



CONNECTWISE™

CONNECTWISE
EBOOK SERIES

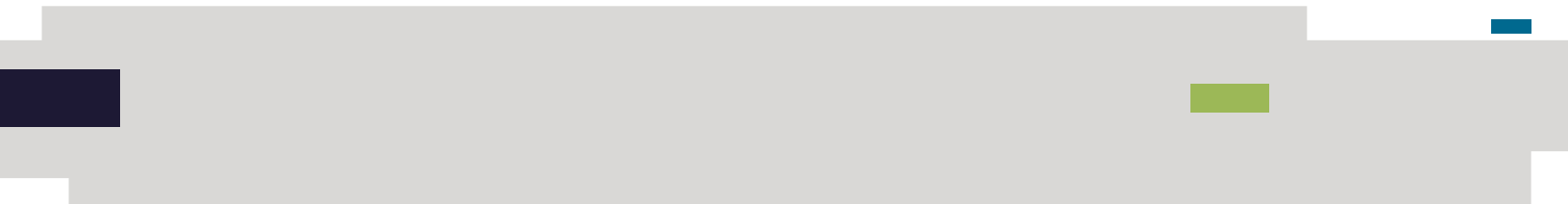
Underserved and Unprepared:

THE STATE OF SMB
CYBERSECURITY IN 2019



CONTENTS

Executive Summary	3
Key Findings	4
Methodology	5
Current State of Cybersecurity for SMBs	6
Security Outsourcing Trends in SMBs	10
Improving Cybersecurity for SMBs	13
Conclusion	15





EXECUTIVE SUMMARY

No business is too small to evade a cyberattack or data breach. Unfortunately, small and medium-sized businesses —SMBs— may lack the in-depth tools and in-house expertise to harden their systems and networks against potential threats.

In this survey of 850 global organizations with sizes ranging from 10 to 1,000 employees, 64% of respondents have reported that their organization has suffered a cyberattack. Cyberattacks among businesses of this size are becoming more and more commonplace, and the ramifications can be huge. What is more concerning, however, is that many of these organizations are not fully educated on what "good" security is. It is this lack of education and understanding that has led to lower levels of advanced protection within SMBs, which in turn leads to attacks on these businesses becoming more commonplace. It is important to establish the areas where SMBs need protection, and where there are potential pitfalls in order for managed IT service providers —MSPs— to appropriately support them. Cybersecurity

is a critical element to all organizations, and is potentially too important to remain solely within the organizations, especially bearing in mind the gaps in knowledge within SMBs. MSPs can provide this sought-after protection, but how are organizations working with them to achieve this? It is up to MSPs to ensure that organizations know what to expect from them, as well as who assumes responsibility in the event of a cybersecurity attack. MSPs should be working with their clients to ensure that they are educated on the evolving threat landscape and the solutions that are needed to stay protected, as well as the risks involved if a robust security strategy is not in place. Additionally, MSPs must offer their SMB clients a full portfolio of security solutions in order to reduce their risk levels and maintain proper protection.

This white paper identifies the following:

- SMBs' attitudes and concerns with cybersecurity
- SMBs' current protection levels
- SMBs' security expectations of their MSPs
- The risks and opportunities for MSPs



KEY FINDINGS

Protecting against cybersecurity attacks has become the highest priority for SMBs, both within the business and in terms of investment.

89%

see cybersecurity as the top or top five priority in their organization.

75%

agree that there should be more emphasis placed on security in their organization.

79%

of SMBs are planning to invest more in cyber security in the next 12 months.

The majority of SMBs find they are ill-equipped to deal with cyber attacks on their own.

62%

of SMBs agree they lack the in-house skills necessary to properly deal with security issues.

13%

who do not use an MSP feel confident in all cases that their organization would be able to defend itself during an attack.

52%

feel helpless to defend themselves from new forms of cyberattacks.

Cybersecurity has become a determining factor in whether an SMB is likely to use and continue to use an MSP.

SMBs that plan to change MSPs are more likely to have seen inadequate cybersecurity protections from their MSP —32%— compared to those who plan to stay with their current provider —25%—.

84%

who do not use an MSP would consider using one if they offered the "right" cybersecurity solution.

93%

would consider moving to a new MSP if they offered the "right" cybersecurity solution, even if they weren't planning to change.



METHODOLOGY

Independent technology market research specialist Vanson Bourne conducted and undertook the research that this report is based on, commissioned by Continuum.

Between January and March 2019, the quantitative study was carried out, interviewing 850 IT and business decision makers who have involvement in cyber security in their organization. Respondents came from the US (300), the UK (150), France (150), Germany (150) and Belgium (100). Respondents' organizations have between 10 and 1,000 employees and were from a range of sectors.

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

850

IT and business decision makers
involved in cybersecurity

5

Countries

10-1,000

Employee Organization

ANY

Sector



CURRENT STATE OF CYBERSECURITY FOR SMBS

Cybersecurity is a critical priority for organizations, with investment into this expected to increase in the near future.

45% of SMBs state that cybersecurity is currently critical to their business and is a top priority. And, 52% of respondents say that protecting against cyberattacks is one of their organization's biggest priorities in the next two years. What's more, the larger the organization, the higher this priority becomes (fig. 1).

Not only are organizations stating that cyber security is a top priority, they are planning to invest more into this area. Nearly eight in ten respondents report that their organization is planning to invest more in cybersecurity in the next 12 months. Those that use an MSP are also more likely to increase investment in cybersecurity for the next 12 months when compared with those that do not use an MSP at all (fig. 2).

Biggest priority for organizations in the next two years: protecting against cyberattacks

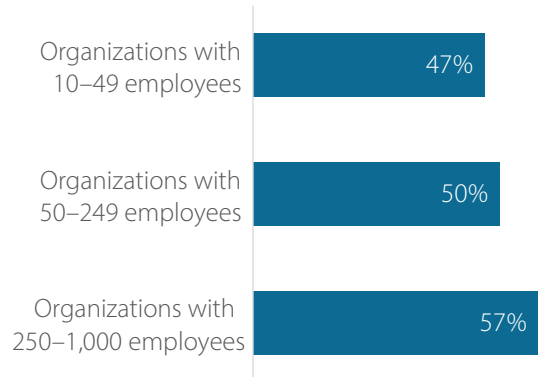


Figure 1: Analysis of respondents who say that protecting against cyber security attacks is a top-three priority for their organization in the next two years, split by organization size, asked to all respondents —base: 850—.

Organizations planning to invest more in cyber security for the next 12 months

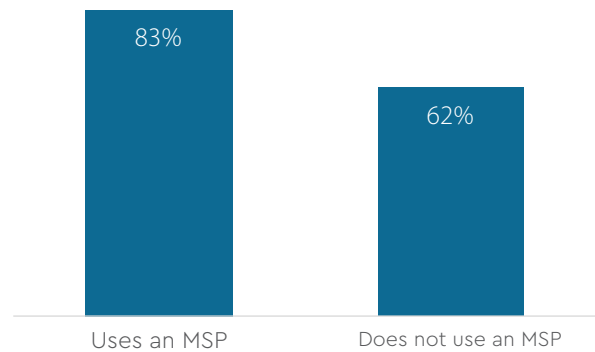


Figure 2: Analysis of respondents' organizations planning to invest more in cybersecurity for the next 12 months, not showing all answer options, split by whether organizations are using an MSP, asked to all respondents —base: 850—.



Security Concerns and Protections

Cybersecurity and the threat of cyberattacks are weighing on SMBs, causing a high level of concern for these organizations. 80% of SMBs are worried that they will be the target of a cyberattack in the next six months, and 75% of respondents think that there should be more emphasis placed on security in their organization.

When it comes to the concerns SMBs have in the event of a cyberattack, the most common are data loss —50%—, customer loss —43%— and damage to company reputation —39%—. Around eight in ten SMBs are currently worried about customer data being breached —82%—, data being stolen from outside the organization —77%— and IT system—s— downtime/unavailability —77%—. Over three quarters —76%— are worried about customer-facing applications being breached.

Due to this high level of concern, SMBs feel the need to protect nearly every aspect of their business. The majority of SMBs want to protect company finances, customer data, customer-facing applications, HR records and employee data and internal applications —fig. 3—. This highlights the high importance these businesses see cybersecurity having to their critical data.

Level of protection organizations would be comfortable with for various types of data

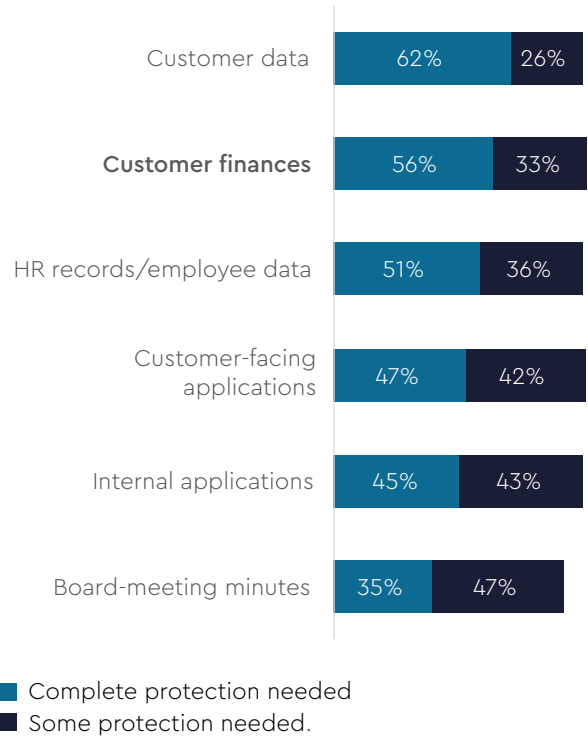


Figure 3: Analysis of the level of protection that organizations would be comfortable with for various types of data, not showing all answer options, asked to all respondents —base: 850—.

80% of SMBs are worried that they will be the target of a cyber attack in the next six months.



However, there still exists a disparity between SMBs' desired level of protection and their current level of protection. Less than two in five respondents feel that customer data —37%—, internal data —38%— and internal applications —38%— are very well protected against cybersecurity attacks in their organization, and only a third —33%— say the same for customer facing applications. This is also the case in terms of data being breached, with less than four in ten saying they are very well protected against data being stolen from inside the organization —36%— or outside the organization —37%—.

Many SMBs do not feel confident in their ability to defend against cyberattacks on their own because there is a gap in both their security skills and solutions. More than six in ten SMBs agree that they lack the skills in-house to deal with security issues and around half say their organization feels helpless to defend themselves from new forms of cyberattack. To add to this, there are gaps in comprehensive coverage when it comes to security.

Around half of SMBs do not currently have specific cybersecurity experts in their organization —56%—, incidence response planning in the event of a cyber attack —52%— or cybersecurity insurance —51%— —fig. 4—. Smaller organizations are also less likely to have these three protections in place, particularly in the case of in-house experts—six in ten —60%— SMBs with 10–49 employees do not currently have security experts, compared with half —51%— of those with 250–1,000 employees.

Security solutions that organizations do not currently have

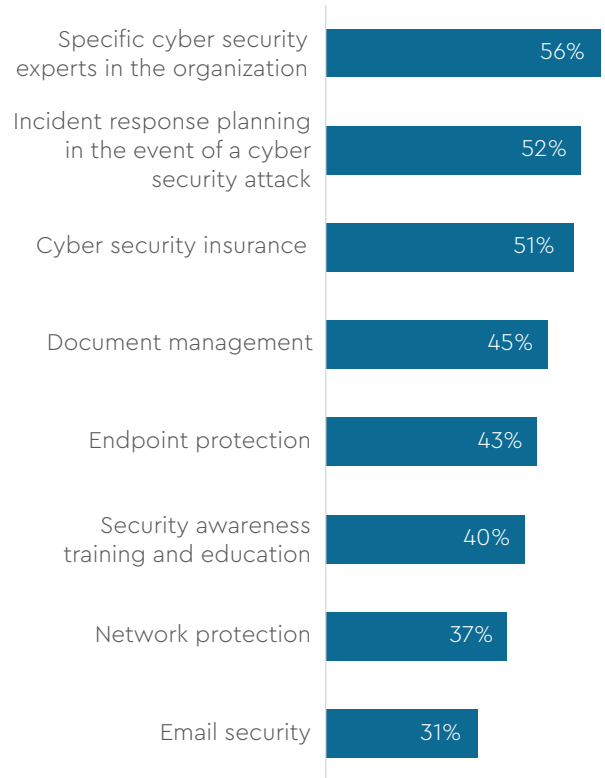


Figure 4: Analysis of security solutions that respondents' organizations do not currently have, not showing all answer options, asked to all respondents —base: 850—.



From the results, it is clear that SMBs have yet to realize what good, comprehensive security entails. Even though most organizations claim to have basics like email security and network protection, around a third do not currently have these protections in place. Without these critical elements, SMBs are putting their organization at considerable risk, particularly in the event of a cyberattack.

Impact of Cybersecurity Attacks

Cyberattacks have become commonplace for the majority of SMBs, with the impacts and costs being significant. Almost two thirds of respondents' organizations have suffered a cyberattack and around a third have experienced at least one in the last 12 months. Of organizations who have suffered an attack, only 2% claim there was no impact to their business. For the remaining majority that were impacted by a cyberattack, the most common include cost in terms of money —35%—, cost in terms of time/effort in dealing with the issue —33%— and data loss —32%— —fig. 5—.

Respondents that say their organization was affected by cost due to a cyberattack report a total business cost of \$53,987, on average. What's more, the larger the organization, the higher this cost becomes. SMBs that have between 250–1,000 employees report a higher business cost —\$64,085—, on average, than those with 50–249 employees —\$48,686—, or 10–49 employees —\$41,269—.

With significant costs such as these, it highlights the importance for SMBs to strengthen their cyber protections and reduce the risk of attack against their business.

Impact of cyberattack(s) on organizations

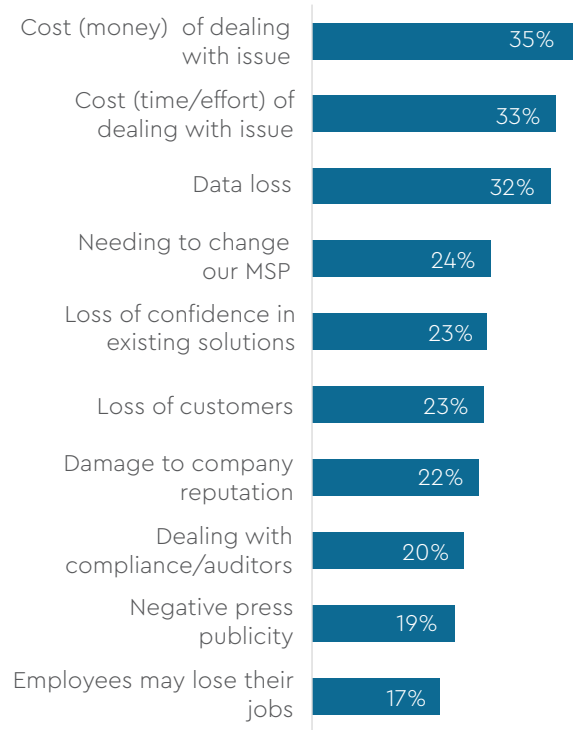


Figure 5: "What has been the impact of cybersecurity attack—s— on your organization?", not showing all answer options, asked to respondents whose organization has suffered a cyberattack —base: 548—.



SECURITY OUTSOURCING TRENDS IN SMBS

Most organizations recognize that they are unable to take on the task of dealing with security alone, and because of this, most have turned to using an MSP.

Over eight in ten surveyed SMBs are using an MSP, with around half planning to continue with their current provider —fig. 6—. Three in ten plan to change to a different provider in the near future, while 12% who don't currently use an MSP plan to start doing so within the next year. Of SMBs who use an MSP, 45% report that their organization currently outsources all or the majority of their IT services. This jumps to 57% when looking at the same group that currently outsources all or the majority of their cybersecurity, further suggesting that SMBs recognize cybersecurity as a critical area that needs to be supported by third party resources and expertise. What's more, access to security resources and expertise will remain important to SMBs' future plans for outsourcing, with almost six in ten SMBs reporting that the majority or all of their organizations' cybersecurity will be outsourced in five years' time.

Organizations' use of an MSP

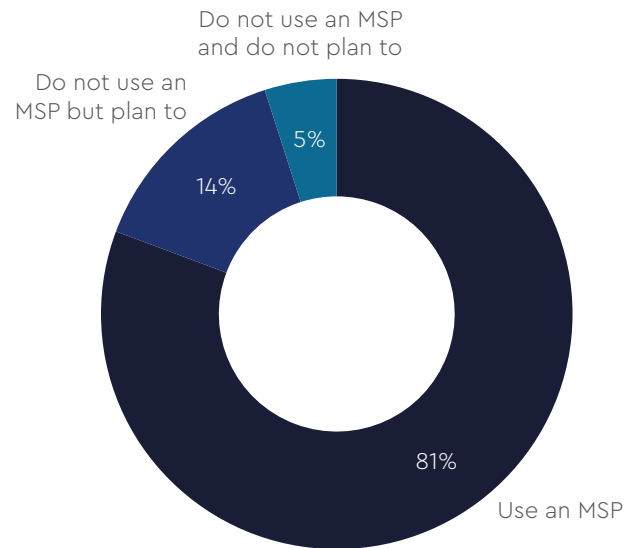


Figure 6: "Is your organization using an MSP?" not showing all answer options, asked to all respondents —base: 850—.

51%

plan to continue with their current MSP.

29%

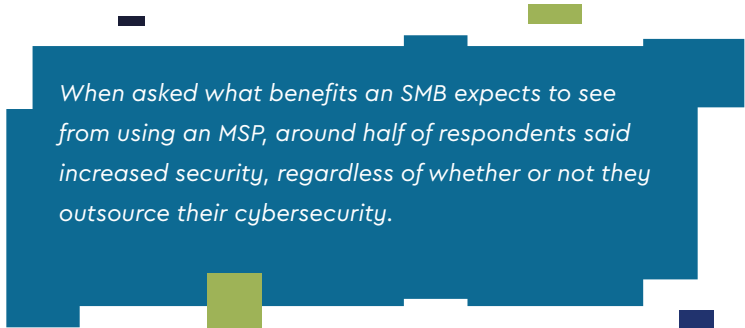
plan to change to a different MSP in the near future.



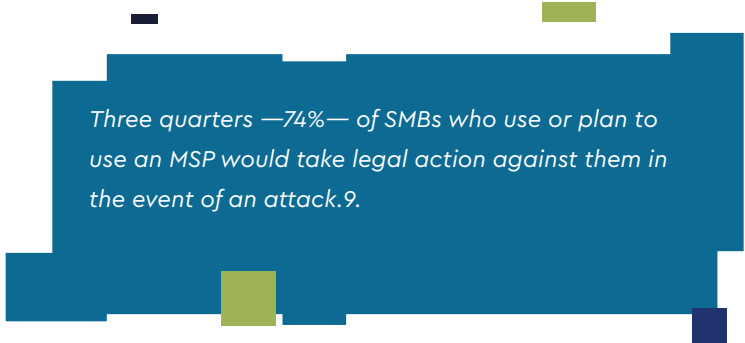
SMB Security Expectations

When asked what benefits an SMB expects to see from using an MSP, around half of respondents said increased security, regardless of whether or not they outsource their cybersecurity. Organizations that outsource half, the majority or all of their cybersecurity to MSPs expect the benefit of increased security —54%, 53% and 47%, respectively—. Coincidentally, organizations that outsource the minority or none of their cybersecurity also expect to see increased security from using an MSP —56% and 48%, respectively—.

It is clear that SMBs have high expectations of the benefits of using an MSP, but also in terms of who is liable in the event of a cyberattack. Of those that use an MSP, 69% claim they would hold their MSP accountable at some level in the event of an attack, with 35% saying they would hold their MSP solely accountable. Three quarters —74%— of SMBs who use or plan to use an MSP would take legal action against them in the event of an attack, while 38% report they expect their MSP to have complete accountability for legal issues in the event of a security issue. This emphasizes the importance for MSPs to not only provide their SMB clients with sufficient and robust protection, but also properly set expectations as it pertains to responsibility and liability in the event of a cyberattack.



When asked what benefits an SMB expects to see from using an MSP, around half of respondents said increased security, regardless of whether or not they outsource their cybersecurity.



Three quarters —74%— of SMBs who use or plan to use an MSP would take legal action against them in the event of an attack.⁹



Risks of Not Meeting SMB Security Expectations

Cybersecurity is a major factor in whether an SMB is likely to use, continue to use or change their MSP. Seeing as most organizations expect increased security from their MSP, when this expectation is not met, providers could risk losing those organizations' business.

SMBs that plan to change MSPs are more likely —32%— to have seen or to expect inadequate cybersecurity protections from using an MSP when compared with those that plan to stay with their current provider —25%—. Respondents from organizations that are planning to change MSPs are more likely —17%— to lack confidence in their providers' ability to defend the organization from a cyberattack, compared to those that are planning to stay with their current provider —7%—. Additionally, SMBs that plan to change their MSP have fewer conversations with their provider about their organizations' security —32 times per year, on average—, compared to those that plan to stay with their current provider —40 times per year, on average—. This highlights the risk MSPs face if they do not regularly communicate with SMBs about cybersecurity and the protections they are providing.

One of the biggest risks to an MSP's business is when its clients are hit by a cyberattack. Nearly a quarter of respondents whose organization suffered a cyberattack needed to change their MSP/IT solutions as a result of the attack.

SMBs will not hesitate to change providers for the "right" cybersecurity offering and they are prepared to pay more to do so

SMBs will not hesitate to change providers for the "right" cybersecurity offering. Even for respondents that say their organization plans to stay with their current provider, 93% would consider moving to a new MSP if they offered the "right" cybersecurity solution. And not only are SMBs willing to change IT service providers for this new offering, they are prepared to pay more to do so. On average, respondents' organizations who are using an MSP and could consider moving to a new one claim they are willing to pay 25% more per year to receive the "right" solution from a new provider. And, this average is consistent across SMBs of all sizes —fig. 7—.

How much more organizations would be willing to pay a new MSP for the "right" cybersecurity solution per year



Figure 7: Analysis of how much more an organization would be willing to pay a new MSP for the "right" cybersecurity solution per year —average—, split by size of organization, asked to respondents whose organization would consider using/moving to a new MSP if they offered the "right" solution and is using an MSP —base: 643—.



IMPROVING CYBERSECURITY FOR SMBS

When security is done properly by MSPs, SMBs can enjoy a better sense of protection through leveraging their provider's solutions, knowledge and expertise.

Organizations that use an MSP and plan to stay with their current provider are more likely to say that customer data and internal data are very well protected against being breached —47% and 46%, respectively— than those that use an MSP but plan to change to a different provider —27% and 31%, respectively— or those that don't use an MSP at all —26% and 28%, respectively— —fig. 8—.

This stresses how important the MSP's role is in the protections they can offer an organization. Additionally, it emphasizes how educating SMBs on security best practices and what good security looks like can help increase that organization's sense of protection.

More and more SMBs are now realizing the benefits an MSP can offer their organization—almost eight in ten SMBs anticipate that at least half of their cybersecurity will be outsourced in five years' time, and almost six in ten expect all or the majority will be outsourced in that time. And for organizations who currently outsource the minority of their cyber security, 59% anticipate this to increase to half or more, presenting a significant revenue opportunity for providers in the SMB security space.

Impact of cyberattack(s) on organizations

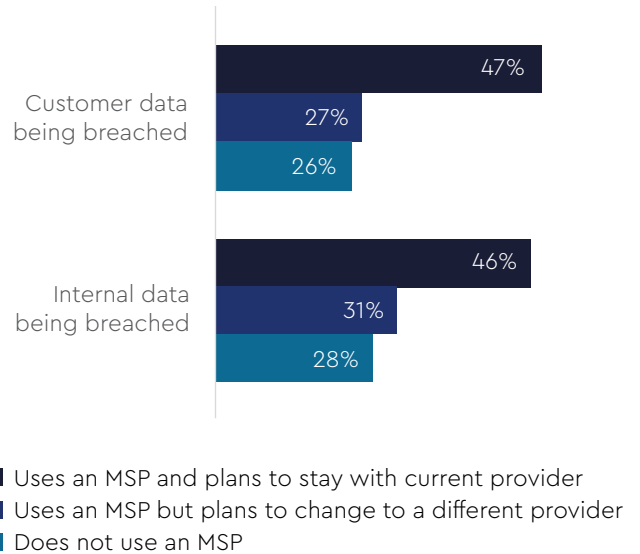


Figure 8: Analysis of elements that respondents feel are very well protected in their organization against cybersecurity attacks, not showing all answer options, asked to all respondents —base: 850—.



What SMBs Need

In order to ensure security is correctly managed, organizations need to regularly discuss security needs with their MSP and take full advantage of their skills and resources. Six in ten —62%— respondents report that their organization lacks the skills in-house to be able to properly deal with security issues, while only four in ten —41%— currently have specific cybersecurity “experts” in the organization. However, organizations are heading in the right direction, with 45% saying they plan to add these experts in the future.

SMBs will not hesitate to change providers for the “right” cybersecurity offering and they are prepared to pay more to do so

It is also essential that SMBs define and implement a recovery plan in the event of a cyberattack. Less than half —46%— of organizations currently have an incidence response plan, and a smaller proportion —45%— have cybersecurity insurance. Bearing in mind the amount of SMBs that have experienced a cyberattack-and the worry that many are feeling -more should be done to ensure these organizations are not only able to prevent an attack, but recover from one when necessary.

What MSPs Can Offer

With more than half of organizations prioritizing cybersecurity in the next two years and a significant proportion seeking out better protections, the SMB security space presents an important opportunity for IT service providers. While SMBs need to understand that there is no solution that will protect them entirely, providers can step in to better educate organizations on the nature of the threat landscape and the types of protections that should be implemented. Additionally, it is critical for MSPs to explain that cybersecurity is a shared responsibility between organizations and their providers, and by clearly defining service-level agreements —SLAs— from the onset of the relationship, MSPs can drastically reduce their risk of legal action against them. However, it is not enough to provide a basic security solution. Nine in ten —92%— respondents state their organization would consider moving to a new MSP if they offered the “right” cybersecurity solution, and of those respondents, they’d be willing to pay 25% more per year, on average. Since the “right” solution is up to the interpretation of the SMB, it emphasizes the importance for MSPs to offer a full portfolio of security solutions. Only then can providers properly address the range of SMB security needs and demonstrate that they have the right cybersecurity solution for these organizations.

Nine in ten —92%— respondents state their organization would consider moving to a new MSP if they offered the “right” cybersecurity solution and of those, they’d be willing to pay 25% more per year, on average.



CONCLUSION

Even though MSPs are being used by a large proportion of SMBs, cybersecurity is a key factor that affects the relationship between an MSP and their clients.

The importance of cybersecurity for organizations is clear, but IT and business decision makers are still worried that their organization will suffer a cyber attack. This is partly due to the disparity between where their organization's security currently is, and where they need it to be. Also, few organizations have recovery planning in place in the event of an attack, which emphasizes there is still a lot of work to be done within organizations.

The level of worry respondents are experiencing is justified, as cyberattacks can have huge ramifications for these organizations. However, as SMBs leverage the skills and solutions provided by MSPs, their organizations can experience increased security and higher levels of confidence. By offering comprehensive cybersecurity, MSPs can play a key role in filling gaps in coverage and ensuring SMBs are sufficiently protected against cyberattacks. At the same time, they must also inform and educate organizations

on what they are protected against and discuss their security needs on a regular basis.

The cybersecurity solutions that an MSP offers are crucial to their success in retaining their current clients and winning new business. Organizations need to recognize that in order to achieve the best possible security protection, it is not necessary to undertake it alone-effective help is available from MSPs.

MSPs should embrace this opportunity to offer cybersecurity services to SMBs. As highlighted in the results, these organizations recognize that they do not have the advanced solutions and skills they require, and they are willing to pay more for a security solution that fulfills these needs. However, MSPs need to be clear when it comes to liability and responsibility in the event of an attack, which can be addressed with the right combination of education, awareness and clearly defined SLAs.

Both SMBs and MSPs need to realize that the threat landscape is dynamic, and in response, security technologies and strategies must continually evolve in order to remain effective.