CONNECTWISE

CONNECTWISE EBOOK SERIES

The State of SMB Cybersecurity in 2022

THE MSP OPPORTUNITY AMID THE QUEST FOR CONTINUOUS IMPROVEMENT

CONTENTS

CHAPTER 1: FOREWORD

By Raffael Marty, EVP and General Manager, Cybersecurity

Cybersecurity is a growing concern for businesses of all sizes. While small-to-medium businesses (SMBs) are typically more focused on day-to-day operations and customer service, they have much to lose if their information or networks get breached. Especially with the emergence of ransomware, cyber criminals have found a way to easily monetize their activities and they have succeeded in developing a business model that nicely fits SMBs into their 'ideal customer profile'. While the ransoms might not be as big as when focusing on large organizations, there are many more SMBs to target and it's easier to find the ones that are 'easy' targets. Cyber criminals will generally stay on top of new vulnerabilities and go out, scan for vulnerable systems on the wide-open Internet. It only takes a few unpatched systems for these campaigns to be lucrative, as the needed infrastructure is available for very cheap.

It's not just ransomware that has been causing SMBs headaches, but the criminals need a distributed infrastructure for their other ways of monetizing Internet crimes, such as denial of service attacks, phishing, and spamming. By compromising devices across the Internet, vulnerable systems are added to so-called botnets that are then abused to execute the intended attacks.

While we have seen large ransomware attacks in the last years, governments have been incentivized to step in and start tracking down the criminals, which in turn has shifted the criminals' behavior. Instead of exposing themselves to government action, they are trying to stay below the radar by playing the long game against the SMBs.

As MSPs trying to help protect the SMBs, you don't have an easy job as your targets are not staying still. Commonly MSPs have to deal with at least five drivers of the moving targets that the SMBs are exposed to and they are coming to you for guidance and solutions:

- An emerging and changing **threat landscape**: New vulnerabilities, new exploit methods, new ways to trick people into giving up their information, and new ways that the criminal underground organizes and scales their operations makes it really hard to keep pace and protect company's effectively.
- An evolving **technology landscape**: the pace of innovation and the pace of SMBs adopting new technologies is gaining more and more velocity. New types of devices are introduced on a regular basis. More and more 'things are connected to the Internet and are expanding the attack surface. BYOD makes it harder to keep devices monitored and secured and users' demand for flexibility is making the information security department's job harder.

- Complex **regulatory and legal landscape**: understanding what regulations apply to a business can be confusing. In the US, for example, some States have put out data privacy laws. Unfortunately, they are all slightly different, and understanding the nuances if often needed. But also, industry regulations, such as the PCI DSS or HIPAA, place their demands on businesses. Keeping up with the changes of these regulations is a full-time job in itself.
- A scattered and sizable **security product landscape** has emerged over the past couple of decades. It used to be simple. It was anti-virus and firewalls. Today, there are application layer firewalls, universal threat management (UTM), web application firewalls, cloud application security brokers, etc. to mention a few product categories hovering around the concept of the 'old firewall'. I have a hard time counting how many security product categories we have today, but I'd argue probably too many to keep track of. As an MSP, you have to decide which product categories are relevant and necessary to be used in your clients' environments to keep them secure.
- A tough **security labor market** makes it difficult to offer not just managed security solutions, but even support the most basic of security products at client sites.

In this report, we have aggregated research into what SMBs think about MSPs and cybersecurity. We hope this report helps MSPs understand the larger needs for cybersecurity in their customer base and can see some of the nuances that might help shape service offerings and cybersecurity approaches. Fundamentally, the report highlights how cybersecurity is a key concern for SMBs and they need help from MSPs to deliver and manage solutions.

CHAPTER 2: EXECUTIVE SUMMARY

Year after year, the cybersecurity threat landscape grows ever larger, more complex and more daunting

Businesses – regardless of their size – are regularly finding themselves facing attack from threat actors ranging from criminal gangs to hacktivists to nation-states, meaning that the challenge of defending against such attacks is more important but equally more difficult than ever before.

In small and medium sized businesses (SMBs), this holds completely true. A tipping point has been reached, where cybersecurity can no longer be considered as a secondary thought after other priorities have been addressed. Cybersecurity is – correctly – seeing increased level of attention within board-level conversations and spending in this area is continuing to rise.

Cybersecurity attacks have risen in the past year, and there is a notable lack of confidence among SMBs around their capacity to defend against these. With the repercussions of an attack being potentially devastating, there is a clear need to improve defenses.

The issue is, however, that SMBs often lack the expertise, processes and solutions in-house to enable them to defend themselves against cybersecurity threats. There's a clear need for a trusted partner that can help them with this. Most SMBs are already exploring this – partnerships with managed service providers (MSPs) are relatively common and growing more so each year – however there is widespread disillusionment with current partners, and many are expecting to change partner in the near future.

This equates to a huge opportunity for MSPs. Those that can provide the right solutions and deliver them in the right way, complementing best-in-class technology with education, risk assessment support, and effective endpoint and network protection will be very well-placed to address SMB needs moving forwards.

Read on to find out more about what SMBs are demanding in 2022 and beyond and what an MSP needs to do to get ahead of the competition.

CHAPTER 3: KEY FINDINGS

Recognition of the importance of cybersecurity is growing within SMBs, likely because of so many suffering from cybersecurity attacks. However, SMBs often do not have the skills in-house to protect themselves adequately…

73%

of SMB respondents agree that their organization has reached a tipping point where cybersecurity concerns demand action

78%

of SMB respondents say that their organization is set to increase investment in cybersecurity in the next 12 months

31%

highlight board-level pressure as influencing the increased cybersecurity investment that they have planned – in 2020 only 14% said this

76%

of SMBs in the 2022 study have been impacted by at least one cybersecurity attack, a considerable increase compared to 55% that said this in 2020

67%

respondents admit that their organization does not have the skills in-house to properly deal with security issues

It is now fairly common for SMBs to partner with MSPs, a trend that is likely to continue, but many SMBs are not satisfied with the service they receive and may change provider. MSPs must strive to deliver the "right" services if they want to address SMBs' needs more effectively

89%

of SMB respondents' organizations are already using an MSP, up from 74% in 2020

Yet 42%

suggest that although they are currently working with an MSP, they plan to change to a different one in the near future

88%

of SMB respondents identify at least one MSP-related challenge that they face or expect to face

94%

of respondents would consider using or moving to a new MSP if they offered the "right" cybersecurity solution

39%

SMB respondents suggest that they would be willing to pay a new MSP 39% extra each year, on average, if they were able to provide the "right" cybersecurity solution

CHAPTER 4: THE MSP CYBERSECURITY OPPORTUNITY FOR SMBS IS NOW

Cybersecurity is a standout priority in SMB organizations

SMBs – just like any other organization – face a whole host of competing business priorities. Whether it is improving productivity, reducing operational costs, increasing business growth or upgrading technology infrastructure, the balancing act is immensely difficult to get right, especially in smaller organizations where budget and resource can be limited.

It's therefore hugely telling that when asked to rank their organization's biggest priorities for the next two years, "Protecting against cybersecurity attacks" came out on top according to surveyed IT and business decision makers, with 43% placing this in their top three priorities. This reveals a widespread recognition among SMBs of the importance of this area in this day and age.

Of course, labeling something as a priority and actually acting on that prioritization are two different things, but encouragingly SMBs appear to be putting their money where their mouth is here, with approaching four in five (78%) SMB respondents saying that their organization is set to increase investment in this area in the next 12 months.

With the threat landscape constantly evolving and with threat actors' cyberattack methods becoming more sophisticated seemingly by the day, greater investment in this area is a must. This presents a clear opportunity for MSPs, with those that are able to help SMBs to build their cybersecurity infrastructure potentially being highly desirable as partners.

For those that are anticipating an increase in spending in this area, a range of influencing factors are at play. There's widespread acknowledgement that doing so can reduce risk (46%) and help to increase customer trust levels (42%), but increasingly this pressure is coming from the very top of the organization. In 2022, around one in three (31%) highlight board-level pressure as an influencing this increased investment – more than double the proportion that said this only a couple of years ago.

Cybersecurity investment plans for the next 12 months

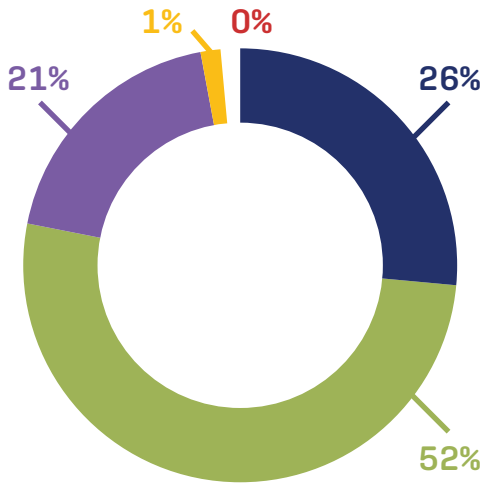
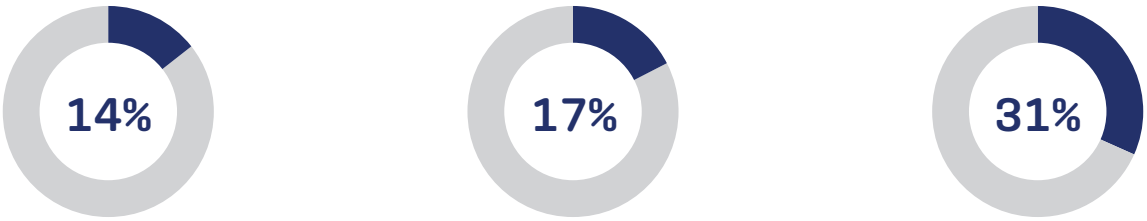


Fig. 1: Which of the following statements best describes your organization's level of investment in cybersecurity for the next 12 months? [700]

"Pressures from the board/decision makers" as an influencing factor for increased cybersecurity investment



Total 2020 [510] Total 2021 [541] Total 2022 [546]

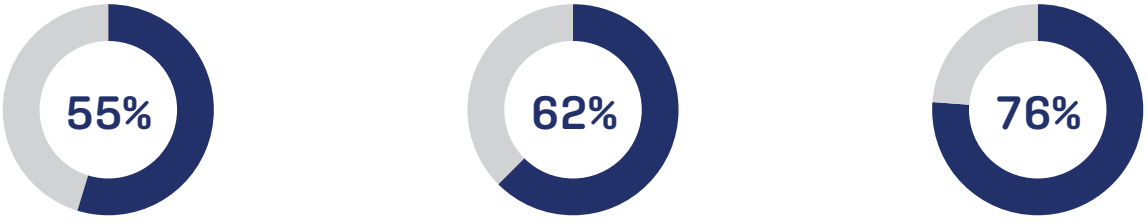
Fig. 2: Showing the proportion of respondents that consider "Pressures from the board/decision makers" to be one of the biggest influences for their organization to invest more in cybersecurity [Base numbers in chart] Asked to respondents from organizations that plan to invest more in cybersecurity in the next 12 months. Split by historical data

What this really hammers home is the fact that cybersecurity in modern-day SMBs is increasingly becoming a top table conversation point. Crystallizing this point, 73% of respondents agreed that their organization has reached a tipping point where cybersecurity concerns demand action. While some SMBs might still have their head in the sand, perhaps believing that they are too small to be attacked, the vast majority now recognize the threat that is facing them and are ready to act on it. The question is: Who will they go to in order to strengthen their defenses? For an MSP that can offer a range of cybersecurity enhancements, opportunity beckons.

Increasingly, SMBs are being negatively impacted by cybersecurity attacks

The 76% of surveyed SMBs in the 2022 study that have been impacted by at least one cybersecurity attack continues an upward trend over the last few years, highlighting that SMBs should take the mindset of "not if, but when" when they are considering if they are at risk.

Proportion that have suffered at least one cybersecurity attack in the past



Total 2020 [700] Total 2021 [700] Total 2022 [700]

Fig. 3: Showing the proportion of respondents' organizations that have suffered at least one cybersecurity attack in the past [Base numbers in chart] Split by historical data

The research also found that even the smallest SMBs (10-49 employees domestically) – those that may conceivably see themselves as too small to be a target – are at risk, with 73% of those interviewed in 2022 admitting that they have experienced at least one attack.

Looking to the future, concerns are very clear, with 83% of respondents stating that they are either extremely worried or somewhat worried that their organization will be targeted by a cybersecurity attack within the next 6 months. This could be as a result of high-profile cybersecurity attacks in the news but could also be a reflection of attacks that have hit many of these organizations previously.

Regardless, what it clearly indicates is that SMB organizations now tend to be highly conscious of the threat landscape that faces them.

This appears to be breeding a culture of fear in many SMBs. Around three in four respondents are either extremely or somewhat worried that their organization may experience remote devices or employees being breached (75%), customer data being breached (74%), or IT system downtime (73%), all of which have the potential to severely hinder operations and deliver considerable consequences.

Worse still, over two in three (69%) respondents admit that they are concerned a serious cybersecurity attack could be enough to put them out of business entirely. While it won't be especially common that this happens, the array of operational, reputational and regulatory issues that can come with a successful cybersecurity attack means that this outcome certainly is not out of the question.

Meanwhile, for those that have already experienced at least one cybersecurity attack, the widespread concerns noted above were justified, with almost all (98%) facing at least one impact. These impacts frequently included more obvious things, such as the time and effort needed to deal with the issue (38%) and loss of confidence in existing cybersecurity solutions (36%), but over one in three (36%) also noted that this was a trigger for them to change their IT managed service provider.

What this indicates is that SMBs are often not going to tolerate an MSP that cannot deliver on their cybersecurity promises. MSPs need to be able to walk the walk as well as they can talk the talk, so this means helping SMBs to build and maintain a truly secure and resilient IT environment that doesn't falter when threat actors come knocking.

Over two in three (69%) respondents admit that they are concerned a serious cybersecurity attack could be enough to put them out of business entirely

SMBs' current cybersecurity defenses in place

So, what are SMBs tending to do or have in place already as a means of strengthening their cybersecurity position? The most common implementations are foundation security (such as firewall or anti-virus) (53%), compliance security policies (52%) and security awareness training and education (46%), but alarmingly, it is only around half that have each.

These are all relatively basic cybersecurity elements but many SMBs appear to be missing them, inviting considerable risk in a time when defenses ought to be stronger than ever. This is another opportunity for an MSP to highlight their value to an SMB, by educating them on why each of these cybersecurity elements is important and then supporting them in implementation.

Cyber insurance in SMBs

While certainly not commonplace yet, three in ten (30%) SMB respondents indicate that their organization has some form of cyber insurance policy currently in place. With threat levels growing and SMBs evidently recognizing the need for strengthening their cybersecurity position, this could be another offering that is worth MSPs exploring and potentially helping their SMB customers with implementing in future.

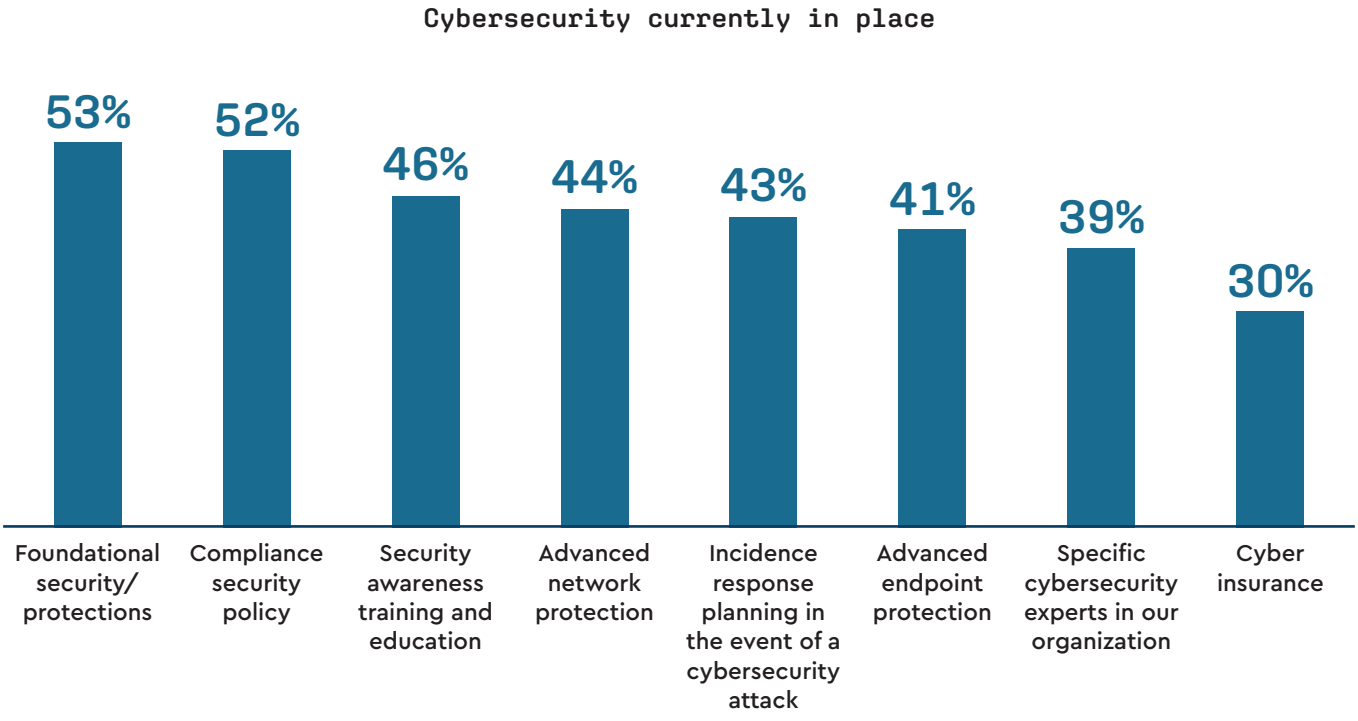


Fig. 4: Showing the proportion of respondents from organizations that currently have/do each of the above [700]

With the limited levels of implementation for a number of important cybersecurity functions, such as foundation security or security awareness training, it's perhaps unsurprising to see that many SMB respondents lack confidence in how well prepared their organization is to defend against cybersecurity attacks.

For example, only 40% consider their organization to be very well protected against customer data being breached, with 41% saying the same about protection against IT system downtime. Either of these scenarios could be catastrophic for a small business, so for the majority that are lacking faith in their protection against them, there's considerable work to do. Once again, this presents an important opportunity for an MSP to help improve cybersecurity infrastructure and processes in these organizations and help them to grow in confidence.

A similar story is true in relation to securing cloud services, with only 22% of respondents being completely confident that their organization's cloud services are secure against cybersecurity threats. Almost all (99%) surveyed SMBs are using cloud services to some extent, so it is imperative that they are safeguarded to ensure that systems and data sources are not left vulnerable.

In summary, there's a huge amount of work to be done in many SMBs in terms of their cybersecurity. It's a clear focus area and one where investment is set to rise and where board-level conversations and recognition are growing more common by the year. A fundamental problem, however, is that most SMBs cannot combat the cybersecurity threat on their own. Two in three (67%) respondents admit that their organization does not have the skills in-house to properly deal with security issues.

What this points to is a glaring need within SMBs for greater support and guidance from outside of the organization. The opportunity is there for MSPs to be this trusted cybersecurity partner, it's just a question of whether they have what it takes to deliver the right solutions and the right support.

Two in three (67%) respondents admit that their organization does not have the skills in-house to properly deal with security issues

CHAPTER 5: SMBS ARE SEARCHING FOR THE RIGHT PARTNER WITH THE RIGHT CYBERSECURITY OFFERING

Current and future utilization of MSPs by SMBs

There is already a clear appreciation among SMBs of the value that can be derived from working with an MSP. Whether their help is enlisted to provide additional IT manpower to the organization, to provide expertise and guidance, or to help with implementing new technologies, around nine in ten (89%) SMB respondents' organizations are already using an MSP. And over time, these partnerships tend to be growing more common, with this figure up from 74% in 2020.

However, while the idea of partnering with an MSP clearly appeals to most SMBs, this does not mean that MSPs have an easy ride ahead of them. With so many partners to choose from, each with different product offerings and service arrangements, SMBs can afford to be choosy. As such, an impressive 42% suggest that although they are currently working with an MSP, they plan to change to a different one in the near future. For MSPs that cannot keep their customers happy, this is worrying reading. For those that know what SMBs want and how best to deliver it to them, this presents an exciting opportunity.

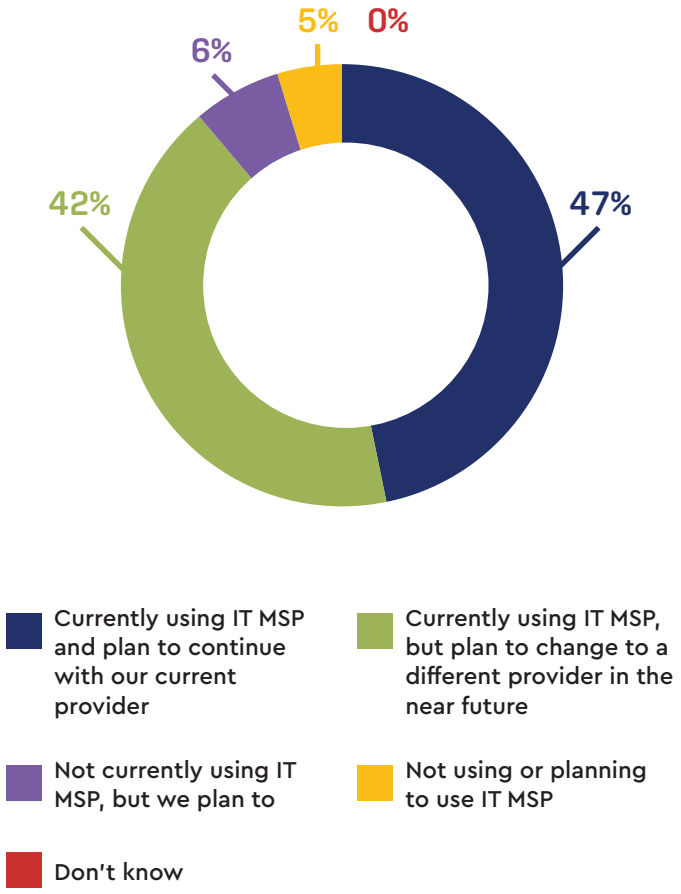


Fig. 5: Is your organization using a managed IT service provider? [Base numbers in chart] Split by historical data

More generally, the data also suggests a trend wherein SMBs are set to outsource more of their IT to an MSP over the next few years. Taking IT services as an example, 43% of respondents suggest either all or the majority of this is outsourced currently, but in five years' time 51% predict that this will be the case. For cybersecurity, a similar trend is seen (47% up to 54%). While relatively modest increases, they do illustrate a growing willingness among SMBs to leave the bulk of their IT to an external partner.

However, these SMB and MSP relationships are certainly not without their challenges. 88% of SMB respondents identify at least one MSP-related challenge, but challenges are much more common in organizations where they are expecting to change to a different provider in the near future.

Many SMB respondents highlight a lack of trust in their provider as a challenge, indicating that for any MSP that wants high customer satisfaction and customer longevity, trust-building is a must. One way that they could help build this trust is via enhancements in SMBs' cybersecurity protections. An MSP that can educate SMB employees on cybersecurity attacks and help them to safeguard their IT systems and processes against such threats stands a much better chance of being able to position themselves as the trusted partner that SMBs clearly seek.

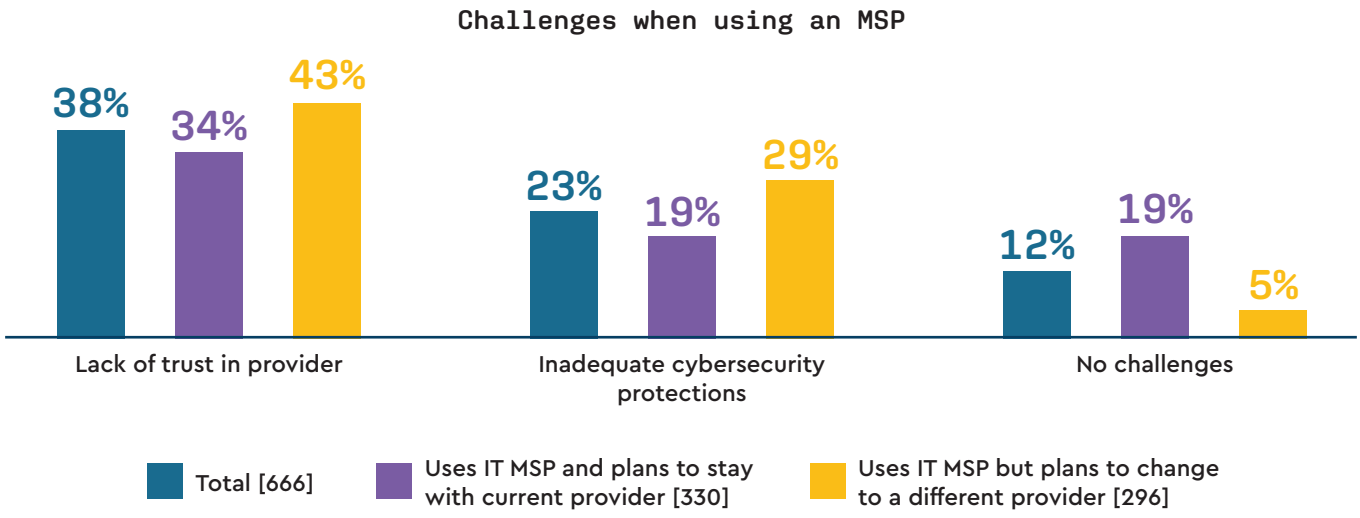


Fig. 6: What challenges have you seen/do you expect to see for your organization from using a managed IT service provider? [Base numbers in chart] Asked to respondents from organizations which are currently using or planning to use a managed IT service provider. Split by use of MSP, not showing all answer options

Not only is it essential for MSPs to build trust, but they also need to be aware of the ramifications if any of their SMB clients were to hit by a cybersecurity attack. In 2022, 84% of SMB respondents said their organization would consider taking legal action against their MSP in the event of a cybersecurity attack (up from 61% in 2020). If this were to happen, it could have many consequences for the MSP, one of which being that it could quickly sour a relationship. With attacks being relatively commonplace now, it is likely that sooner or later, SMBs and their MSPs will face this scenario and potentially see their relationship damaged if it is not handled appropriately.

Communication is likely to be another variable that can really differentiate an average MSP from a great MSP in the eyes of an SMB, especially in the context of cybersecurity. It's important for MSPs to be proactive in their outreach to ensure that SMBs are never left second guessing.

This appears to be an area that some improvements are being made over time – in 2022 43% of SMB respondents report that their provider brings up cybersecurity conversations on their own, versus 28% in 2020. That does however still leave ample room for improvement. At the same time, only 5% of 2022 respondents indicate that such conversations happen as a matter of course, compared to 13% in 2020.

Regardless, for any MSP that wants to build trust among their SMB customer-base and thereby be able to take advantage of potential new SMB customers in the future, they must be ready and able to deliver above and beyond on cybersecurity infrastructure and processes as well as on the conversations and advice needed to support these.

Finding the "right" MSP partner – what are SMBs searching for?

We have already established that many SMBs do not see their MSP partnerships as having a great deal of longevity, with 42% actively expecting to change partner in the near future.

However, beyond this group that are already considering different options for the future, an even greater proportion are also open to change, if the right alternative presented itself – **94% of respondents would consider using or moving to a new MSP if they offered the "right" cybersecurity solution**.

This demonstrates two things: First, simply that SMBs' prioritization of cybersecurity really cannot be understated. And second, that in order to "win" as an MSP in the coming years, complacency must be avoided. It is essential that MSPs are able to clearly and concisely illustrate to SMBs exactly how their solutions, services and support can help them to stay safe while also continuously developing offerings to ensure they keep pace with the ever-changing needs of modern-day SMBs.

So, when talking about becoming an MSP with the "right" cybersecurity solution, what exactly does that mean? Inevitably, a range of different factors apply here and there's no one size fits all, but the most likely factor (54%) relates to giving SMBs confidence in their ability to respond appropriately to security incidents. Considering how often SMBs are now facing cybersecurity threats, this makes a lot of sense.

Most important factors for helping SMBs decide if a provider has the "right" cybersecurity solution for them

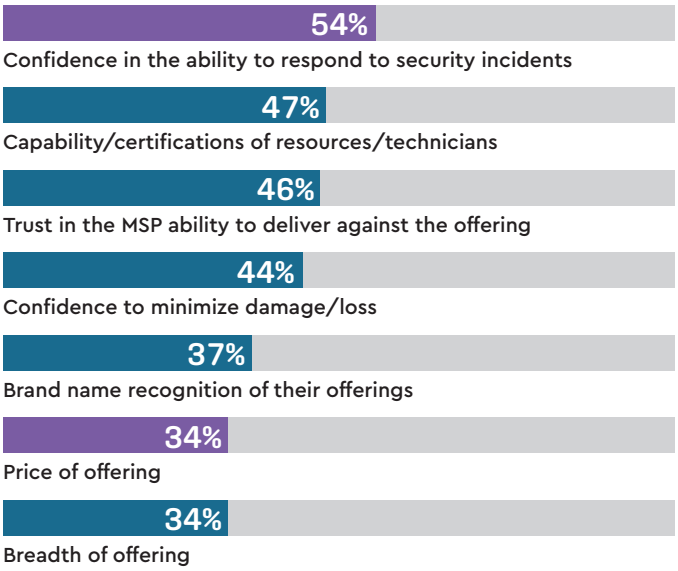


Fig. 7: What are the most important factors that would help you decide if a provider had the "right" cybersecurity solution for your organization? [700]

Elsewhere, it is important to note that "Price of offering" is one of the least likely factors. What this indicates is that for SMBs, it is not always about spending as little as possible, but instead about spending as smart as possible.

In fact, in 2022, SMB respondents suggest that they would be willing to pay a new MSP 39% extra each year, on average, if they were able to provide the "right" cybersecurity solution, a figure that has been gradually increasing over the last few years up from 30% in 2020. Again, what it seems to come down to is MSPs being able to provide clear and compelling evidence to SMBs that their solutions for cybersecurity address the above factors better than others in the market.

Elsewhere, the research found that SMB respondents see the following as being important when speaking to an MSP about cybersecurity:

- 40% – Recognition of the role that people and processes have to play in cybersecurity, in addition to technology
- 38% – Being solution-oriented (i.e., working out solutions rather than just highlighting problems)
- 35% – Directly relating offerings to specific parts of the SMB's business
- 29% – Empathizing with those within the SMB as people

The best MSPs should aim to address all of these points, ensuring that they convince an SMB of the value that they could deliver as a partner.

As things stand, there is a lot of room for improvement in terms of SMBs' overall confidence in their cybersecurity defenses. Only 28% of respondents are fully confident that if a cybersecurity attack were to target their organization, they would be able to defend against it without any impact to the business.

These confidence levels are also closely related to whether SMBs are satisfied or dissatisfied with their MSP partners, with those that plan to stay with their current MSP far more likely to have a high level of confidence in their ability to fend off attacks.

The ideal scenario for any small or medium business is that they don't need to live in fear of a cybersecurity attack derailing their operations or leaving their data exposed, and while completely removing this fear factor is perhaps an unrealistic target, reducing it considerably is not, if they have a partner that they can trust. Improving cybersecurity defenses and thereby increasing these confidence levels is what MSPs must strive for if they want to be successful as a partner to SMBs.

"Confident in all cases" about being able to defend against a cybersecurity attack without any impact to the business

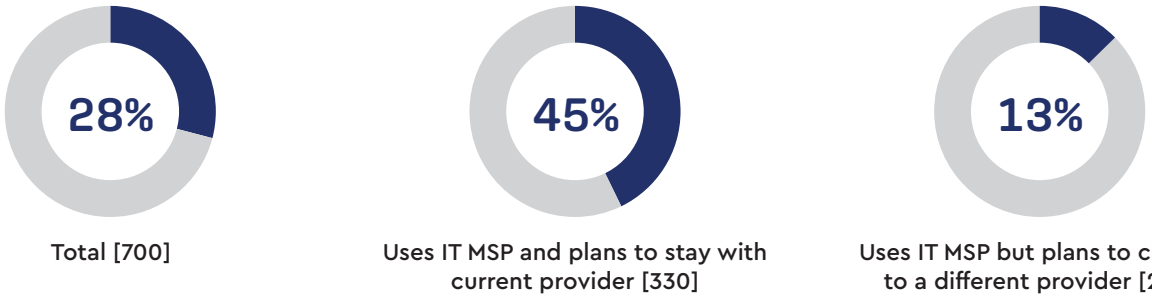


Fig. 8: Showing the proportion of respondents that are confident in all cases that if their organization were the target of a cybersecurity attack, their IT service provider would be able to defend them against the attack without any impact to the business [Base numbers in chart] Split by use of MSP

ConnectWise call to arms:

In short, having the right cybersecurity means giving your SMB clients confidence in your ability to prevent the most common attacks and help them avoid costly security breaches. The research indicates that for SMBs it is not always about spending as little as possible but instead about spending as smartly as possible.

The second factor that matters when talking about becoming an MSSP (Managed Security Service Provider) is the being able to deliver the "right" cybersecurity solution to their customers. This goes hand-in-hand with the first factor because it speaks directly to customer empathy: understanding what your clients need before they do so you can provide them with solutions before they even ask for them.

The third factor of a good MSSP with the right cybersecurity solutions is being solution-oriented (i.e., working out complete solutions rather than just selling individual products).

The fact is, no one can predict when an attack will happen. It's not a question of if an attack will succeed, but when.

That's why we urge MSPs to be ready for the inevitable by going through an incident response readiness exercise. This could be as simple as documenting your process or as complex as **working closely with** us to create a full-blown incident response program.

At ConnectWise, we are committed to helping our partners deal with the five market dynamics and 'moving targets' above and help MSPs deliver the most adequate portfolio of security solutions with products and services to secure the SMBs. With our standalone products for MSPs that have their own staff and with our expert services or security operations center (SOC) driven solutions, we have solutions tailored to your mode of operation, whether you need us to help you attackers or plan for the future.

Remove the complexity associated with 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 client security outcomes.

CHAPTER 6: 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 May 2022, 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.

About ConnectWise:

ConnectWise is the world's leading software company dedicated to the success of IT solution providers (TSPs) through unmatched software, services, community, and marketplace of integrations. ConnectWise offers an innovative, integrated, and security-centric platform—Asio™—which provides unmatched flexibility that fuels profitable, long-term growth for partners. ConnectWise enables TSPs to drive business efficiency with automation, IT documentation, and data management capabilities and increase revenue with remote monitoring, cybersecurity, and backup and disaster recovery technologies. For more information, visit **connectwise.com**.

About Vanson Bourne:

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 **vansonbourne.com**