CONNECTWISE

CONNECTWISE EBOOK SERIES

THE STATE OF SMB CYBERSECURITY: RACING AGAINST AI-DRIVEN CYBERTHREATS

VansonBourne

Vanson Bourne Research
Commissioned by ConnectWise

2025

Contents

Foreword

The cybersecurity landscape is evolving at a pace and scale unlike anything we've seen before.

Small and midsized businesses (SMBs) now face unprecedented cybersecurity challenges, driven by the rapid adoption of artificial intelligence (AI) and the widespread shift to remote work. These technological advances have created powerful new opportunities but have also introduced increasingly sophisticated threats, putting greater pressure on businesses to strengthen their defenses.

Cybersecurity is a critical business priority that directly impacts an organization's reputation, financial health, and long-term success. SMBs that recognize this shift are taking action, yet concerns about the reliability of their cybersecurity partners persist. Building trust, demonstrating transparency, and delivering proven protection are more important than ever for managed service providers (MSPs) seeking to support and safeguard their clients.

The message is clear: success in 2025 and beyond will belong to those who lead with expertise, innovation, and partnership. To build lasting relationships with their customers, MSPs must start with these three strategies: engage proactively with SMB clients, deliver AI-informed cybersecurity solutions, and find the right balance between risk mitigation and budget management. MSPs and SMBs can confidently navigate today's threats together and build a more secure future.

We invite you to explore the valuable insights in this report as we work together to create a stronger, safer digital future for all.

Patrick Beggs
Chief Information Security Officer
ConnectWise

Introduction

AI and the rise of remote work are transforming how businesses operate and how they are attacked.

Cybercriminals are weaponizing AI to automate attacks, exploit vulnerabilities, and bypass traditional security measures, creating a more complex threat environment. At the same time, the rise of remote work has expanded the attack surface, giving adversaries more entry points than ever to exploit.

SMBs are increasingly recognizing this and are placing greater emphasis on cybersecurity in 2025. In fact, over half (51%) now rank cybersecurity as one of their top three future priorities, higher than business growth (40%) and customer satisfaction and retention (33%). This shift reflects a more proactive approach as more SMBs recognize the importance of cybersecurity for their reputation, revenues, and long-term viability.

MSPs are seen as valuable partners in this fight, helping to:

- ✓ Strengthen security
- ✓ Enhance IT performance
- ✓ Accelerate technological adoption
- ✓ Offer specialized expertise
- ✓ Provide advice on AI security

However, SMB concerns about MSP reliability continue to linger year-over-year (45%), potentially threatening long-term customer satisfaction and loyalty. Reliability can encompass a range of factors, from consistent uptime and dependable IT service delivery to responsiveness and customer support quality.

The stakes for MSPs are high: almost four-fifths (79%) of SMBs would consider legal action after a successful cyberattack, and nearly half (47%) would consider moving to a new MSP if offered the "right" cybersecurity solution.

To address these concerns, MSPs can focus on the robustness of their solutions, continuously upskilling staff, and providing evidence of reliability through transparent reporting, certifications, and customer success stories. Staying ahead of the cybersecurity curve is not only about risk mitigation; it's about building competitive advantage and fostering long-lasting customer trust and loyalty.

To explore these trends in more depth, ConnectWise partnered with market research agency Vanson Bourne.

Vanson Bourne's research explores these trends and examines how SMBs are evolving their cybersecurity strategies and expectations of MSPs. Seven hundred IT and business decision-makers were interviewed across the US (300), UK (150), Canada (100), and Australia/New Zealand (150) from private and public sectors, representing organizations with between 10 and 1,000 employees.

Key Findings

SMBs underestimated their cybersecurity risk, leaving them underprepared and overexposed. As a result, many added unplanned budgets to ensure proper protection. In 2025, cybersecurity is becoming a top priority for SMBs, including increased focus on protecting endpoints, networks, personnel, and AI-driven systems.

- **58%** spent more on cybersecurity in 2024 than originally anticipated
- **57%** say that cybersecurity is their organization's top priority, compared to 43% in 2024, an increase of 14 percentage points in a single year
- **51%** state that protecting against cybersecurity attacks is among their top three priorities over the next 2 years compared to 35% in 2024; it's a bigger concern than increasing growth (40%) or customer retention and satisfaction (33%)

Malicious actors are increasingly leveraging AI to launch more sophisticated cyberattacks, leaving many SMBs worried that cyberattacks could shut down their operations entirely. Yet, despite these fears, the slow adoption of security for AI integrations continues to leave many vulnerable.

- **61%** are worried that a serious cybersecurity attack could be enough to put them out of business
- **83%** state that AI/GenAI increases the cybersecurity threat level for their organization
- But only **51%** have implemented security policies and practices for AI/GenAI

Despite growing reliance on MSPs for cybersecurity, doubts about their ability to deliver remain, with many SMBs ready to walk—or take legal action—if they're let down.

- **58%** now see increased security as a key benefit of using an MSP, up from 40% in 2024
- Almost a third (**32%**) would hold their MSP solely responsible in the event of a cyberattack, with many (79%) open to pursuing legal action
- Almost three quarters (**73%**) are not confident their MSP would be able to defend their organization effectively in all cases if they were a target of a cybersecurity attack
- Nearly half (**47%**) would definitely consider using or moving to a new MSP if they offered the "right" cybersecurity solution.
- MSP reliability remains a top challenge for organizations (**45%**), with little improvement since 2024 (44%)

Section 1

The Cybersecurity Wake-Up Call for SMBs

SMBs underbudgeted for cybersecurity in 2024; many underestimated the growing threat landscape.

In 2024, SMBs increased their cybersecurity investments for advanced network protection (85% increased their budgets), securing AI use (84%), endpoint detection (83%) and security awareness/training (80%). These increases reflect the pressures of integrating AI technologies with new security frameworks (including solutions like security awareness training). Meanwhile, the continued use of hybrid and remote work environments has broadened **the attack surface**, introducing additional endpoints and distributed networks.

However, the results suggest that many SMBs initially underestimated their cybersecurity risk, with 58% spending more on cybersecurity in 2024 than originally anticipated. This underestimation wasn't isolated, with roughly 30% noting unplanned investments across each investment area (Figure 1). This points to a systemic risk assessment and planning shortfall, indicating that many SMBs lacked a clear understanding of the shifting threat landscape.

Ultimately, a lack of understanding could leave organizations exposed to risks, potentially requiring resources to be diverted from other strategic initiatives to focus on cybersecurity, resulting in disrupted business plans for the wider organization.

> "The severity of cyber risks is not fully recognized, leading to underinvestment in cybersecurity."
>
> *– IT decision maker, Information Technology, USA*

Areas organizations invested more in over the past 12 months

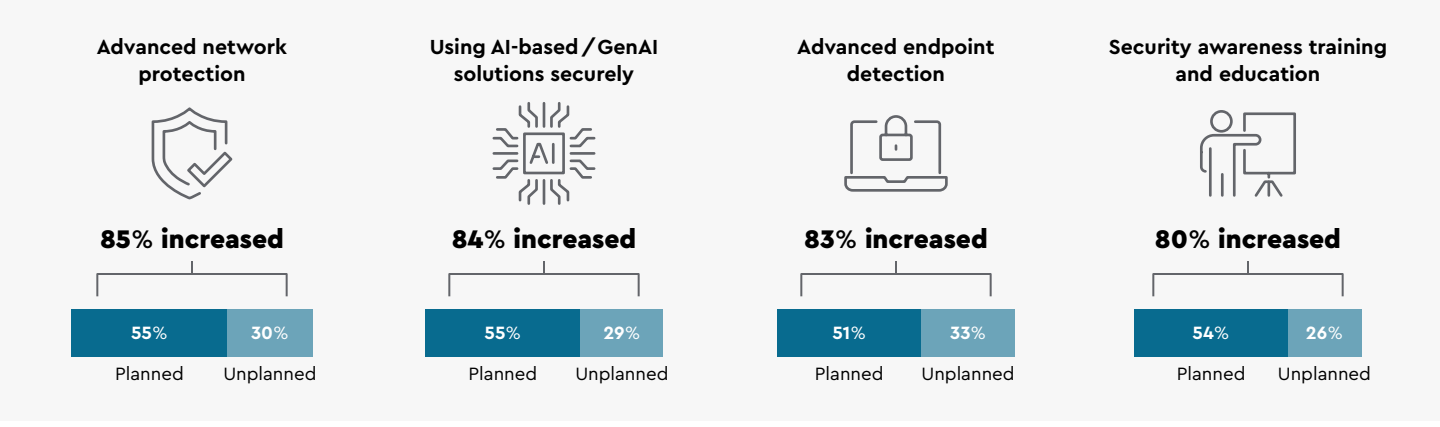


Figure 1: Which of the following areas did your organization invest more in during the past 12 months, if any? How did this align with your organization's plans?

Organizations are ramping up their cybersecurity focus in 2025.

Cybersecurity is now more likely to be seen as a top organizational priority than in any year surveyed since 2021. This heightened focus is expected to persist as cybersecurity remains a leading priority area for the next two years, reflecting a shift towards more proactive risk management in a rapidly evolving threat landscape.

Interestingly, SMBs are more likely to rank cybersecurity (51%) among their top three future priorities, above increasing growth (40%) or customer satisfaction and retention (33%). As awareness of cybersecurity threats and their potential impact grows (see Section 2), SMBs seem to be seeing cybersecurity as a cornerstone of business resilience.

Cybersecurity is critical to our business—it is a top priority

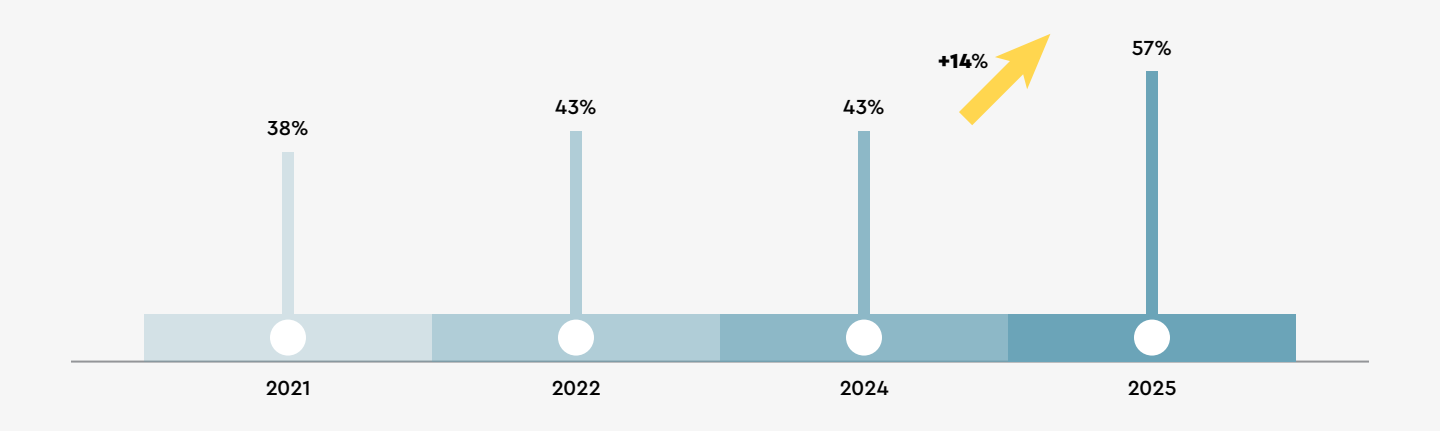


Figure 2: Which of the following statements most closely reflects your organization's stance on cybersecurity? Cybersecurity is critical to our business—it is a top priority

> "A brand-new vulnerability gets discovered, and before companies can patch it, attackers are already exploiting it. We do our best to stay updated, but there's always that window where you're just exposed." *– IT decision maker, IT & Technology, USA*

Planned cybersecurity investments in 2025 point to a reassessment of previously underestimated risks. Key focus areas include security awareness training (46%), advanced network (45%) and endpoint protection (44%), and securing growing AI use (40%).

Country and sector highlights

Cybersecurity is most frequently cited as a top priority in the following sectors:

- IT, technology, and telecoms (**75%**)
- Financial services (**71%**)

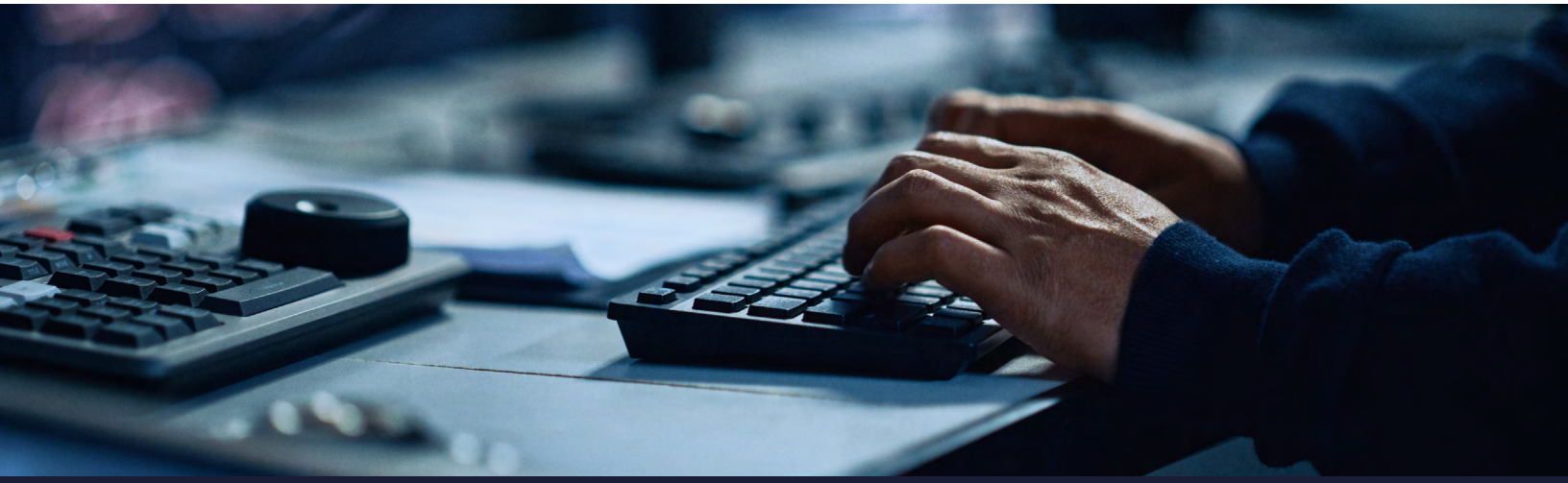
Professionals in IT and financial services are likely more attuned to cybersecurity threats and their potential impact on operations and business continuity.

Among the markets surveyed, **Australia and New Zealand** prioritized cybersecurity the most, with 63% identifying it as a top priority. This also underscored the greatest increase in cybersecurity prioritization compared to 2024 as they catch up with other countries.

Together, these findings point to **mounting regulatory pressure and heightened risk awareness** across both high-risk industries and responsive regions.

MSP CALL TO ACTION

Conduct regular risk assessments to help SMBs anticipate evolving threats, budget strategically, and implement tailored cybersecurity strategies that prevent costly surprises and reduce the need for reactive crisis management.



Section 2

The Challenge

AI's Double-Edged Sword: Innovation vs Vulnerability

AI is reshaping the threat landscape, leaving organizations vulnerable to increasingly sophisticated attacks.

The majority (83%) of respondents say that AI increases the cybersecurity threat level for their organization. Yet, despite these fears, only just over half (51%) of SMBs have put in place specific policies or approaches to mitigate **AI-related security threats**. Positively, 46% do have plans to do so, but the pace of AI evolution means many may struggle to develop and maintain security frameworks.

The use of policies and approaches to defend against AI-based attacks

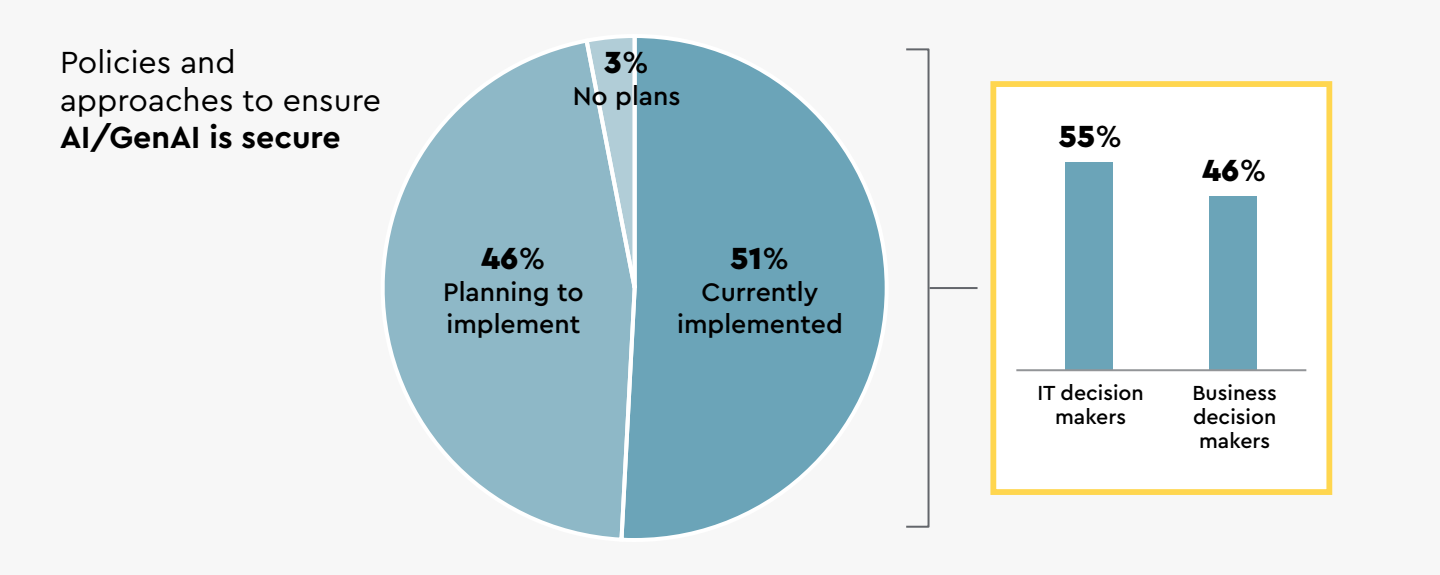


Figure 3: Which of the following does your organization currently have/do, or is planning to implement? Policies and approaches to ensure we are using AI/GenAI securely, showing current implementation split by IT decision makers (ITDMs) and business decision makers (BDMs).

> "The rise of AI threats means malicious actors can automate and enhance cyberattacks and malware changing to avoid detection from current cyber software." *– Business decision maker, Financial services, USA*

> With the advent of AI, I fear it will be more complicated to stop the bad actors from conducting malicious activities in cyberspace."
>
> *– Business decision maker, IT & technology, USA*

Country and sector highlights

- Smaller organizations (10–24 employees) (61%) and the public sector (61%) are the most likely to have implemented AI security.
- Manufacturing and production (42%) and Canadian organizations (46%) are among the least likely to have taken action, suggesting they require greater education and support.

MSP CALL TO ACTION

Deliver tailored solutions and expert guidance to SMBs to combat the growing threat of AI-driven attacks, including regular audits to ensure their AI strategies address emerging risks.

Underprepared and Overexposed: Why Cybersecurity Action Can't Wait

Around three in five organizations (61%) are worried that a successful cybersecurity attack could be enough to put them out of business, leaving them facing serious reputational and financial damage and potentially legal consequences. This stands out among those without cyber insurance (74%), being more vulnerable to disruption and loss. These anxieties appear to be reaching a critical juncture, with almost three-quarters (72%) at a tipping point where cybersecurity concerns demand action.

> "The risk of losing documents and data and downtime to restore services. I think overall the reputation and trust from customers will be greatly impacted." *– IT decision maker, Manufacturing, Canada*

Organizations are concerned about potential breaches involving internal (75%) or customer (76%) data, as well as attacks targeting remote workers (71%). Especially as many organizations admit they remain underprepared: 55% don't feel very well protected against internal data breaches, 53% against customer data leaks, and 60% against threats related to remote work. SMBs are recognizing the need to ensure comprehensive, compliant, and complete protection that leaves no weaknesses for malicious actors to exploit.

> "The fear faced by our organization is bearing financial losses and attacks leading to reputation loss which may lead to future risks in growth."
>
> *– IT decision maker, Information Technology, USA*

Bridging the Gap: Cybersecurity Awareness and Preparedness Disparities Between IT and Business Leaders

IT leaders (91%) express higher concern about the likelihood of a cyberattack in the next six months compared to business decision-makers (75%). It's likely that IT leaders are more aware of elements that can go wrong, often being blamed when they do, while business leaders may not grasp the full extent of their organization's vulnerabilities.

This disconnect could have real consequences. Misalignment between IT and the broader leadership team may lead to slower decision-making and delayed implementation of essential protections, leaving organizations exposed.

Encouragingly, many are taking steps to close this awareness gap. Investments in cybersecurity training (see Section 1) indicate recognition of the need for cross-functional understanding that could lead to a more coordinated response to security threats.

MSP CALL TO ACTION

Host regular cybersecurity updates and AI-specific training to inform clients about emerging threats, AI-driven risks, and best practices for securing AI tools.

By positioning cybersecurity as a business imperative—not merely a cost center—MSPs can strengthen trust, deepen client loyalty, and stand out in an increasingly competitive market.

Cracks in the Foundation: How Reliability Concerns Threaten MSP Trust

To seize the cybersecurity opportunity, MSPs need to overcome reliability concerns and protect their reputation.

MSPs are increasingly recognized for their ability to strengthen security, enhance IT performance, offer specialized expertise, **advise on AI adoption** vs security, and accelerate technological adoption. This partnership is often vital in allowing organizations to access knowledge and capabilities they may not have in-house, helping to navigate a fast-evolving cybersecurity landscape and address critical IT and security challenges.

The benefits of using an MSP (2024 vs 2025)

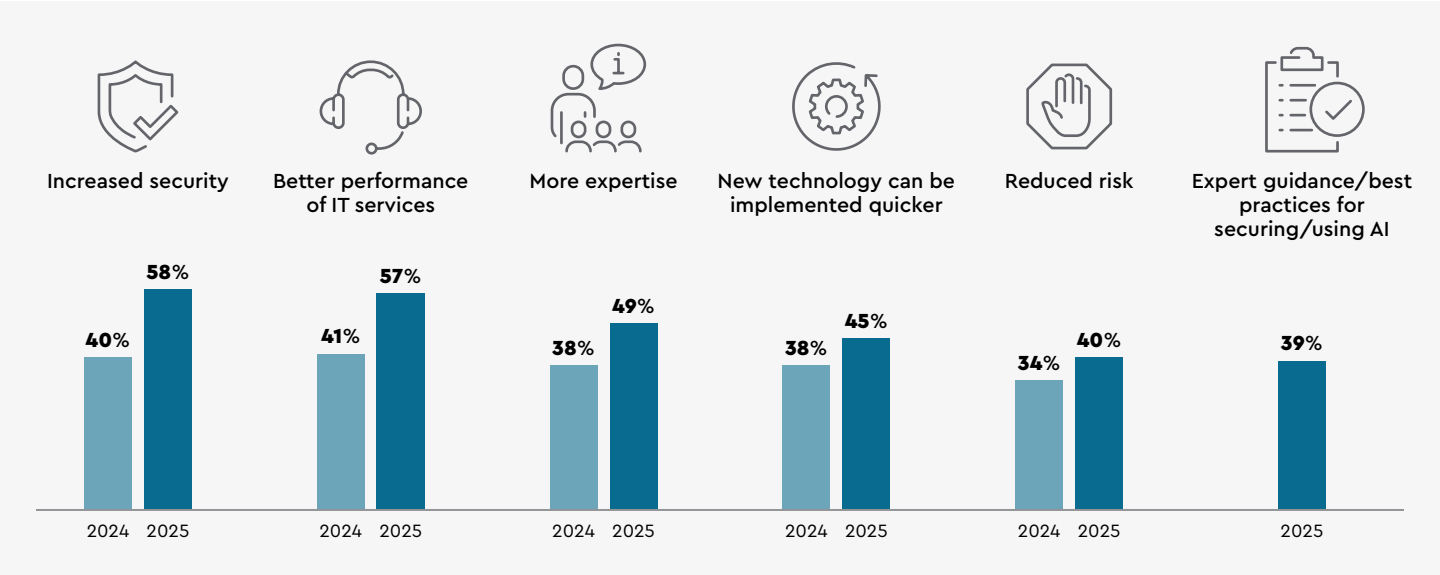


Figure 4: What benefits have you seen/do you expect to see for your organization from using a managed IT service provider? Shown to those whose organizations are using or planning to use a managed IT service provider.

> "The evolving nature of cyberattacks is a huge concern for me because it's hard to keep up with new tactics, and we're always a step behind."
>
> *– Business decision maker, Retail, UK*

While many elements of MSPs have improved in the eyes of SMBs, lingering concerns about reliability remain. Without confidence in an MSP, trust can quickly erode. Over time, these concerns can impact customer satisfaction and loyalty; results suggest this may already be happening. Almost three-quarters (73%) are not confident their MSP would be able to defend their organization effectively in all cases if they were a target of a cybersecurity attack, and nearly half (47%) would definitely consider using or moving to a new MSP if offered the "right" cybersecurity solution.

The challenges of using an MSP (2024 vs 2025)

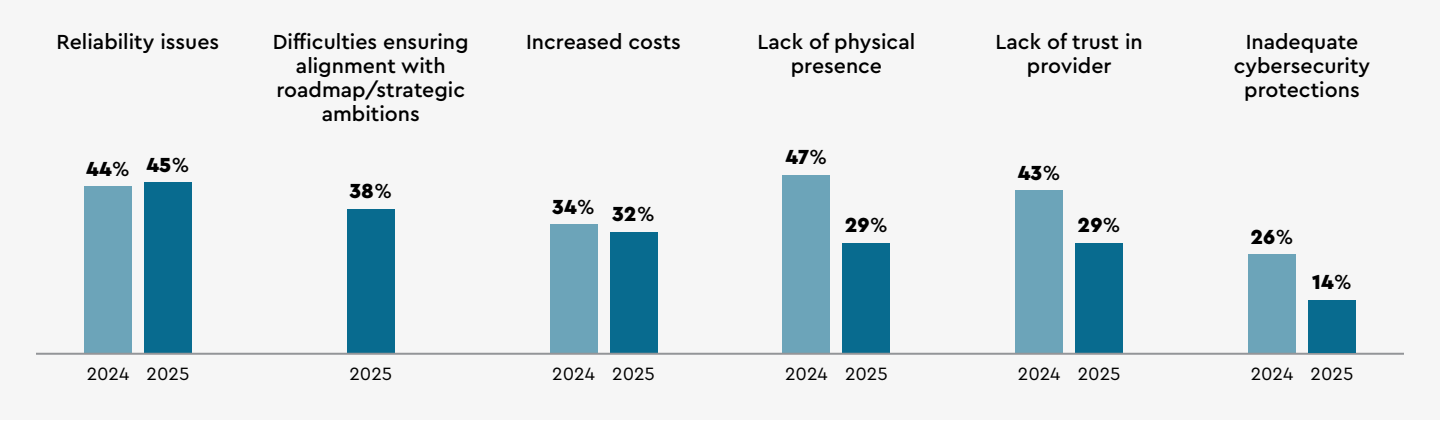


Figure 5: What challenges have you seen/do you expect to see for your organization from using a managed IT service provider? –Shown to those whose organization is using or planning to use a managed IT solution provider.

Most important factors for an SMB to decide if a provider has the "right" solution

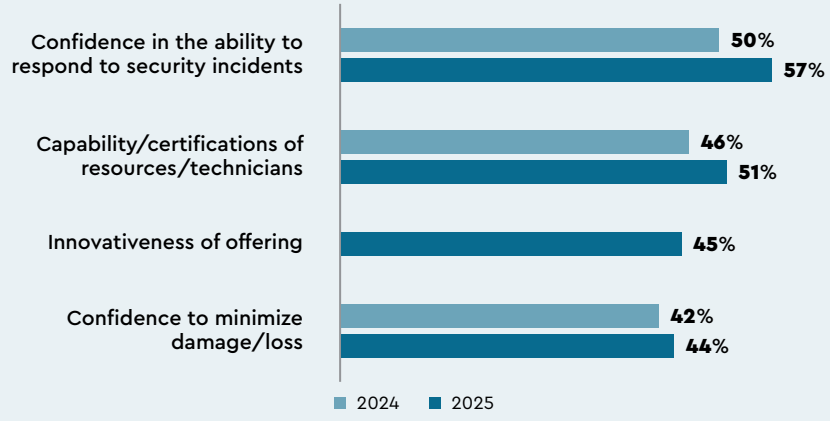


Figure 6: What are the most important factors that would help you decide if a provider had the "right" cybersecurity solution for your organization? (Note: innovativeness of offering was a new answer option for 2025.)

When evaluating MSP's cybersecurity solutions, SMBs are guided by several criteria:

- Overall confidence in the provider
- Skills and expertise of the MSP's staff
- Innovativeness of offerings
- Ability to minimize damage from a cyberattack

MSPs can showcase AI innovation and skills in their solutions and staff, particularly as SMBs become more aware of the dual nature of AI as both a source of cybersecurity threats and an enabler of stronger defenses. By proactively sharing their cybersecurity roadmap, MSPs may help grow confidence among SMBs, strengthening their partnerships and supporting long-term revenue growth for both parties.

Accountability is high: almost a third (32%) would hold their MSP solely responsible in the event of a cyberattack, with many (79%) open to pursuing legal action. **Against a backdrop of persistent reliability concerns, this underlines the serious consequences MSPs could face if they fail to meet expectations, both in terms of revenue and legal repercussions.**

MSP CALL TO ACTION

MSPs can take proactive steps to strengthen trust and reliability perceptions. This includes increasing the robustness of their solutions, upskilling staff, and providing evidence of their reliability through transparent reporting, certifications, and client success stories.

MSPs need to stay ahead of evolving threats, not just to sidestep legal consequences but to protect their reputation and customer base in a competitive landscape.

The MSP Opportunity: How ConnectWise Can Help

To meet rising client expectations, seize new market opportunities, and lead in a rapidly evolving threat landscape, MSPs must take bold, strategic action—starting with these three critical focus areas.

1. **Capitalize on Growth Areas: AI Security, Advanced Protection, and Awareness Training**

As SMBs face an increasingly complex threat landscape, demand is rising for MSPs who can deliver expertise in three critical areas:

- **AI Security Expertise and Advice:** SMBs are looking for guidance on how to safely deploy, monitor, and defend AI-driven systems. ConnectWise provides access to the tools, frameworks, and educational resources MSPs need to position themselves as trusted AI security advisors.
- **Advanced Network and Endpoint Protection:** With cybercriminals exploiting every available weakness, SMBs demand comprehensive, real-time protection. ConnectWise empowers MSPs with **advanced network monitoring**, MDR (with the EDR of your choice), and threat prevention technologies that help eliminate vulnerabilities before they are exploited.
- **Security Awareness and Training:** Human error remains one of the leading causes of breaches. ConnectWise partners can join the **ConnectWise Partner Program**, which includes white-labeled resources, assets, and campaigns for cybersecurity customer education and solution selling.

By addressing these growth areas, MSPs can meet evolving client expectations and create powerful new revenue opportunities.

2. **Enhance Your Cybersecurity Offerings with AI-Driven Innovation**

AI isn't just a threat; it's a powerful ally in defense. MSPs can integrate AI-driven cybersecurity solutions that detect and respond to threats faster and smarter than human teams alone.

ConnectWise is leading the way with AI-enhanced capabilities across our cybersecurity suite, helping MSPs:

- Accelerate threat detection and incident response
- Predict vulnerabilities and prioritize risk mitigation
- Automate repetitive security tasks, freeing teams to focus on strategic initiatives

AI-driven intelligence is infused in many solutions, including **ConnectWise SIEM** and **MDR** (with the EDR of your choice), MSPs can deliver the advanced protection SMBs expect while improving operational efficiency and scaling their cybersecurity practices.

3. **Prove Your Reliability—Every Day**

Trust is everything in today's cybersecurity market. The research shows that concerns about MSP reliability remain high and client loyalty is increasingly conditional.

ConnectWise helps MSPs build and demonstrate trustworthiness through:

- **Transparent Reporting:** Detailed, real-time reporting and visibility are available with the **Security Dashboard** and the **Backup Dashboard**. These unique tools help show clear evidence of cybersecurity performance and protection effectiveness.
- **Industry Certifications and Best Practices:** ConnectWise solutions and services align with major global **cybersecurity frameworks** and compliance standards, allowing MSPs to showcase adherence to best practices.
- **Continuous Upskilling:** **IT Nation Secure™** is an annual cybersecurity conference specifically for MSPs. Industry leaders, MSP peers, and other subject matter experts discuss security challenges and solutions, network, and get hands-on solution experience.

Providing clear proof of reliability and performance can help MSPs strengthen client relationships, reduce churn, and build a reputation that attracts new opportunities.

The Future Belongs to the Cybersecurity Leaders

Cybersecurity is no longer optional—it is foundational to business success for SMBs and MSPs. ConnectWise is committed to equipping MSPs with the solutions, expertise, and support needed to lead in this new era. Together, we can help SMBs protect and grow their businesses.

Equip your team with the tools, training, and support to deliver unmatched cybersecurity outcomes for your clients and position your business as a leader in the next era of managed services. Connect with a cybersecurity expert today to explore how ConnectWise can power your cybersecurity and growth strategy. **Book a Demo >>**

Cybersecurity and Data Protection

The ConnectWise cybersecurity collection of solutions includes software and support services that enable MSPs to protect their client's critical assets. With tools for 24/7 threat detection monitoring, incident response, and security risk assessment, the solution removes the complexity of building an MSP-powered cybersecurity stack while lowering the costs of support staff.

The ConnectWise Data Protection collection of solutions empowers MSPs with comprehensive business continuity and disaster recovery (BCDR) tools for servers, workstations, and the cloud. The solutions are designed to help MSPs build business profitability while protecting their clients with reliable, affordable technology. **Learn more >>**

ConnectWise Partner Program™

Our Partner Program assists ConnectWise partners with growth acceleration, including strategic planning, lead generation, and sales. A cybersecurity-specific track is available to give our partners more tools and support for driving revenue around their cybersecurity offerings. **Learn more >>**

Methodology

ConnectWise commissioned independent market research specialist Vanson Bourne to undertake the research upon which this whitepaper is based. A total of 700 IT decision makers (ITDMs) and business decision makers (BDMs) were interviewed in March 2025, with representation in the following countries: US (300); Canada (100); UK (150); Australia and New Zealand (150).

Respondents were from organizations with between 10 and 1,000 employees and from a range of private and public sectors.

The interviews were conducted online and were undertaken using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated, the results discussed are based on the total sample.

Throughout the report we reference data from previous waves of the research, which was with a similar audience and make up to the 2025 study, carried out in 2024, 2022, 2021, 2020, and 2019.

About ConnectWise®

CONNECTWISE

ConnectWise is the leading software company empowering managed service providers (MSPs) with the technology that runs small and midsized businesses (SMBs) worldwide. With over 40 years of commitment to partner success, ConnectWise delivers innovative software, services, and an open ecosystem of integrations that drive growth. The ConnectWise Asio™ platform offers unmatched scale and AI-backed automation to provide a comprehensive technology stack for MSPs, including PSA, RMM, cybersecurity, and data protection. Discover how ConnectWise is transforming the IT industry at **connectwise.com**.

About Vanson Bourne

VansonBourne

Vanson Bourne is an independent specialist in market research for 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 **www.vansonbourne.com**