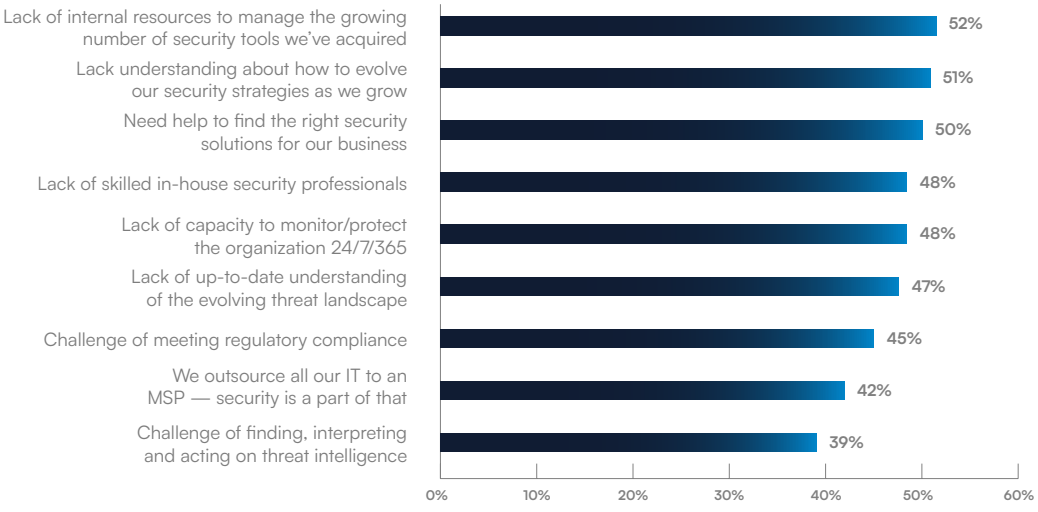

FIGURE 2

The reasons for outsourcing security to an MSP

n=2,000

Key finding: 52% of organizations turn to MSPs for help when the number of security tools becomes unmanageable

Support for juggling an ever-growing stack of security products was the most common reason given for turning to MSPs. Many of these tools are likely to be from different vendors, and most don't integrate with each other.

This figure rises to 60% among respondents in manufacturing. Manufacturing companies are likely to have a significant number of connected systems and IoT devices and therefore a higher probability of security tool sprawl.

Other findings from the study show that the lack of integration can increase security risk and exposure, making it harder and more expensive to manage security and to detect and mitigate threats.

Key finding: 51% of organizations turn to MSPs to help them evolve their security strategies as they grow

The second most widely cited reason for turning to an MSP for security support reflects the evolving role of service providers as security advisors: 51% look to their service partner to help them evolve and update their security strategies as the organization expands and changes. Education and healthcare organizations were particularly likely to list this as a reason for engaging an MSP (both at 55%).

Educational institutions are also among the most likely to worry about the growing complexity of their IT security (48% compared to 38% overall), which suggests that they are struggling to protect a growing number of digital assets. Turning to an MSP for help is a natural step for them.

Key finding: 48% of organizations turn to MSPs for 24-hour security support

Most organizations recognize that cybersecurity is an around-the-clock activity, and that this demands staffing levels and investment that many of them don't have in-house. Relying on an MSP for help in monitoring and responding to threats and security alerts 24/7 is another top driver of engagement.

Many MSPs now operate, often together with security vendors, a managed security operations center (SOC) that provides such expert coverage. To get the most comprehensive security, this can be combined with a managed extended detection and response (XDR) solution that can cover the breadth of the attack surface, including endpoints, email, cloud, applications, and networks.

For many of the organizations surveyed, engagement with MSPs is also closely tied to the lack of in-house cybersecurity professionals — cited as a reason by 48%. The skills shortage appears to be a universal challenge as the proportion remains consistent across all company sizes.

In the case of 42% of respondents, security is outsourced to an MSP and bundled with other IT services. This represents both an opportunity and a risk for MSPs, particularly when it comes to customers deciding to move their business — see the section on deal-breakers.

Customers will need more support with AI and network security in the future

Over the next two years, customers are most likely to seek help from MSPs for implementing AI and machine learning tools and applications. This is followed by help for network security implementations such as zero-trust measures and SASE (secure access service edge) solutions.

Key finding: 39% of organizations expect to need MSP support with AI and machine learning tools and applications in the next two years

AI and network security are areas of growing business focus, security vulnerability and technical complexity. They can be hard to understand, especially for the 48% of understaffed organizations.

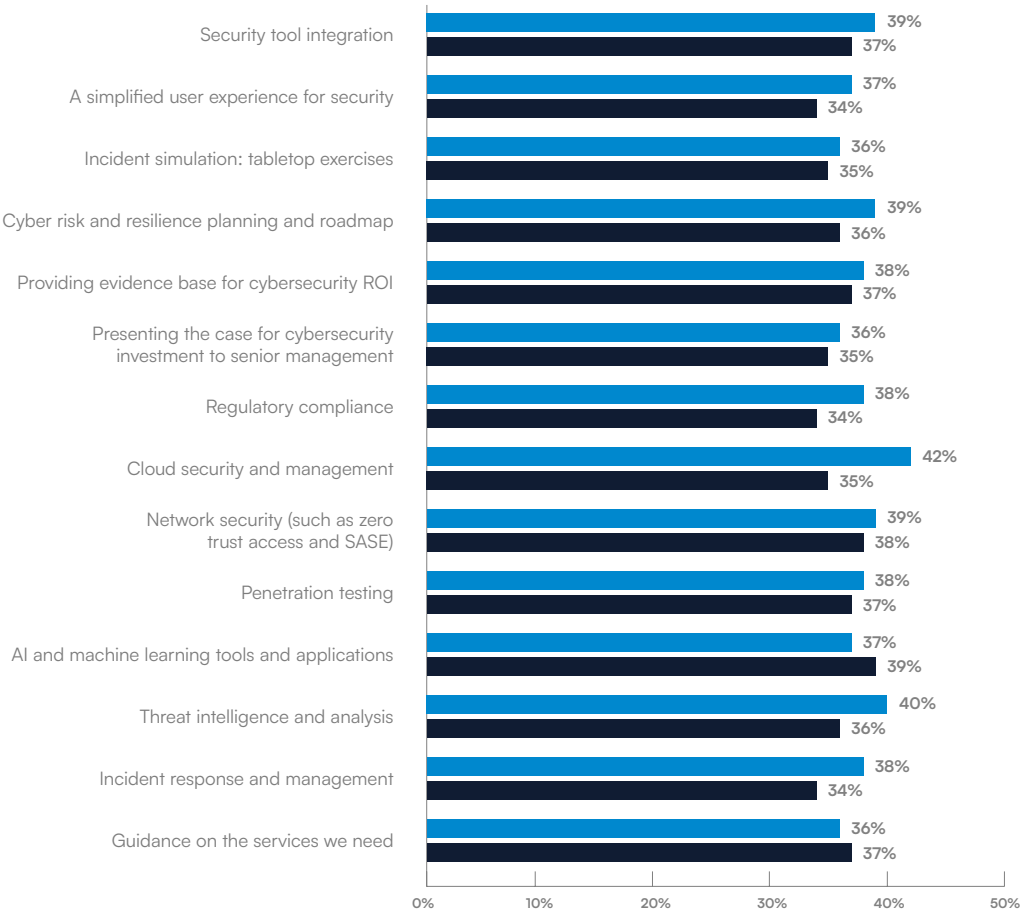

FIGURE 3

Security opportunities for MSPs: Where organizations expect to need support from service providers in the next 1 to 2 years

n=2,000

Already use from MSP

Expect to need support

The findings highlight the different journeys for organizations of different sizes.

For example, among organizations with 50 to 100 employees, the proportion looking for future support with AI rises to 44%, with 29% already engaged. For the largest organizations, 44% are engaged with MSPs on AI, and 37% expect to need support in the next two years.

This suggests that the larger organizations already understand the limitations of dealing with AI and machine learning by themselves — and are actively engaging with MSPs to optimize their use of AI in both IT and security. A similar picture, but with smaller differences, is seen for network security.

It is also worth noting the widespread use of and demand for strategic services such as cyber risk and resilience planning, incident response simulation and presenting the case for cybersecurity ROI.

Customers are willing to pay more for the services they want

The survey found that almost all MSP customers are prepared to pay more for the additional services they need over the next two years, and around 70% are prepared to pay up to 10% or 25% more.

Key finding: 92% of organizations are prepared to pay more for support with security tool integration

The services for which they are most likely to be willing to spend more include AI and machine learning tools and applications, cloud security and network security. The results remain consistent across all company sizes.

Overall, operational tools and activities fare better when it comes to added spend. There is some reluctance to spend extra on 'softer' services such as incident simulation, presenting the case for cybersecurity investment or guidance on the services needed.

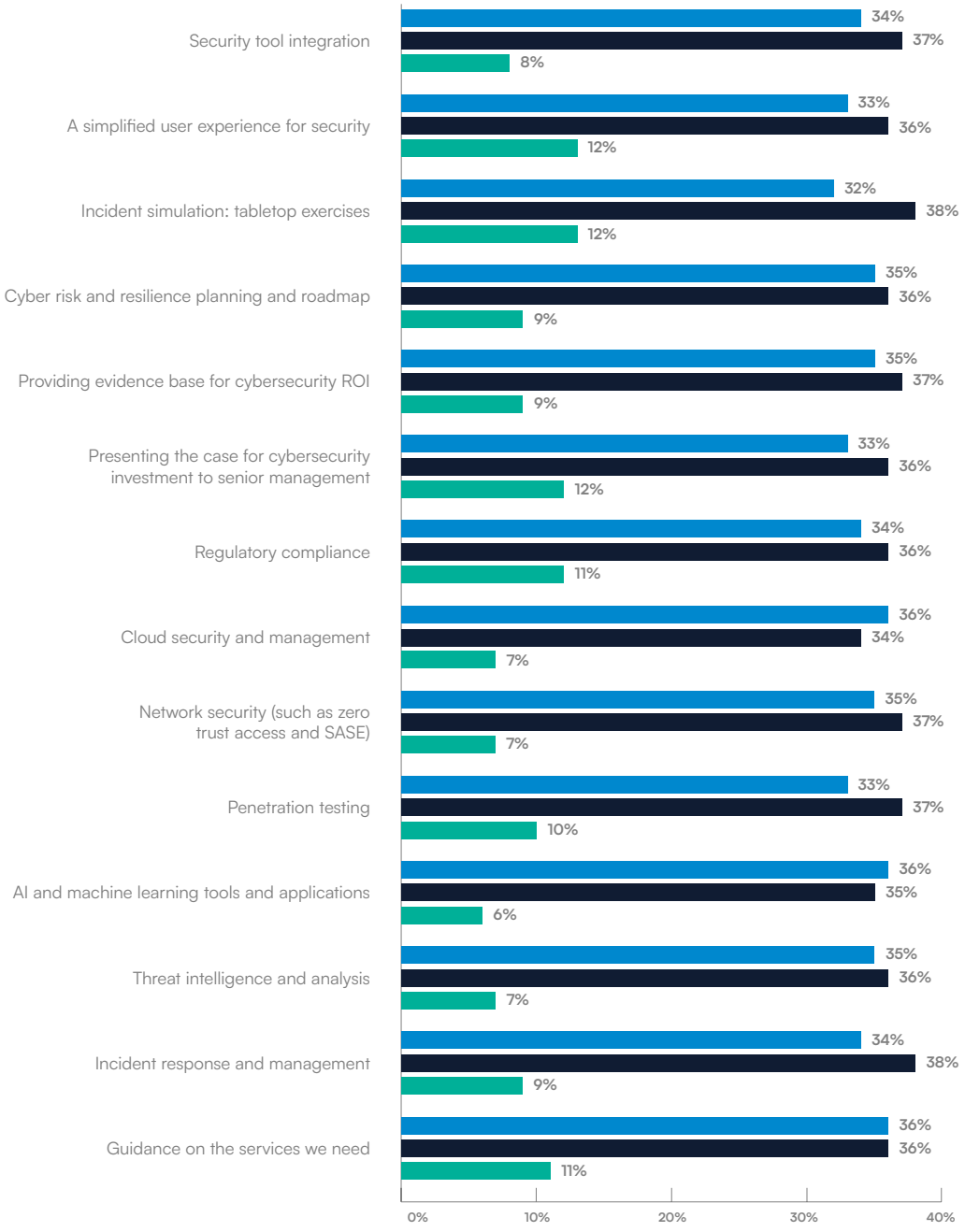

FIGURE 4

Additional costs organizations are prepared to pay for these services from MSPs in next 1 to 2 years

n=2,000

- Prepared to pay up to 25% more
- Prepared to pay up to 10% more
- Not prepared to pay more for this

However, what customers prioritize and are prepared to invest in looks very different when seen through the lens of a security incident — such as an email-based incident or a ransomware hit — see the section on the impact of a security breach below.

MSPs risk losing customers if they can't prove expertise

The findings show that when it comes to sticking with an MSP partner, loyalty is limited and depends on the customer's confidence in the expertise, quality and business stability of the service provider. Just 2% of respondents said they couldn't imagine switching to another MSP. For everyone else, there are some clear deal breakers.

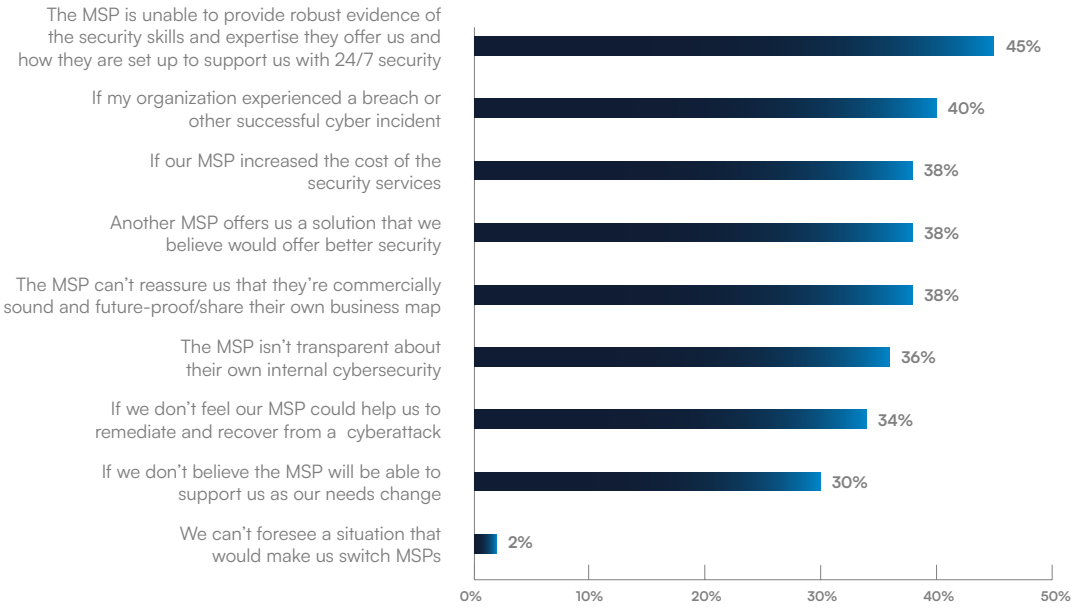

FIGURE 5

What would make you consider switching to another MSP for cybersecurity support?

n=2,000

A security breach is a clear relationship killer, and for more than a third (38%) of MSP customers a price increase or a better offer from another MSP would lead them to switch sides.

Key finding: 45% will switch MSPs if they can't see evidence of skills, expertise and the ability to support them with 24/7 security

For the impacted MSPs, this is not just a question of losing the cybersecurity business — 89% of the outgoing customers who have bundled IT services with security will remove those activities too, either at the same time (46%) or later (42%).

It is worth mentioning that 38% of MSP customers say they will switch if the MSP increases costs. Taken together with the findings around willingness to invest, this suggests that MSP customers will happily pay more for the services they want and need but are less comfortable about price hikes arbitrarily imposed on them by the MSP.

The good news is that the potential deal-breakers are almost all areas that MSPs can address by investing in their own business and security resilience and that of their customers, and by strengthening trust and transparency.

Organizations hit with a breach invest more in security and outsourcing

A successful email breach or ransomware attack shifts security priorities.

The differences between those who have been hit and those who have not are clear when you look at the services that they are prepared to pay more for and the activities they have realized they cannot effectively manage in-house. These findings shine a light on the areas where the victims may feel particularly exposed.

Key finding: 91% of attack victims are willing to pay more for a simplified security user experience, compared to 77% of non-victims

For example, 91% of victims are willing to pay more for a simplified user experience for security, compared to 77% of those that haven't been hit. The overall figure is 88%. This suggests that for many victims, human error or misconfiguration — both easily triggered by complex user interfaces — may have played a part in the attack.

Victims are also more willing to pay more for cyber resilience services such as incident response planning, regulatory and compliance understanding, and strategic guidance on security services. This suggests that victims are willing to invest in areas that leave them better prepared to respond to and recover from future attacks.

When it comes to activities undertaken in-house or outsourced, the same disparity is seen — those that have not been directly affected by an incident are more likely to feel they can handle things themselves.

Key finding: 81% of attack victims plan to outsource cloud security and management, compared to 73% of non-victims

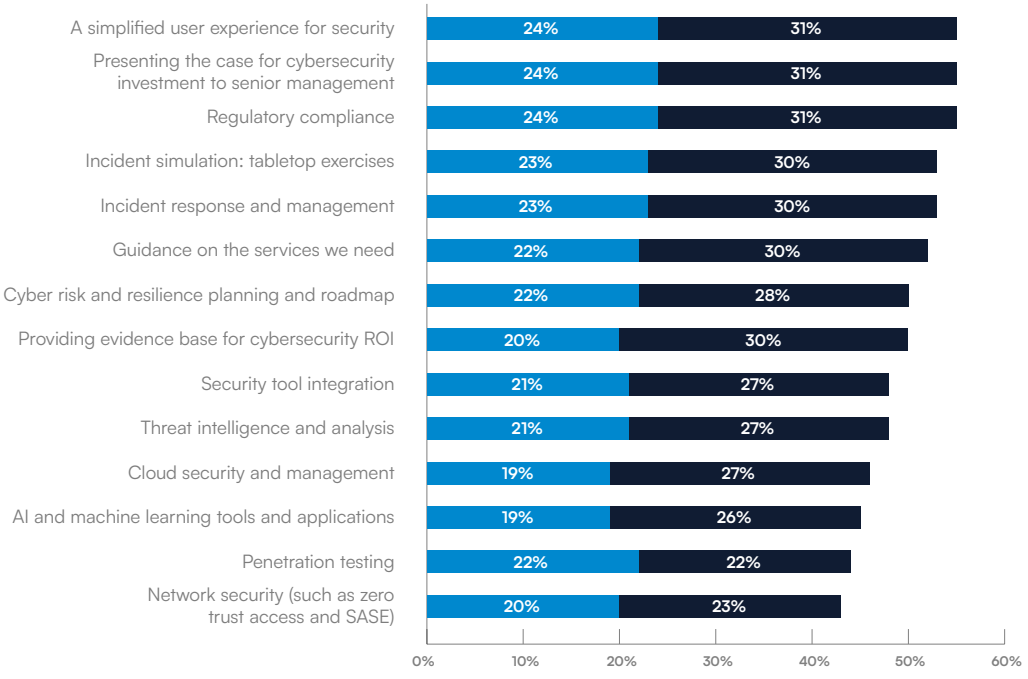

FIGURE 6

Organizations that plan to manage each of the following in-house over the next 1 to 2 years

n=2,000

- Has experienced an email breach or a successful ransomware attack in the last year
- Has not experienced an email breach or a successful ransomware attack in the last year

Conclusion

The findings show that in 2025 MSPs face many promising opportunities — but there are also some challenges.

For example, many customers want help managing security sprawl. However, helping multiple customers juggle multiple products can quickly become overwhelming for providers. Security vendors have an important role to play in helping MSPs integrate management, response and reporting activities through centralized dashboards and product consolidation. Similarly, vendors can help MSPs meet the clear demand for 24/7 security monitoring with managed SOCs.

Then there is the need to support customers through compliance and regulations and with the implementation of AI and machine learning tools and applications.

In addition, MSPs need to prepare for customers wanting more proactive and predictive services, such as threat intelligence, incident response planning, risk management, and strategic consulting.

As if that isn't enough, MSPs also need to look to their own commercial viability and provide evidence of expertise and a robust business model — or risk losing customers to competitors. This requires a product portfolio that is advanced and innovative but also easy for customers to buy, deploy and use. It also requires security vendors who are committed to partnering.

How Barracuda can help

At Barracuda, we are 100% committed to the channel and to helping our partners succeed and grow.

BarracudaONE™

BarracudaONE is an AI-powered cybersecurity platform that delivers integrated products accessible from a centralized dashboard to maximize protection and cyber resilience, while being easy to buy, deploy and use.

The platform simplifies the administration of security tools for an MSP across all of their customers, ensuring tools are properly configured, alerts are centralized, and reports are provided that show the value an MSP brings to their customers around security.

BarracudaONE is available at no additional cost to MSPs, other channel partners and customers already using Barracuda Email Protection, Barracuda Cloud-to-Cloud Backup and Barracuda Data Inspector. The platform provides a centralized interface for MSPs and partners to easily manage solutions and licenses.

Barracuda Managed XDR™

MSPs, partners and end users can further strengthen their security posture with Barracuda Managed XDR, a 24/7 service that delivers expert threat detection and response backed by Barracuda's award-winning SOC.

About Barracuda

Barracuda is a leading global cybersecurity company providing complete protection against complex threats for all sized businesses. Our AI-powered platform secures email, data, applications, and networks with innovative solutions, managed XDR and a centralized dashboard to maximize protection and strengthen cyber resilience. Trusted by hundreds of thousands of IT professionals and managed service providers worldwide, Barracuda delivers powerful defenses that are easy to buy, deploy and use.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research in the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision-makers across technical and business functions in all business sectors and all major markets. For more information, visit vansonbourne.com.