CONNECTWISE

CONNECTWISE EBOOK SERIES

The State of SMB CYBERSECURITY *in 2024*

The Opportunity of Powerful MSP Partnerships

VansonBourne

Vanson Bourne Research
Commissioned by ConnectWise

Contents

Foreword by ConnectWise **3**

Introduction **4**

Key Findings **5**

Cybersecurity: The Heart of Business **6**

Adapting to Changing Priorities: Embracing Technology and Strengthening Cybersecurity 6

Cybersecurity plans vs the reality of implementation 7

Impact amplified: the growing toll of cyber incidents 8

The Progressive Reliance on MSP Partnerships 10

The Power of Partnership: Optimizing the MSP-Organization Relationship **12**

Navigating Loyalty: The Importance of Continuous Value in MSP Partnerships 12

Pivoting to a Solution-Orientated Cybersecurity Approach 14

ConnectWise Call to Arms **16**

Methodology **17**

Foreword by ConnectWise

The Cybersecurity Opportunity for MSPs

It's common to hear about large cybersecurity attacks in mainstream news, and governments and institutions are stepping in to create frameworks and regulations to help. This work trickles down to help everyone, but creating policies versus having boots on the ground for protection and remediation are two different things.

As a managed service provider (MSP), you're the boots on the ground for small and midsized businesses (SMBs). The trends and research are clear: SMBs are asking for your help more than ever.

As attacks on SMBs increase and the landscape becomes more complicated, they are losing confidence in their in-house ability to defend their businesses and livelihoods. About 78% report that they are worried that a serious attack could put them out of business.

As a result, their collective mindset is trending toward an educated and proactive approach. They are:

- Keeping cybersecurity at the forefront of their plans, on par with improving technology and growth
- Increasing their use of MSPs as they increase their investments in cybersecurity
- Looking for the "right," solution-oriented MSP rather than keeping loyalties to current providers

This creates a huge opportunity for MSPs. However, as SMBs become more worried and are experiencing risks and consequences, they are not settling for "good enough" or the status quo. *SMBs are counting on their provider to be the expert who can navigate the ever-changing cybersecurity landscape.*

A rising trend that will be important for MSPs to differentiate their cybersecurity offerings is the ability to *create personal relationships with their customers*. SMBs report that they are willing to switch providers and pay for the right solutions and relationships with a 47% increase in spending (up from 30% in 2020).

Those that can provide best-in-class technology with education, risk assessment support, effective endpoint and network protection, and a focus on relationships will be very well-placed to address SMB needs now and in the future.

Introduction

SMBs are navigating the complex interplay between advancing technology, emerging cybersecurity risks, and strategic responses to these demands. Businesses need to recalibrate their approaches to cybersecurity, not just as a defensive measure but as a proactive part of their overall business operations. This shift underscores the growing recognition of cybersecurity's impact on every aspect of organizational health, from safeguarding data and maintaining customer trust to facilitating innovation and driving competitive advantage.

MSPs themselves must continuously evolve to meet the demands of their clients in this high-stakes field. The changing business landscape demands a proactive and solution-oriented approach from MSPs to meet the rising cybersecurity challenges. However, there is a balance to strike between offering cutting-edge technological solutions and fostering personal relationships that build trust and loyalty with their clients. Organizations are keen on partnerships that promise post-incident, reactive measures *and* proactive threat anticipation and mitigation. They want relationships that exhibit trust and confidence. This research emphasizes the importance of these dynamics in fostering long-term and resilient partnerships that enhance organizational security postures.

This introduction sets the stage for a detailed examination of the interplay between technological advancements, cybersecurity challenges, and the critical role of MSPs in supporting organizational resilience against a backdrop of increasing cyberthreats.

Key Findings

Cybersecurity remains at the heart of organizations, ensuring that organizations can defend against an increasing threat landscape. Organizations are progressively more reliant on MSP partnerships; their usage being a key factor in an organization's defensive capabilities.

- **90%** report that cybersecurity is critical or very important to their business, therefore it's no surprise that protecting against cybersecurity attacks is ranked in the top three priorities for organizations in the next two years (35%)
- **94%** have suffered from at least one cybersecurity attack in the past (up from 64% in 2019); translating into high levels of worry about further attacks; 89% have concerns over being a target of an attack in the next 6 months
- **76%** agree that their organization lacks the skills in-house to be able to properly deal with cybersecurity issues
- Over 8 in 10 (**83%**) organizations are planning to invest more in cybersecurity in the next 12 months, with an average budget increase of 19%
- An increased **94%** of organizations are using an MSP, compared to 89% in 2022 and three quarters (74%) in 2020
- **More than half** of SMBs are outsourcing all or a majority of their IT infrastructure (59%), IT services (59%) and IT cybersecurity (57%)

Increasingly, the relationship between the service provider and the SMB is tenuous and reliant on the MSP being able to provide solution-orientated services alongside a personal connection to forge long-term and successful partnerships.

- **62%** reporting they would *definitely* consider changing providers if they offered the "right solutions," compared to 40% in 2020
- For half (**50%**), the "right" solution is having confidence in the MSP's ability to respond to security incidents, which organizations are willing to pay an average of 47% more for the "right" cybersecurity solution at a new IT provider
- An MSP demonstrating a solution-orientated focus is appealing to **47%** of organizations, increasing from 38% in 2022, with over third (36%) valuing the personal touch (empathy and bonding)
- MSP proactivity when speaking to organizations about their cybersecurity only occurs in **49%** of cases, therefore if MSPs prioritize this, this will further foster the feelings of trust, engagement and partnership that SMBs are craving

Chapter 1

Cybersecurity: The Heart of Business

Adapting to Changing Priorities: Embracing Technology and Strengthening Cybersecurity

In the fast and evolving technical landscape of 2024, organizations have a host of priorities to juggle as resources are squeezed, budgets tightened, and outgoing costs spiral. Not only surviving, but thriving, in this tumultuous landscape is a challenge that all organizations are facing, and many are recalibrating their strategies to prioritize advancements and fortify their defenses.

First and foremost, improving technology is seen as the biggest priority areas for organizations in the coming two years, being placed as the top priority by 38% of interviewed IT and business decision makers. Organizations are looking to the opportunities presented by technological advancements to make headway with operational efficiency, to elevate customer experience and drive innovation. Investment in emerging technologies, such as artificial intelligence (AI) and generative artificial intelligence (GenAI) is one area in which many organizations (32%) are targeting and is key to remain at the forefront, ensuring they aren't left behind with the latest technical developments and trends.

Despite other competing priorities, cybersecurity is not being overlooked, and it remains at the heart of what organizations are focusing on—with 35% reporting that protecting against cyberattacks is a top priority. A vast number of other priority areas would be impacted if cybersecurity was not front and center within an organization's strategy and planning. For example, technological improvements can't be successful if the new technology and systems aren't adequately protected against cyberthreats and attacks. Similarly, customer retention and satisfaction would be severely affected if there is a breach or inadequate security. Organizations recognize this importance with a large majority (89%) agreeing that cybersecurity should encompass all aspects of the organization, demonstrating understanding that all facets of their operations are ultimately impacted by, and must therefore consider, cybersecurity.

90%

*say that **cybersecurity** is **very important** or **critical** to their organization*

83%

*are planning to **invest more**, or much more, in their **cybersecurity** in the next 12 months*

19%

*is the **average budget increase** compared to last year*

vs. 14% increase in 2022

Figure 1: Which of the following statements most closely reflects your organization's stance on cybersecurity? [700] / Which of the following statements best describes your organization's level of investment in cybersecurity for the next 12 months? [700] / What change, if any, has your organization made to its cybersecurity budget for this year compared to last year? [700]

And this is further reflected by nine in ten reporting that cybersecurity is either critical or very important to their business. Organizations are exhibiting their priority in cybersecurity by increasing their investments, not only in the last year already but also over the course of the next 12 months, with the average increase in budget at 19% more than in 2023. It's great to see this level of investment and priority, but organizations need to be sure that they are investing in the right areas and against the right threats to ensure that their protection is as advanced as it can be. For some, this may be a straightforward task, but for many the challenge this poses may mean that outside advice and guidance is sought from MSPs.

Cybersecurity plans vs the reality of implementation

As is expected in 2024, organizations have many cybersecurity measures in place, across a broad range of areas, from compliance security policies (46%), incidence response planning (45%) and security awareness training and education (44%).

Some of these have been prioritized more greatly in implementation since 2022, with cybersecurity insurance seeing a 47% increase in uptake. The increased threat landscape means that over three-quarters (78%) have concerns that a serious cybersecurity attack could be enough to put their organization out of business. This, in combination with financial implications, regulatory pressures, and the maturation of the cyber insurance market, are all likely driving increased uptake in insurance among organizations seeking to enhance their cyber resilience and protection levels.

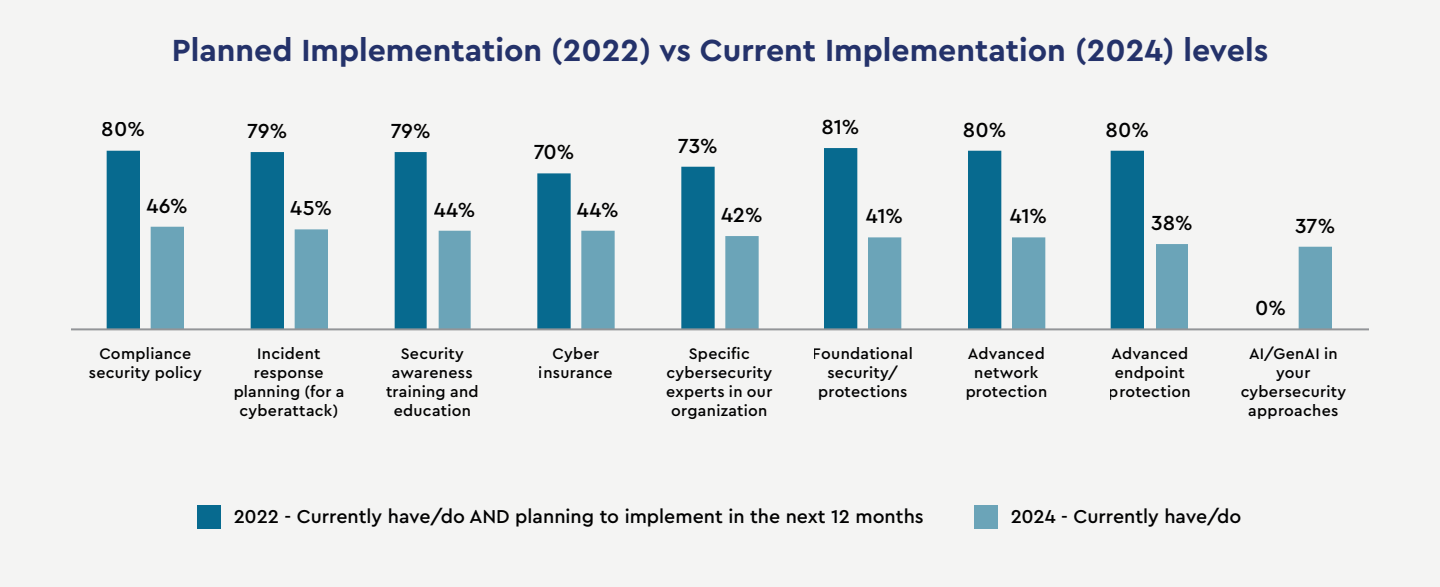

Figure 2: Which of the following does your organization currently have/do, or is planning to implement? [700] Split by historical data

Cyber insurance being the largest area in increased implementation is a recognition of the increased threat landscape, however there is a risk of over-reliance on insurance, therefore it is a careful balance for organizations to strike. While cyber insurance can provide valuable financial protection, it should not serve as a substitute for robust cybersecurity measures. Organizations have to also consider the coverage limitations and exclusions of insurance which may lead to unexpected financial losses in the event of an attack. This can also lead to higher premiums or difficulty obtaining coverage in the future, which is a real fear for 81% who report they are worried that a future attack would have a concerning impact on their cyber insurance costs and coverage. Therefore, cyber insurance must be viewed as a complementary tool in a broader risk mitigation strategy, alongside proactive measures, to provide a holistic cybersecurity approach.

In the realm of cybersecurity, organizations often craft one-, two- or five-year plans as part of their strategy and business evolution—yet the stark reality reveals a misalignment between these well-intentioned plans and their practical implementation. Despite the plethora of measures in place, organizations find themselves grappling with implementation to the timings they set. In 2022, many organizations believed that their implementation levels of these measures would be much higher just 12 months later, but the reality is that this has not come to fruition. Whether other priorities have taken precedence, measures have taken longer to implement, or perhaps their plans were not grounded in reality (through resource availability or company support), it is evident that organizations need to ensure that their implementation plans are robust. Addressing the root cause of implementation challenges is key, and working alongside an MSP could help to manage an implementation schedule or alleviate any challenges which are slowing progress.

The great news is that investment in cybersecurity is increasing, and therefore these planned implementations should have a good backing to be achieved in the timelines anticipated. Influencing organizations' decisions to increase their investments come from previously experiencing a cybersecurity issue (39%), it being a requirement of their cyber insurance (38%), and pressure from the board (37%). These are likely interlinked, with past incidents raising board scrutiny of security measures, and will serve as catalysts for organizations to forge ahead with planned changes to strengthen their defenses.

Impact amplified: the growing toll of cyber incidents

There is a notable increase in cybersecurity attacks in recent years, which means it is almost a certainty that organizations will experience one. Over half (56%) have experienced at least one in 2024 already, demonstrating the very real threat that organizations are facing every day, so much so that it can now be considered commonplace.

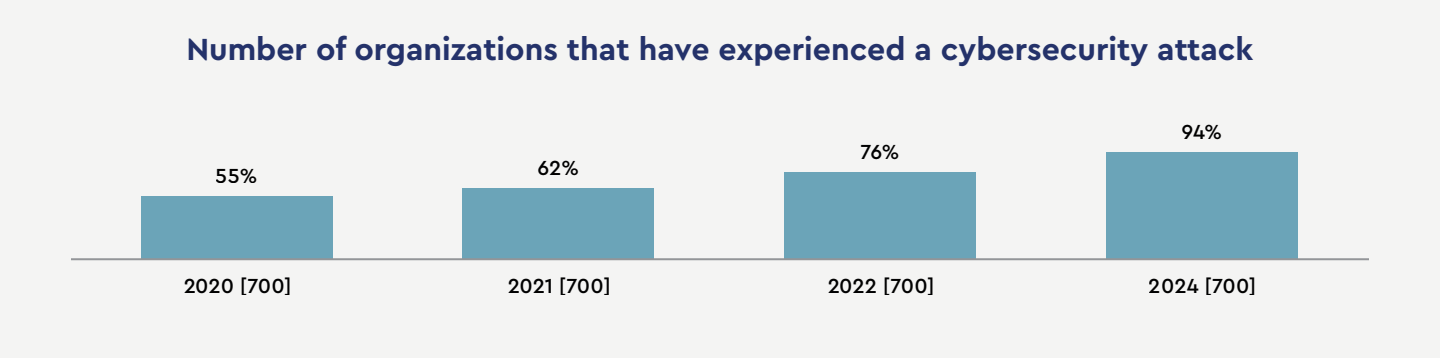

Figure 3: Has your organization suffered a cybersecurity attack? [base sizes in chart] Split by historical data

This attack threat translates into high levels of worry among IT and business decision makers, with further attacks likely on the horizon. The next six months are a critical time period, with 89% worried that they will experience an attack in this time—an all-time high having increased from 77% in 2020. Top areas of concern include remote devices and employees being breached (83%), the increased costs of attacks (82%) and legal ramifications (82%). Perhaps the concern is due to the acknowledgement that many areas of their defense require bolstering as we have already explored, however it's clear that organizations feel there are numerous areas in which their security is lacking. Organizations are therefore very likely to have high expectations of MSPs and their capabilities to support and alleviate concern in these areas of worry.

But it appears that these concerns are warranted, with 99.5% stating their organization has experienced impacts as a result of a cybersecurity attack. The cost (time and effort) of dealing with the issue is faced most often in 2024 (38%), however seeing increasing frequency is experiencing damage to company reputation (a 64% increase since 2019), employees losing their jobs (106% increase) and needing to change their MSP (46% increase). The critical nature of these impacts leaves organizations vulnerable to financial losses, logistical challenges and the erosion of customer and employee confidence. The need to address these impacts highlights the vital importance for organizations to not only invest in robust cybersecurity measures, but also to maintain strong and reliable relationships with their MSPs.

The good news is that those that work with MSPs report slightly lower impacts in terms of company reputation damage, monetary costs of dealing with the attack and negative publicity, than those that do not use an MSP. With 76% agreeing that their organization lacks the skills in-house to be able to properly deal with security issues, it ensures that the role of the MSP is more critical than ever. Support and guidance are vital for organizations when facing threats, and though working with an MSP does not reduce the chances of experiencing cyberattacks, it is likely that the success of the attack or impacts experienced will be reduced through this partnership.

The Progressive Reliance on MSP Partnerships

Amid the challenging cyber environment, MSPs are becoming an increasingly vital lifeline for organizations striving to boost their IT resources and cyberdefense capabilities. Organizations are increasingly relying on MSP partnerships to manage and enhance their cybersecurity efforts, and more seemingly satisfied with the service they are receiving and therefore intending to remain with their current provider.

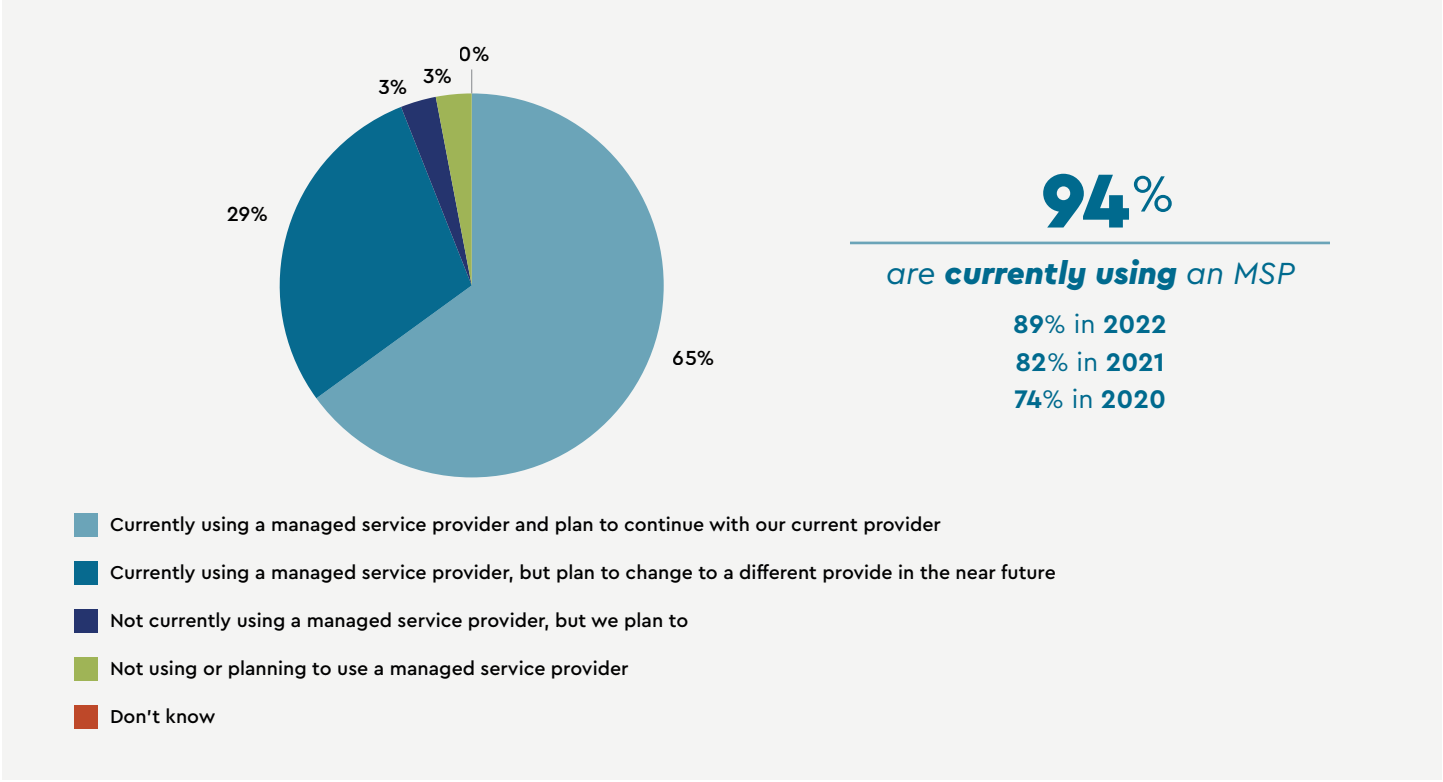

Figure 4: Is your organization using a managed IT service provider? [700] Split by historical data

This level of MSP usage has increased since 2020, and indicates that many who previously were planning to change provider have done so and are likely in the early stages of cultivating newly formed partnerships. And it's clear to see why so many find the MSP partnership so successful. Having better performing IT services (41%), increased security (40%) and being able to implement new technology quicker (38%) are just some of the benefits reported; the latter particularly important for those that are looking to prioritize technological improvements in their 2024 strategy and beyond.

Organizations are also increasingly outsourcing all or a majority of their IT in 2024, in infrastructure (59%), services (59%) and cybersecurity (57%). These levels are set to remain over the next five years, indicating that MSPs are becoming further embedded into the everyday running of organizations' operations and security. This demonstrates the importance of deepening the relationships between MSPs and organizations. With outsourcing remaining steadfast, there is potential for long-term associations to be built and for MSPs to become integral to the functioning of the organizations they work with.

However, this isn't to say that these relationships aren't without challenge. Increasingly, the lack of physical presence is of concern to organizations that work with an MSP (47%), and particularly for organizations of a smaller size (reported by 54%). With almost three in ten organizations looking to change supplier in the near future, and many having done so in the past two years, it seems that there is difficulty in establishing strong and personal relationships. Without regular face-to-face interactions, it can be harder to build trust—demonstrated by 43% also reporting that a lack of trust in their provider is a challenge they face. This disconnect may lead to misaligned priorities and expectations, potentially affecting the quality and responsiveness of the services provided. Additionally, the absence of an onsite presence can complicate the immediate response and resolution to a cyber incident. With the increasing number of cyberthreats and attacks that organizations are exposed to, they are likely to seek immediate and intensive support from their MSP, and with this help not being onsite, this could increase a feeling of stress and pressure on their security.

Figure 5: In the event of a cyberattack, would your organization take legal action against your IT service provider? [676] Asked to respondents whose organization is using a managed IT service provider

Increasingly, organizations believe that their provider would be held accountable in the event of a cyberattack. Over two in five (42%) organizations believe their provider would be accountable, and 95% would likely take legal action against them (up from 61% in 2020). This demonstrates the fragility of the MSP-organization relationship at this current time, and these fine nuances mean that a partnership could easily change should a cyberattack prove successful.

Though commitment to their current providers is relatively high, organizations do remain open to changing providers should the "right" solutions be available elsewhere, which we explore later in this research. Therefore MSPs must remain abreast of organizations' needs and priority areas as best as possible, in order to anticipate and adapt to their customers' needs, providing the right levels of security, before they feel the need to move their business elsewhere.

Chapter 2

The Power of Partnership: Optimizing the MSP-Organization Relationship

Navigating Loyalty: The Importance of Continuous Value in MSP Partnerships

The increasing exposure to major cybersecurity incidents means that organizations are now, more than ever, aware that the MSP they work with has to be offering the right solutions for them. And this hinges on the continuous delivery of value and assured cybersecurity. In the past, less than half of organizations reported that they would change providers should the "right" solutions be offered elsewhere. This has now increased to almost two-thirds (62%) willing to make this change in 2024; even by organizations that reported they plan to stay with their current MSP.

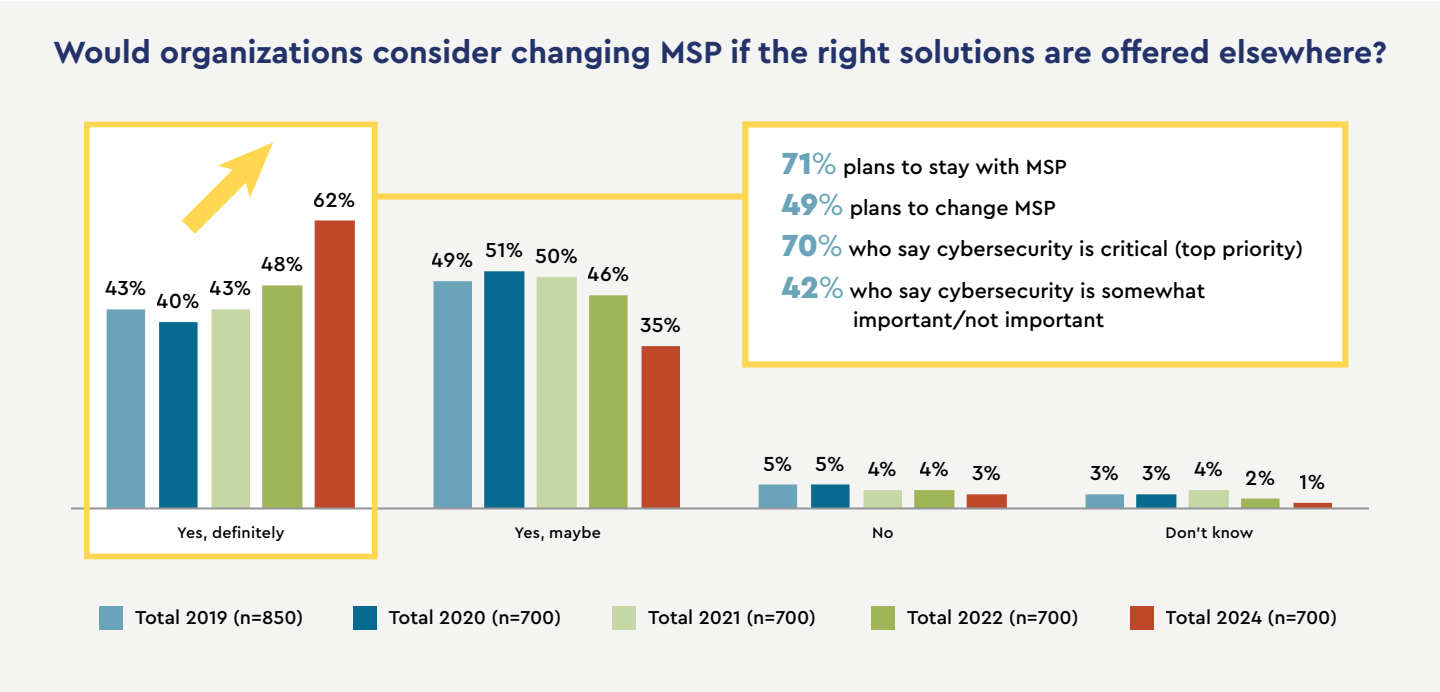

Figure 6: Would your organization consider using/moving to a new IT service provider if they offered the "right" cybersecurity solution? [base sizes in chart]. Split by historical data, usage of MSP and view on cybersecurity's importance to their organization

This is driven by an overwhelming need for assured cybersecurity, demonstrated by 70% of those who say cybersecurity is critical (a top priority) agreeing they would definitely change supplier. While initial engagement with an MSP may be driven by the promise of enhanced security and operation efficiency, sustaining this partnership requires an ongoing commitment to meeting and exceeding the organization's evolving needs. Loyalty, in this context, is not guaranteed; it must be earned through consistent performance and adaptability.

One of the decisive aspects of maintaining loyalty in an MSP partnership is the ability to demonstrate value continuously. This involves not only addressing current cybersecurity challenges but also anticipating future threats and proactively adapting strategies to mitigate them. Only a third (37%) of IT and business decision-makers surveyed reported confidence in *all cases* that their MSP or organization would be able to defend during an attack without any impact to the business. Similarly, less than half of respondents felt very well protected across numerous circumstances that could occur during a cybersecurity attack—such as cyber insurance or legal ramifications, and internal or customer data being breached (as depicted on the chart below). Even though working with an MSP does bolster confidence in the perception of impacts experienced when compared to organizations without any external support, this highlights that there is some way to go for MSPs to demonstrate their ability to protect organizations in the event of an attack.

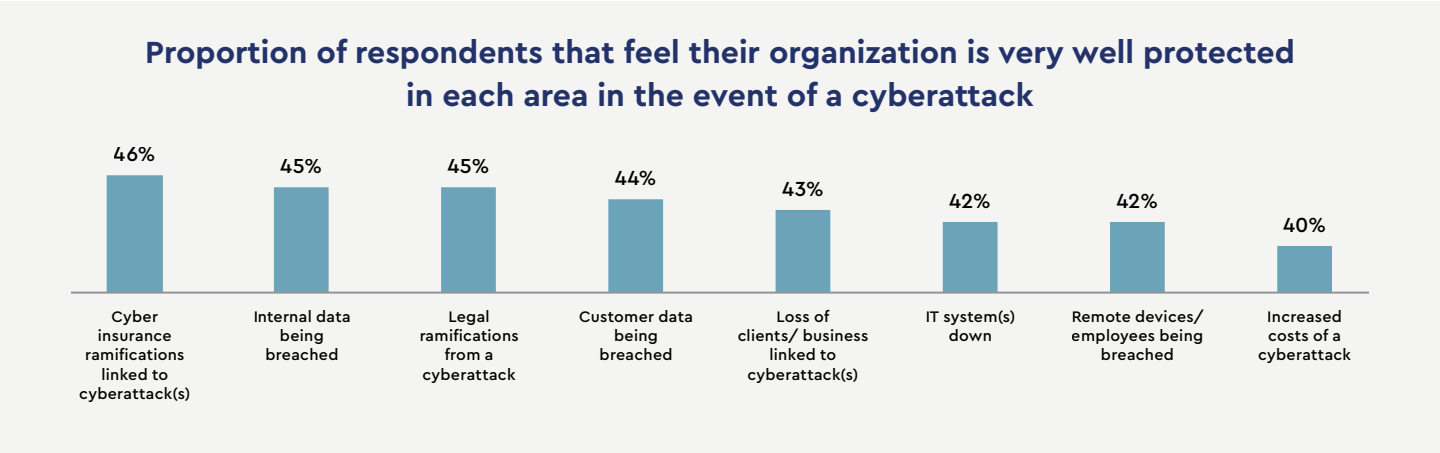

Figure 7: How well protected do you feel the following are in your organization against cybersecurity attacks? [700] Showing the proportion of respondents that feel that their organization is "Very well protected" against the above if they were to experience a cybersecurity attack.

Communication provides a pivotal role in this dynamic. Clear, transparent, and frequent communication helps build trust and ensures that both parties are aligned in their objectives. By creating a bespoke approach tailored to the goals of their clients, the perceived value of the partnership can only be increased, making it less likely that an organization will seek alternatives.

And it is not only in the event of an attack that MSPs should be prepared to have conversations surrounding cybersecurity with the organizations they work with. In just under half of cases (49%) it is the MSP that brings this up on their own, and whilst this is positive, it is certainly something that MSPs could be more proactive about. Waiting until a quarterly or annual review could mean that an opportunity is missed to tackle a vulnerability or prevent a breach, and would leave an organization feeling as though their protection level isn't sufficient. As we have already seen, organizations are struggling with the lack of physical presence of an MSP, and therefore the opportunity is there for MSPs to build a deeper and more trusting relationship by raising cybersecurity with organizations themselves. In-person meetings or reviews will further demonstrate to organizations that their security and protection is being thought about by the MSP and will aid in fostering the feeling of engagement, protection, and partnership with their supplier.

With four in five (81%) organizations feeling that they are at a tipping point where their cybersecurity demands action, this time is critical for MSPs. By continuously delivering exceptional value, staying ahead of the curve and maintaining proactive communication, MSPs can create a compelling value proposition that not only retains clients but also strengthens the partnership over time.

Pivoting to a Solution-Orientated Cybersecurity Approach

There are key questions arising from what we have uncovered so far—namely, what is the "right" cybersecurity solution that organizations are seeking, and, what is it that organizations are looking for in a managed service provider? Although the answers to these questions are probably both "many things," there are a few key standouts that MSPs should be aware of in their quest to build upon relationships and provide top-rate services to the organizations they work with. **Firstly, what are the "right" solutions that would help an organization decide if a provider is best suited to them?**

Figure 8: What are the most important factors that would help you decide if a provider had the "right" cybersecurity solution for your organization? [700]

Having **confidence** and **trust** in their MSP to respond to security incidents and to provide what they have said they will is critical, with these both appearing in the top three important factors. As we saw earlier, confidence in MSPs and their own organization's defences is lacking for many, therefore this is a key area that organizations are looking to boost when partnering with a new MSP. Trust also remains key, which although is often built over time, can be demonstrated by delivering over and above with cybersecurity infrastructure and processes as well as support, guidance, and knowledge-sharing.

In the current economic climate, price will certainly remain important to consider for many organizations, though with it appearing lower down the list in terms of importance demonstrates that organizations are willing to pay a higher amount to ensure the solutions they are employing are suitable. The price organizations are willing to pay is also much higher than in the past, with organizations willing to pay on average 47% more compared to 30% more in 2020, emphasizing that finding the *right* solution really is key.

Following on from this, it's pertinent to delve into what it is that organizations are looking for in an MSP. In the 2024 landscape, being **solution-focused** and **directly relating their offerings** to an organization are key attributes for IT MSPs to display. Solution-oriented MSPs don't just respond to incidents as they occur; they anticipate potential threats and implement preventative measures, demonstrating a proactive stance to cybersecurity. With staying ahead of cyberthreats ever more important as pressures only continue to rise for organizations, a solution-based approach enables a scalable and flexible approach allowing organizations to flourish without compromising security. MSPs should also target their offerings to a business in a tailored and bespoke way, with pragmatic conversations focused on what their recommendations are. These conversations will help to foster positive feelings of change, build relationships, and movement towards a common goal.

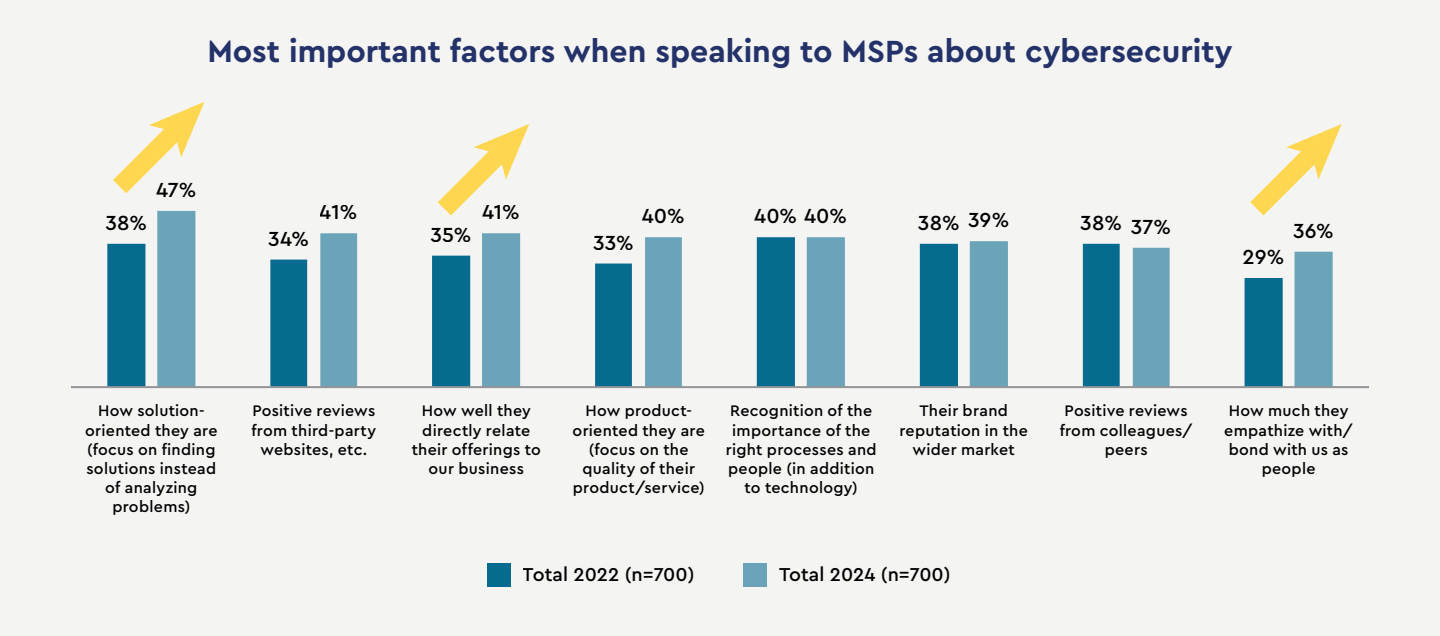

Figure 9: Even if you do not currently use one, when speaking to a MSP about cybersecurity, which of the following would be most important to you? [base sizes in chart] Split by historical data

With pragmatism and a solution-focused approach, there is one further area that MSPs cannot leave behind. Although empathizing and bonding with organizations as people is not the most prominent factor when it comes to speaking with their MSPs about cybersecurity, it is still of great value with it having increased by 24% since 2022. While the technical prowess of an MSP is paramount, the human element cannot be overlooked, with trust and empathy being the cornerstone of successful partnerships. As we have seen throughout this research, confidence, trust, and a feeling of protection are vital in this MSP-organization partnership and organizations need to feel that their assets are safeguarded, and that their needs and concerns are genuinely understood and prioritized.

If MSPs can prioritize this feeling of true partnership, with enhanced and clear communication, and responsive support, it is the gateway to building long-lasting relationships. To pivot successfully to a solution-oriented approach, MSPs must strike a balance between technical excellence and empathetic client engagement. Some strategies to achieve this balance include:

- **Client-centric planning:** Developing strategies that not only address technical needs but also the client's business objectives and values
- **Regular check-ins:** Scheduling regular meetings with clients to review their security posture and discuss concerns and updates on developments. These touchpoints are opportunities to reinforce the personal connection and demonstrate ongoing commitment, and will mitigate against any feelings of lacking physical presence, or lack of engagement from their provider
- **The bespoke approach:** Providing clients with customized reports directly related to the offerings of their business will help clients appreciate the value of the services provided and enable MSPs to become embedded in their client's team

ConnectWise Call to Arms

Two findings stood out to us as guiding lights for MSPs this year:

1) SMBs will pay providers more for cybersecurity solutions that are better than what they have now, and **2)** they are demanding stronger relationships with their providers. For SMBs, it's not always about spending as little as possible; it's about spending smartly and feeling protected and secure. It's an interesting combination of business sense and emotional peace of mind. Finding the right balance between the two is where you'll have the greatest opportunity.

Creating the right cybersecurity tech stack solutions for your business will help you build the right cybersecurity offerings for your customers. ConnectWise is committed to building true partnerships with our partners and innovative solutions that keep pace with the pivots and changes MSPs must make in an ever-changing threat landscape. We purpose-build our software solutions so they can be tailored to your needs, whether you have in-house cybersecurity experts for implementation or need expert services to assist with planning and execution.

Remove the complexity of building an MSP-powered cybersecurity stack and lower the costs of 24/7 monitoring support staff. Whether starting from scratch or expanding services to an existing cybersecurity practice, ConnectWise solutions are purpose-built to launch quickly and deliver outstanding customer outcomes.

ConnectWise Cybersecurity and Data Protection

Our collection of solutions offers software, support services, community, and integrations that enable IT solution providers to launch and grow a profitable cybersecurity practice. It includes propriety threat research and 24/7/365 monitoring and response tools that address complexity, costs, time-to-value, and other considerations when starting, building, and maintaining a successful cybersecurity practice. **Learn more >>**

ConnectWise MDR™

Discover a complete endpoint detection and response (EDR) with 24/7 support from the ConnectWise SOC. This enterprise-level solution is an affordable way to detect and contain threats to your customers' critical business assets. **Learn more >>**

ConnectWise SIEM™

Break down cybersecurity data silos for business-wide visibility, real-time threat detection, and simplified compliance reporting. Your team has the autonomy and control to manage workflows, drive decisions, and take action. **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 and April 2024, 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 in their country 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 this research, which was with a similar audience and make up to this research, carried out in 2022, 2021, 2020 and 2019. The differences in the markets interviewed in may have factored into any differences in the statistics from this year, and further details are available upon request.

About ConnectWise

CONNECTWISE

ConnectWise is the world's leading software company dedicated to the success of IT solution providers (TSPs) that support millions of small and midsized businesses (SMBs) globally. With over 40 years of commitment to partner success, ConnectWise provides unmatched software, services, community, and integrations to fuel profitable growth. ConnectWise introduced the world's first true TSP platform—Asio™—providing unprecedented flexibility and security with built-in artificial intelligence, robotic process automation, and machine learning capabilities. It all adds up to efficient, productive end-to-end solutions, including IT documentation, data management, cybersecurity, remote monitoring, and backup technologies. 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**