CONNECTWISE

CONNECTWISE EBOOK SERIES

Cybersecurity in an Era of Competing Priorities:

THE STATE OF SMB CYBERSECURITY IN 2021

VansonBourne

CONTENTS

FORWARD

By Drew Sanford, Senior Director of Global SOC Operations for ConnectWise.

Drew Sanford, Senior Director of Global SOC Operations for ConnectWise

As I look back on 2020, it is a year of mixed messages. Many say it was one of the most challenging years they have seen. Others propose it was a year of growth and progress. How can one year generate such diverse views? Is one view wrong and another right, or is it that somehow both have a part in the story? Did we see a year of unprecedented challenge and, at the same time, unparalleled success for some?

In truth, one place these diverse conversations played out was in the cybersecurity landscape. On the one hand, we saw dramatic growth in the tools, methods, and successes of nation-state actors and criminal organizations. Through a continued rise of ransomware-as-a-service, extortion schemes, and many other vectors, the rewards these attackers have seen continue to grow at a dizzying clip. While these attacks tell a grim story, we also saw unparalleled growth in many parts of MSP communities. Much of this growth was fueled by realizing how to help their customers identify and protect themselves against these same threats.

Why were these organizations able to see this growth right in the middle of a pandemic, with many others experiencing significant economic challenges? Here in this report, you will find the views of hundreds of SMB organizations, how they are thinking about the cyber landscape and the risks associated with it, and lastly, a piece of the demand that is allowing many MSPs to find success against many odds.

EXECUTIVE SUMMARY

Now more than ever, managed IT service providers cannot afford to be complacent when it comes to cybersecurity. While usage of them is widespread among SMBs, and they play a key role in assisting with their cybersecurity protections, a sizeable proportion of SMBs which currently use a service provider are planning to move to a new one. It is crucial MSPs ensure they offer the support organizations require, in order to attract and retain customers. Understanding the requirements of SMBs is critical to being able to do this.

First and foremost, service providers must take note of the evidence that cybersecurity is a key feature of these requirements. Cyberattacks have risen in the past year, and few SMBs are confident they could defend themselves against them. With the repercussions of an attack being potentially devastating, there is a clear need to improve defenses. Using the right IT service provider could be the differentiator in the ability to defend against an attack.

It is not only that threats are increasing, but the environment in which organizations are attempting to deal with them has become all the more complicated. In many organizations, cybersecurity has to compete with other priorities such as cloud and technology adoption for time and attention. The rise of remote work adds additional complexity to the cybersecurity environment which is not yet being addressed either. Many managed service providers can offer assistance here, if they can convince SMBs of the benefits they provide.

SMBs are aware of the steps they need to take in order to up their game in this area. Many have seen cybersecurity budgets increase over the last year, and investment is set to rise further over the next. The opportunity is ripe for managed IT service providers to attract new customers. To do so they need to demonstrate that they can be relied upon, and how by partnering with them, organizations can realize a whole host of benefits they might not even know they could.

KEY FINDINGS

The need for SMBs to act to improve their cybersecurity protections is urgent. Cybersecurity threats are on the rise, and cost of suffering an attack has skyrocketed

32% of SMBs have suffered a cybersecurity attack in the past 12 months, an increase from 25% who reported the same in 2020

Only 23% of decision makers are confident in all cases that their organization/IT service provider would be able to defend itself in the event of an attack

For organizations which have suffered financial repercussions of an attack, the total cost has been on average $104,296, almost double the figure reported in 2019 ($53,987)

Managed IT service provider usage is common, and their responsibility for cybersecurity is expected to rise. However, organizations are not necessarily going to stay with their current provider

49% of these organizations currently outsource all or the majority of their cybersecurity to their provider, and 57% of all SMBs plan to outsource all or the majority in five years' time

82% of SMBs currently use a managed IT service provider, but 29% plan to change to a different provider in the next 12 months or beyond

The range of competing priorities, the added complexity of remote work, communication breakdown, and lack of in-house skills may all be contributing to the increased threat landscape

+ Cybersecurity has fallen from being a top priority in 45% of organizations in 2019, to 38% in 2021

+ **75% of decision makers agree that the added complexity of a remote workforce means that they are less secure**

+ Only 7% of organizations which use a managed IT service provider have cyber-security-specific conversations with them as a matter of course

+ 61% agree that their organization lacks the skills in-house to be able to properly deal with security issues

However, organizations are looking to improve in these areas, giving plenty of opportunity for MSPs, if they can prove their ability to improve cybersecurity protection

77%
of organizations plan to increase their level of investment in cybersecurity in the next 12 months

92%
of organizations would consider using/moving to a new IT service provider if they offered the "right" solution

34%
And these organizations would pay on average 34% more for a service provider who could provide this solution, a rise from 25% in 2019*

*Please see methodology section for more information on the 2019 sample

SECTION 1

The SMB & MSP relationship – a blooming partnership, but not yet a match made in heaven

There are numerous examples throughout history of actors failing to achieve their goals when success seems ready for the taking. From historic military disasters such as Napoleon's invasion of Russia, to the collapse of a sporting sensation's career in their prime due to injury or misadventures off the field, to the musician unable to recreate the dizzying heights of a stellar first album; success is never guaranteed, no matter how favorable the circumstances or opportunity may initially seem. Without an awareness of what these circumstances really are, inevitable success can turn into devastating failure in a heartbeat.

This is again true when you look at the SMB/MSP relationship. Managed IT service providers may well have reason to feel encouraged by their widespread usage among SMBs. 82% of surveyed SMBs currently use a managed IT service provider, and a further 10% plan to do so in the next 12 months and beyond – their popularity is clear to see. However they should not get complacent and assume this popularity represents a stable market – as we can see in Figure 1, 29% of organizations plan to change to a different provider in the near future.

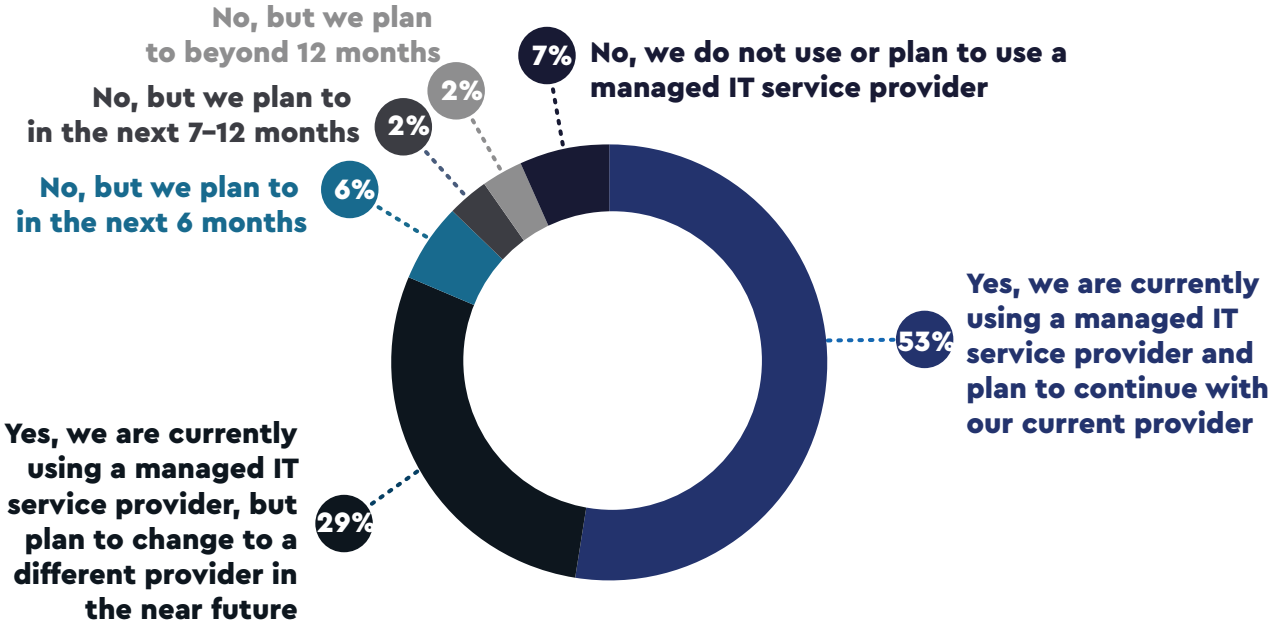


Fig 1: Is your organization using a managed IT service provider? [700]

"Success is where preparation and opportunity meet"

—BOBBY UNSER

This could be cause for concern for managed IT service providers, nonetheless it also presents them with great opportunity. The proportion who are planning or willing to move indicates a lack of satisfaction with the service providers currently in use, and a risk to these MSPs of losing business if they aren't able to address this. On the opposite side of the coin, there is the chance to capitalize on the unstable market and to acquire new customers, if these service providers can show their capabilities in the areas others are currently falling behind.

The question for IT service providers then is how to capitalize on this opportunity, to ensure they are gaining customers, and not losing them to other providers who are better able to meet their requirements. This calls for an understanding of SMBs' needs, both now and in the future.

Key amongst these needs is cybersecurity. Among SMBs who already or plan to use an IT service provider, 49% currently or will outsource the majority of their cybersecurity to them. This figure is only expected to rise – in five years' time, 57% of organizations expect they will do this. It is therefore crucial that IT service providers can demonstrate they have the cybersecurity credentials to be able to cope with this rise. Service providers who aren't able to do this risk losing business to those who can. **Even those who aren't actively looking for a new provider are open to change if an MSP can demonstrate these credentials – 92% would consider using/moving to a new IT service provider if they offered the "right" cybersecurity solution. The simple fact is that the net-winners in this unstable market are going to be the service providers who can provide this solution.**

But what is the "right" cybersecurity solution?

Confidence in the ability to respond to security incidents (62%) or to minimize damage/ loss (51%) are most likely to be reported as key factors – and crucially, more so than price (44%). Organizations need to trust that the service provider can offer protection that works, and if MSPs can do this, price does not have to be a limiting factor. This is further reinforced by the fact that organizations have become increasingly prepared to be flexible on price when it comes to contracting the "right" cybersecurity solution: in 2019*, organizations would be prepared to pay 25% more on average for the right solution, and this has risen to 30% in 2020, and now 34% in 2021.

In order for MSPs to show they can provide the cybersecurity solution which SMBs are looking for, and take advantage of the opportunity this unstable market provides, there is an important question that needs answering – what are the cybersecurity challenges organizations are currently facing?

SECTION 2

Cybersecurity – a challenge increasing in frequency and in devastation

Looking at the current threat landscape, cybersecurity is not an issue which SMBs can afford to ignore. The proportion of SMBs who report suffering a cyberattack in the past 12 months has risen from 25% in 2020 to 32% in 2021. With the risks of an attack growing, we can see it is of ever-increasing importance organizations can ensure they are able to protect themselves.

Yet worryingly, organizations are not fully prepared to cope with these attacks. 77% of decision makers aren't confident in all cases that their organization or managed IT service provider, where one is in use, could defend against an attack without any impact to the business. This figure rises to a staggering 95% in organizations which aren't using an MSP, and 87% in those who are using a service provider but plan to change to a different one. Meanwhile only 65% of decision makers from organizations which currently plan to stay with their service provider lack this confidence – likely as a result of the support their MSP has provided, although even for these organizations, there is still a way to go. Many SMBs are therefore exposing themselves to risk at a time when attacks are on the rise, and there is a clear need to improve their cybersecurity protections to protect against this risk, improvements which the right managed IT service provider could help them make.

The need for action is urgent, with 79% of decision makers concerned their organization will be the target of a cybersecurity attack in the next 6 months. IT Decision Makers (ITDMs) are more likely to be recognizing this threat (83%) than Business Decisions Makers (BDMs) (75%), suggesting BDMs may not be fully aware of the extent of the threats their organization is facing. Organizations must ensure they aren't lulled into a false sense of security when it comes to cybersecurity and are listening to the concerns of their IT department.

The business case to make improvements to cybersecurity protections is clear when looking at the impacts of cybersecurity attacks over the past two years. Not only are attacks growing in frequency, but they are also becoming more financially harmful for organizations to suffer. **For those who have incurred costs as a result of a cyberattack, the total business cost of the attack in the last two years has been $104,296, almost twice the cost reported in 2019 ($53,987)*.** SMBs need to ask themselves, can they afford to expose themselves to the threat of this level of loss, when the answer to reducing the risk of a successful attack might simply be using a service provider?

But it is not only financial repercussions which organizations are at risk of experiencing. 40% of organizations who suffered a cybersecurity attack in 2021 experienced data loss as a result, 36% were impacted by the cost (time/effort) of dealing with the issue, 36% by the cost (money of dealing with the issue), and 33% experienced damage to company reputation. Protection against cybersecurity attacks is therefore crucial to ensuring business operation and profits are not at risk, and to offer protection against damage to company reputation.

It is not just organizations who should be concerned about the rise in cybersecurity attacks, however. In the event an attack did occur, 82% of organizations who use an IT service provider would hold the service provider at least partly accountable for it. Perhaps even more worryingly, 68% of organizations **would take legal action against their IT service provider**, a rise from 61% in 2020 – service providers are not just at risk of losing business in the case of an attack, but of suffering devastating reputation and financial damage.

It is apparent SMBs feel their service providers hold strong responsibility for their security, and service providers need to ensure they have the capabilities to meet this. If they don't, they risk suffering the same, if not greater, financial and reputation damage than the organization itself.

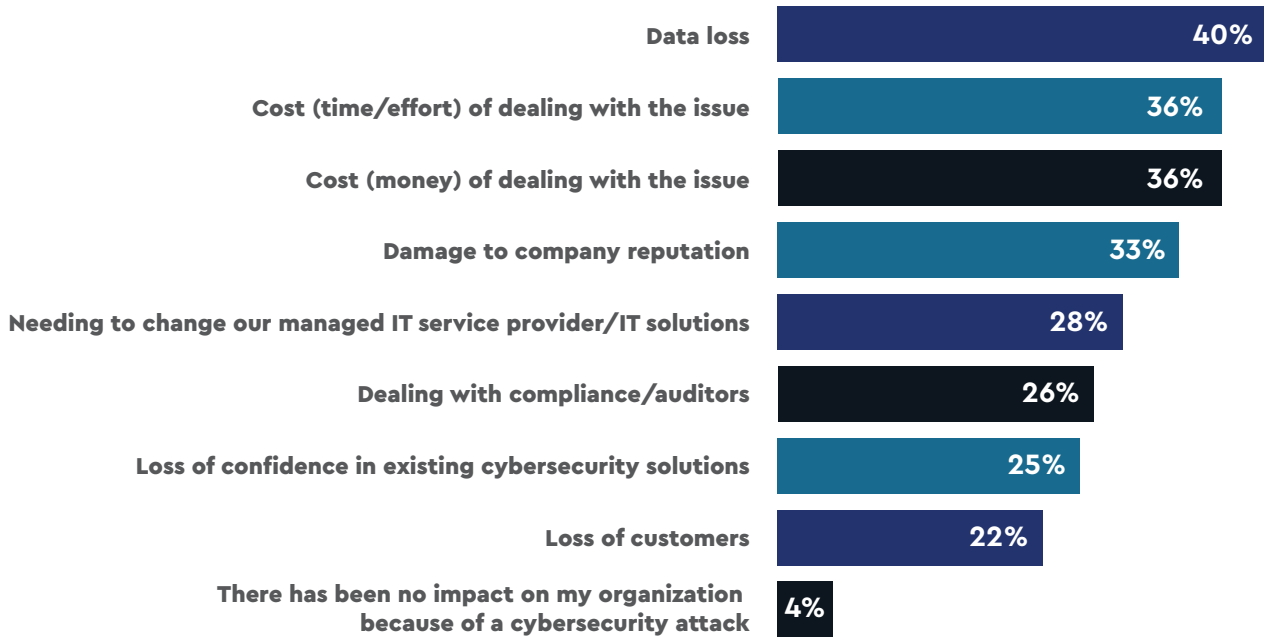


Fig 2: What has been the impact of cybersecurity attack(s) on your organization? [433] Respondents from organizations which have experienced a cyber attack, not showing all answer options

*Please see methodology section for more information on the 2019 sample

SECTION 3

The four critical challenges SMBs can't afford to ignore in 2021.

Recognizing that cybersecurity threats are growing and demand response is one thing, but taking the action to alleviate these threats is another. Cybersecurity threats do not exist in a vacuum; the activities and events occurring within organizations and the world at large have a huge impact on the way threats manifest. These activities and events can create challenges within the cybersecurity environment and increase the difficulty of dealing with them. We have identified four of the key challenges SMBs are facing which could be reducing their ability to tackle the cybersecurity threats:

- **Challenge one**: The difficulty of managing cybersecurity in an environment of competing priorities
- **Challenge two**: The added complexity of |remote work
- **Challenge three**: Poor communication between organizations and their managed IT service providers about cybersecurity needs
- **Challenge four:** Poor cybersecurity skillsets within the organization

These are all areas which managed IT service providers can help SMBs to address, and by providing evidence of their ability to do this these providers will be able to better compete in the unstable service provider market which currently exists.

Challenge one: The difficulty of managing cybersecurity in an environment of competing priorities

There was a time when cybersecurity was perhaps THE key focus for organizations when it came to their technology infrastructure. However, as the breadth of technologies available to organizations has evolved, and the economy in which they operate has rapidly slowed, SMBs are no longer able to prioritize in the way they have in years past. By not giving cybersecurity sufficient attention, organizations increase the risk of their protections being inadequate to meet the challenges of 2021.

Nonetheless, protecting against cybersecurity attacks has fallen from being a top three priority in 49% of organizations in 2020, to 44% in 2021. Meanwhile, technology has grown from being a priority in 41% of organizations to 47%. Cloud adoption, while still not as common a priority as cybersecurity, has also grown, from 30% to 41%. In this environment of increasing competing priorities, there is less time available for SMBs to prioritize cybersecurity. Likely as a result of this, it has dropped from being critical to the business in 45% of organizations in 2019, to 38% now*. While this is understandable in the context of numerous other emerging, competing priorities, organizations must ensure they aren't falling behind in their cybersecurity protections; it makes them vulnerable to risks.

One issue is the increase in prioritization of the cloud could be exposing organizations to further cybersecurity problems, if cloud solutions aren't adequately protected – while the cloud may be perceived to be more secure, this is not the case if steps aren't taken to ensure protections are in place.

The need to prioritize cybersecurity is better recognized by IT than other departments. ITDMs are more likely to say protecting against cybersecurity attacks is one of their top three priorities (48%) than BDMs (39%), and that cybersecurity is critical to the business (46%) than BDMs as well (31%). Organizations need to ensure they are listening to the concerns of their colleagues in the IT department when it comes to cybersecurity, and prioritize it appropriately; yet at present this doesn't appear to be the case.

The struggle to prioritize cybersecurity in the face of other competing factors appears to be having an impact on the extent to which organizations have been able to implement various security measures and processes within SMBs. Despite the rise in attacks in the last year, there has been a slowdown in the rate in which many measures that could improve their defenses against attacks have been implemented.

As evidenced in Figure 3, the proportion who are implementing security awareness and training has risen only from 55% to 57% since 2020, and the proportion implementing advanced network protection has stayed steady at 52% in this time (compared to 53% in 2020), as has the proportion implementing incident response (49% in both years).

However, this is an area where using a managed service provider can provide immense value. Organizations which use a manage service provider and plan to stay with them are more likely to implement these measures than those who use a managed service provider and plan to change, or who don't use a managed service provider at all. Using the right service provider therefore seems to be key to in facilitating organizations to implement cybersecurity protections in a time of competing priorities.

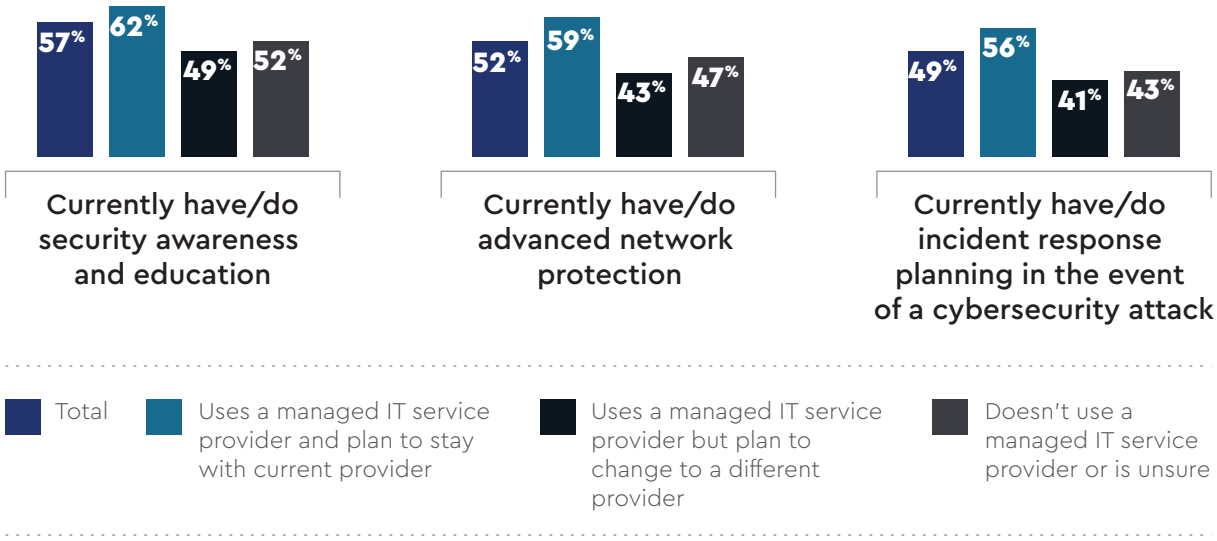
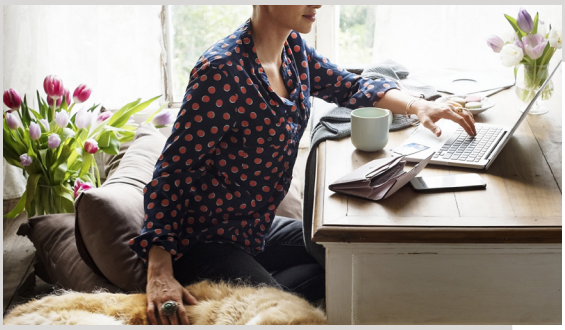


Fig 3: Which of the following does your organization currently have/do, or is planning to implement? [700] Split by usage of a managed IT service provider
*Please see methodology section for more information on the 2019 sample

Feeding into this slowdown also appears to be an attitude of complacency. It is notable that decision makers are less likely to be worried their organization is at risk of customer data being breached (76%) now than they were in 2020 (83%); a similar trend occurs for concerns about internal data being breached (falling from 81% in 2020 to 74% in 2021). This is in spite of decision makers only being slightly more likely to say these areas are very well protected than they did in 2020, with a rise from 43% to 44% saying they are very well protected against customer data being breached, and 39% to 43% saying the same about internal data. It is imperative that organizations not get overconfident in the abilities of their current solutions in times of increasing cybersecurity threats.



Challenge two: The added complexity of remote work

A further challenge to organizations' ability to deal with cybersecurity threats is the complexity that was caused by the move to remote work in 2020. The difficulties this caused are well recognized, with **75% of decision makers agreeing that their organization is less secure due to the added complexity of a remote workforce**.

While it might be tempting to think that this is a challenge which is unique to the height of the pandemic, it is not one which is going to go away any time soon. Although remote work peaked in 2020, when on average 59% of employees worked remotely, it still remains that 42% of employees on average are working remotely now. And this figure is only expected to fall to 34% in one year's time. Remote work is not a trend that will be left in 2020 and 2021, but one that will continue in the long term; organizations will have to be prepared to deal with these challenges well into the future.

However, SMBs don't yet seem to be responding to the challenges to cybersecurity which remote work poses. The same proportion of organizations currently have advanced endpoint protection (47%) as did in 2020, despite endpoints continuing to be at potentially greater risk due to their increased geographic dispersion. **Similarly, only 35% of decision makers report their organization is very well protected against remote devices/employees being breached, further evidencing that organizations are not yet taking the steps they should be to protect remote employees.**

It is perhaps understandable that in a period in which organizations have a range of other priorities battling for attention, many haven't been able to dedicate the time and resources to implementing these measures. However, SMBs need not despair yet, as these are areas in which usage of the right managed IT service provider can provide enormous assistance. 56% of organizations which use a managed service provider they plan to stay with have advanced endpoint protection, compared to 40% of those who use a managed service provider but plan to change, and 33% of those who don't use one at all. Likewise, while 43% of organizations which use a managed IT service provider with no plans to change are very well protected against remote devices/employees being breached, only 31% of those using a managed IT service provider they plan to change, and 19% of those not using a managed IT service provider say the same.

It is therefore again apparent that using the right IT service provider can be the silver bullet to addressing the issues SMBs face in the current cybersecurity landscape. Providers who can prove their ability to help in these areas will likely have a competitive advantage in attracting and retaining business than those who don't.

Currently have advanced endpoint protection

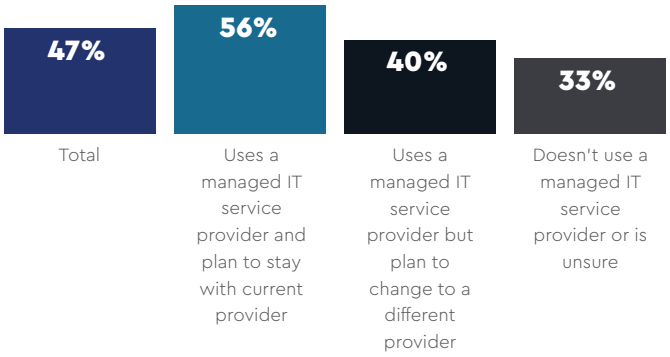


Fig 4: Showing the proportion who currently have advanced endpoint protection e.g. the ability to detect a threat on a device beyond antivirus [700] Split by usage of a managed IT service provider

Very well protected against remote devices/employees being breached

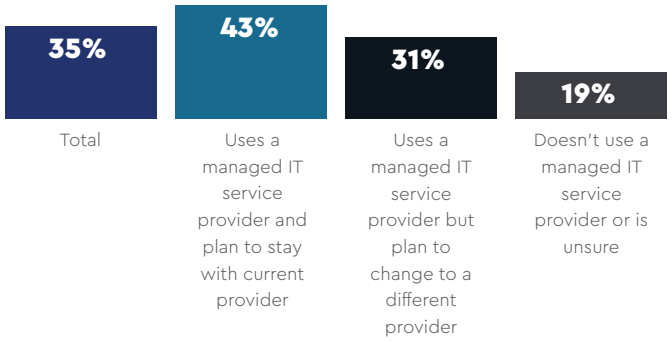


Fig 5: Showing the proportion who feel their organization is very well protected against remote devices/employees being breached [700] Split by usage of a managed IT service provider

Challenge three: Poor communication between organizations and their managed IT service providers about cybersecurity needs

We have already seen that IT decision makers tend to be more aware of the cybersecurity issues their organization is facing than those from other departments, suggesting communication within the organization over issues is often lacking. However it is not just inter-departmental communication which could be causing issues for SMBs, but also poor communication between the organization and its IT service provider.

Only 7% of organizations have cybersecurity- specific conversations as a matter of course, a fall from 13% in 2020. This may be because the cybersecurity landscape was deemed to be more pressing in 2020, as organizations shifted to remote working environments. However, the cybersecurity issues which remote work can create are not going away, and SMBs need to make sure they are staying on top of them. If organizations are only speaking to their service providers about cybersecurity on an annual or quarterly basis, or after an incident occurs, they could be putting themselves at risk of not ensuring they have the most relevant and up to date provisions in place.

Nothing triggers our organization to have cybersecurity-specific conversations with our provider – we do as a matter of course

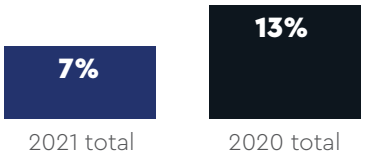


Fig 6: What triggers your organization to have cybersecurity-specific conversations with your IT service provider? [576] Showing the proportion of respondents which are using a managed service provider who selected "Nothing triggers our organization to have cybersecurity specific conversations with our provider – we do it as a matter of course", split by year

Indeed, when it comes specifically to the cybersecurity provisions for remote workers, we can see communication is again poor. **Only 44% of organizations regularly discuss with their service provider how to adapt their cybersecurity protections for remote workers.** It is clear from this research that the problem of cybersecurity is an ever evolving one, and if organizations aren't regularly communicating internally or with their MSPs about the threat landscape, they are at risk of falling prey to an attack which could be devastating to them.

Service providers who want to retain their current customers should ensure they are being proactive to instigate these conversations, to ensure organizations are as satisfied with their service as possible.

Challenge four: Poor cybersecurity skillsets within SMBs

Also contributing to the threats organizations are facing, is the increase in decision makers stating that their organization lacks the skills in house to be able to properly deal with security issues. This figure has risen from 52% in 2020 to 61% in 2021. Organizations are clearly lacking in the ability to deal with the growing cybersecurity threats and complexity in their organization. This provides a clear and compelling case for organizations to work more closely with their managed IT service provider.

SECTION 4

The SMB response to the cybersecurity threat – and what MSPs can do to fix it

Despite SMBs often being slow so far to respond to the cybersecurity issues they are facing, there is clear recognition from respondents that their organization could be doing more. This recognition is the first step for SMBs in taking the action required to address these challenges. **More than three quarters (79%) agree there should be a lot more emphasis placed on security in their organization (a view driven in particular by IT decision makers, 83% of whom agree with this). And even more (88%) agree that cybersecurity should encompass all aspects of their organization.**

And these don't just appear to be empty words. Indications are that organizations are moving in the right direction when it comes to investment in cybersecurity: on average, cybersecurity budgets increased by 10% in 2020. These budget increases have in large parts been driven by the increase in remote working, with 59% of those whose organization has increased their budget at all reporting this as a reason for doing so. This figure is even higher for those that don't currently use an MSP (68%). For these organizations, potentially this budget might have been better spent on contracting a managed IT service provider that could support and direct an organization in increasing their remote working, to more effectively deal with the issues remote work has created.

Even more promisingly, there is likely to be an increased interest going forwards on ensuring remote workforces are secure. Eight in ten (81%) say they are focused on ensuring remote workers are secure after the initial rapid shift to remote working at the start of the COVID-19 pandemic. This is more of a focus for those who currently have an MSP and plan to stay with them (84%), showing they will be looking for help in this area. However, those who don't use an MSP are less likely to be focusing on this (67%), and yet these may be the very organizations that require additional help. There may be business to be won here, if MSPs can convincingly demonstrate the help they can provide.

Further, looking ahead, more than three-quarters (77%) are planning to increase their organization's level of investment in cybersecurity in the next 12 months. **This may present a golden opportunity for MSPs to help a wide range of organizations. However, this opportunity will not always be offered up on a platter for these service providers.** Organizations which don't currently use a managed service provider are less likely to be planning an increase in investment (60%), and so may require a bit more persuasion of the benefits of such a partnership.

This future investment is most likely to be driven by the need to reduce risk (52%), although 42% note the simple fact that more remote workers means they need more cybersecurity. But yet again, IT demonstrates they are more aware of these needs: **51% of decision makers in IT recognize the need for more cybersecurity, whereas only 32% of other BDMs say the same.** This further reinforces the point that BDMs are not always aware of the extent of the threats their organization is facing, and the need for better communication of cybersecurity needs and threats across the organization.

But the question remains, will organizations be directing these budget increases towards MSPs? There are issues that may make organizations less likely to do this. Reliability is a growing problem (with 43% reporting such issues with their MSP in 2021, compared to 35% in 2020), and one that will potentially expose their organization to threats.

Service providers need to demonstrate their reliability in order to fight this perception, as they aim to attract new business and ensure budgets aren't directed elsewhere.

Nonetheless, there is cause for optimism: just 12% report inadequate cybersecurity protections as a challenge for using a managed service provider. This is down from 23% in 2020, demonstrating that MSPs are more likely to be regarded as trusted providers of cybersecurity protections than they were 12 months ago. This is promising for IT service providers who are able to demonstrate their cybersecurity credentials, as SMBs are likely to turn to them for help. However, both organizations and their MSPs must ensure that once they have started working together, they are regularly discussing their cybersecurity needs, to leverage this relationship to best effect.

Fig 7: What is the biggest influence for your organization to invest more in cybersecurity? [541] Respondents from organizations which are planning to increase investment in cybersecurity in the next 12 months, not showing all answer options

Furthermore, benefits of IT services are reported such as better performance (55%) Increased security is the second most common benefit reported (58%). **SMBs clearly recognize the benefits of using a managed service provider – it is up to individual MSPs to demonstrate they can provide these benefits and help organizations with the issues they are facing, to ensure that they are chosen over their competitors.** And if they can do this, there is certainly opportunity in the market: as we have already seen, more than nine in ten (92%) respondents say their organization might consider moving to a new IT service provider if they offered the "right" cybersecurity solution, and organizations would be prepared to pay 34% more on average for this "right" solution.

Organizations may be driven to spend more on cybersecurity for a number of reasons: a rise in suspicious activity on their network (46%) or a cybersecurity attack (45%) are most likely to be reported. But it is also worth noting that 42% may spend more as a result of concerns about the suitability of their cybersecurity protections for the remote workforce – with IT decision makers in particular highlighting this as a factor (46%). With budget commonly available for solutions which can demonstrate the abilities to help defend against cybersecurity threats in a time of heightened risk, the case is clear for managed IT service providers: with the right cybersecurity credentials the opportunity for growth in the SMB market is there for the taking.

CONCLUSION

We are in the midst of a period of heightened risk for SMBs when it comes to cybersecurity. Attacks are increasing in frequency, and in the devastation they cause, yet few are confident in their ability to deal with them. Action is required, and fast, if they are to protect against enormous damage to business operation, profits and reputation.

However, dealing with these threats in 2021 is far from easy; there are numerous challenges making the situation even more difficult. In an era of competing priorities, when the pressure is on to innovate in all areas, and to ensure business continuity during an economic downturn, it is increasingly difficult for SMBs to devote the time and attention required to bolstering their cybersecurity protections. Further complicating the situation is the increase in remote workers, adding complexity to the working environment, and a culture of poor communication over cybersecurity needs improving both within organizations, and between SMBs and their MSPs.

Nonetheless, the picture is not all bleak. SMBs who are using a managed IT service provider they plan to stay with tend to be performing better in multiple ways compared to those who plan to change their MSP, or who don't have one at all. The benefits which can be provided by a well-equipped managed IT service provider are clear to see. SMBs are willing to move to providers which can provide these benefits, and they're willing to increase their spending in order to do so.

In order for MSPs to capitalize on this opportunity in the market, they must demonstrate they are capable of, and have the necessary skillset, to address security concerns and manage incidents in the current cybersecurity environment. MSPs must also be able to reassure organizations that they can protect a remote workforce, but also be proactive in speaking to their clients regularly to ensure they have the sufficient cybersecurity protection. There is a huge opportunity for managed IT service providers to grow their market share, but they need to demonstrate the cybersecurity understanding and capabilities to do so.

THE FINAL WORD

The Final Word from Wes Spencer, VP and External CISO for ConnectWise

The past three years have changed everything about the way MSPs think, operate, sell, service, and protect their clients. The status quo is forever changed; cybersecurity is truly a top risk area that even the smallest of organizations must now grapple with. While security may seem like an expensive and mystic dark art doomed to fail, the truth is that there is both a path forward and an opportunity for a brighter future and more revenue.

The data from this report simply jumps off the page. The time for action is past due, and all MSPs must adapt, enhance, and take control of cybersecurity as never before. Fortunately for our readers, there is another great hope that stands to our benefit.

You do not have to pioneer this journey alone.

Wes Spencer, VP and External CISO for ConnectWise

METHODOLOGY

ConnectWise commissioned Vanson Bourne to undertake research on the topic of cybersecurity in SMBs. Between March and April 2021, a quantitative study was carried out, interviewing 700 IT and business decision makers who have influence on decision making for cybersecurity in their organization.

In 2021 and 2020, respondents came from the US (300), the UK (150), Canada (100), Australia and New Zealand (150), from organizations with 10–1,000 employees, across a range of sectors. In 2019, respondents came from the US (300), UK (150), France (150), Germany (150) and Belgium (100), from organizations with 10–1,000 employees, across a range of sectors. The differences in the markets interviewed in may have factored into any differences in the statistics from this year.

Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

About ConnectWise

CONNECTWISE

ConnectWise is an IT software company that empowers Technology Solution Providers to achieve success in their As-a-Service business with intelligent software, expert services, an immersive IT community, and a vast ecosystem of integrations. The unmatched flexibility of the ConnectWise platform fuels profitable, long-term growth for our Partners. With an innovative, integrated, and security-centric platform, ConnectWise enables TSPs to drive business efficiency with business automation, IT documentation, and data management capabilities. And increase revenue using remote monitoring, security, and backup disaster recovery technologies.

For more information, visit 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 VansonBourne.com.