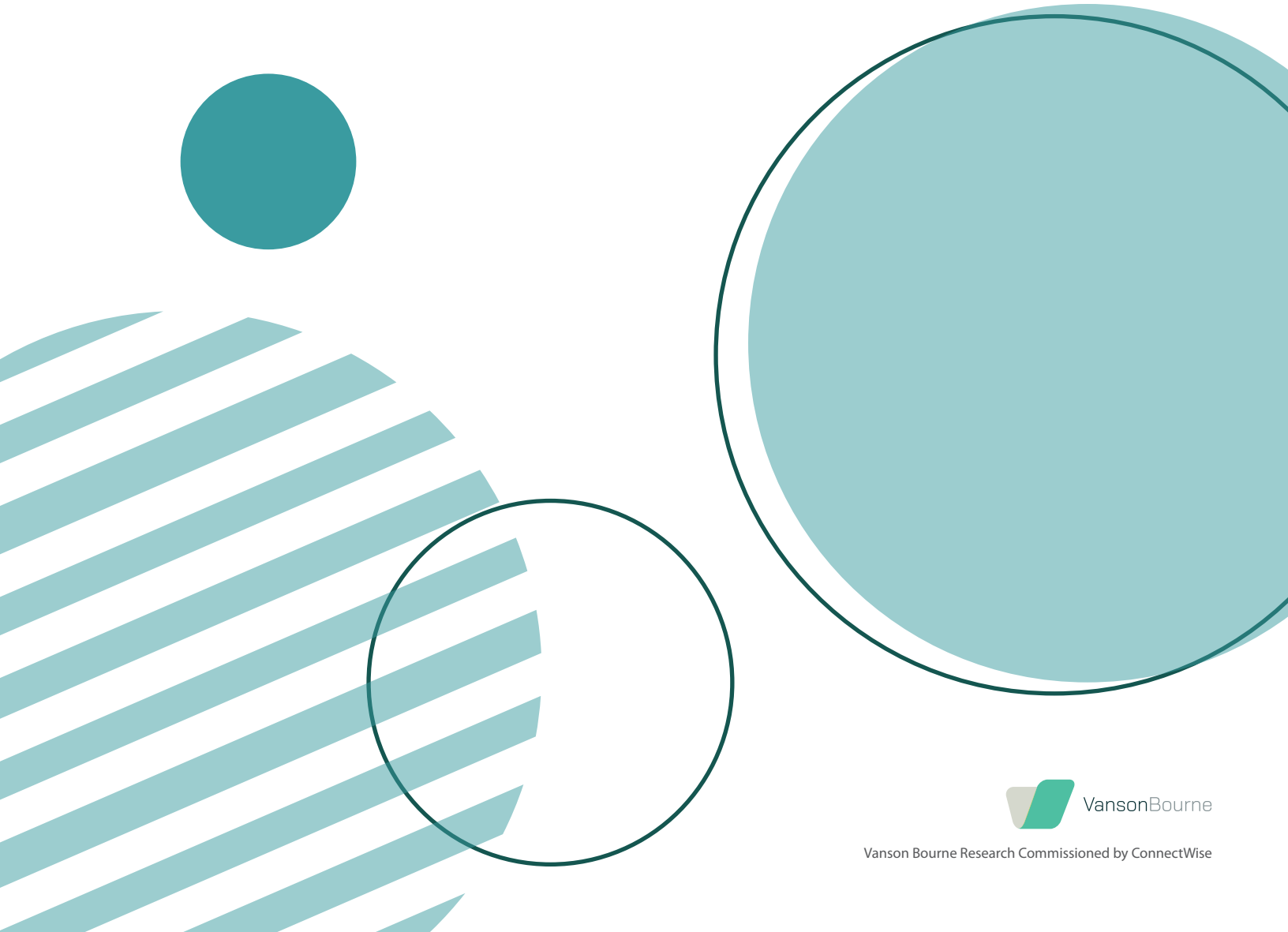
ConnectWise®

Creating Opportunity from Adversity

The State of SMB Cybersecurity in 2020



VansonBourne

Vanson Bourne Research Commissioned by ConnectWise

Contents

Executive Summary

2020 stands apart as a year where the entire world shared a crisis unparalleled in recent memory. Technology infrastructure was tested to the limit, and managed service providers (MSPs) around the world over went above and beyond to support their customers as they built their 'new normal'.

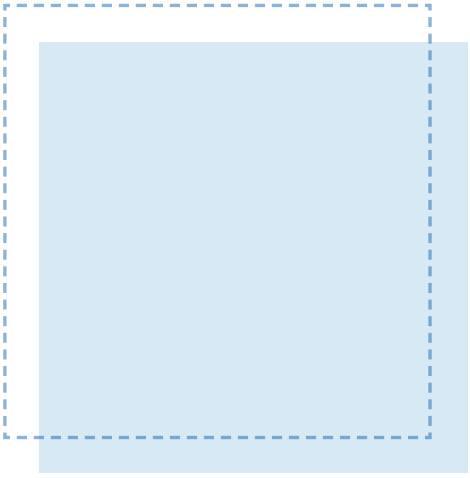
Despite huge challenges, many organizations remained focused on core technology priorities. In this survey of 700 SMB decision makers, cybersecurity continues to be top of mind for nearly every participant. That perhaps explains why over three quarters are worried they will be the target of an attack in the next 6 months.

As a result, the majority of SMBs are planning further investment in cybersecurity during the next year in an effort to reduce risk.

However, more than half recognize their organization lacks the in-house skills needed to properly deal with cybersecurity challenges. This is helping to drive the growing adoption of outsourced security, giving MSPs the opportunity to build additional revenue streams and deepen their relationships with existing customers. Despite facing unique challenges, SMBs remain fully committed to the role MSPs play in their organizations.

Nine out of ten SMBs said they would consider using an MSP or switching MSPs to find the 'right' cybersecurity solution, with the majority looking for a partner with the confidence to respond to security incidents. This sends a clear message to many MSPs that they must raise their understanding across the entire cybersecurity discipline - from technical and customer service capabilities to training, automation, and the ability to manage growth – including the ability to oversee a constantly expanding attack surface.

Those MSPs that take these steps will be strongly positioned to capitalize on a post-pandemic economic recovery, emerging from the experience stronger and more agile, and with customers better prepared for the cybersecurity challenges that lie ahead.



Key Findings

Cybersecurity continues to be top of mind across the SMB community—this is reflected in both perceived risk and investment planning:

86%
of SMBs report cybersecurity to be within the top five priorities for their organization and 38% say it is their top priority.

77%
of SMBs worry they will be the target of an attack in the next 6 months.

73%
of SMBs are planning to invest more or much more in cybersecurity in the next 12 months.

60%
of SMBs will invest more in cybersecurity because it reduces risk for their organization.

A widespread cybersecurity skills gap among SMBs is helping to drive the adoption of outsourced services:

52%
of SMBs agree they lack the in-house skills necessary to properly deal with security issues.

57%
of SMBs do not have specific cybersecurity experts in their organization.

59%
of SMBs believe that all or a majority of their cybersecurity needs will be outsourced in five years.

Only 43%
of SMBs are currently outsourcing all or the majority of their cybersecurity needs.

SMBs are focused on finding the 'right' offering, with many prepared to switch to a partner who can instill cybersecurity confidence:

91% of SMBs would consider using or moving to a new IT service provider if they offered the 'right' cybersecurity solution.

Confidence is a key factor for SMBs in choosing the 'right' offering – 68% of SMBs say the 'right' offering means confidence in an MSP's ability to respond to security incidents, while 58% say its confidence to minimize damage or loss.

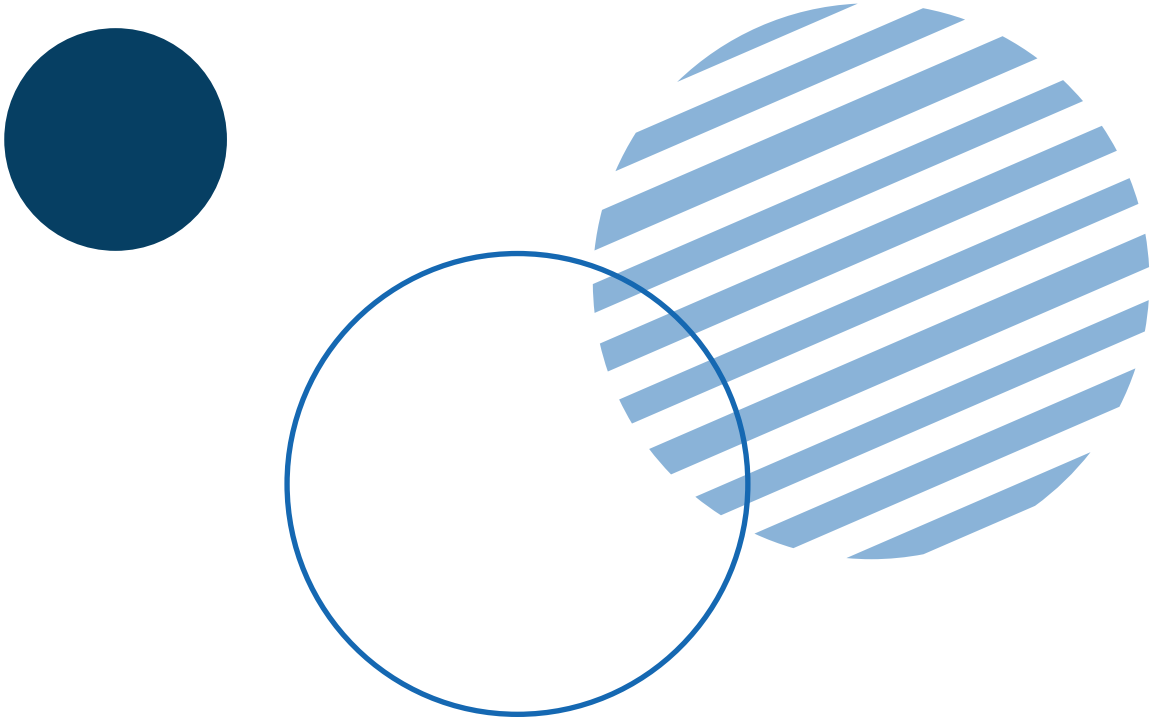
On average, SMBs that use an MSP would consider moving to a new IT service provider if they were offered the 'right' cybersecurity solution, **would be willing to pay 30% more for it.**

Methodology

Independent technology market research specialist Vanson Bourne conducted and undertook the research that this report is based on, commissioned by ConnectWise. Between June and July 2020, the quantitative study was carried out, interviewing 700 IT and business decision makers who have involvement in cybersecurity in their organization. Respondents came from the US (300), the UK (150), Canada (100), Australia and New Zealand (150). 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.

Comparative analysis is drawn from 2019's research data. The report can be found **here**. The previous research in 2019 was carried out in different countries from the 2020 research. In 2019, the countries we interviewed in were: US (300), UK (150), France (150), Germany (150), Belgium (100). In order to provide an accurate comparison, the report shows 2020 adapted figures, and 2019 adapted figures – this means that the adapted figures may be different from the total figures for all countries in both 2019 and 2020.

We've identified the adapted comparative data between the 2019 and 2020 findings with an asterisk throughout this white paper.



The State of Cybersecurity among SMBs

Cybersecurity continues to hold a high position of importance among SMBs worldwide: 86% of respondents say it sits within the top five priorities for their organization and 38% say it is their top priority.

From our research in 2019, it was clear that SMBs recognized cybersecurity as important, but lacked the tools, services, and expertise to properly defend themselves. This year, SMBs are becoming more aware of the key role played by cybersecurity and what is required in order to protect their organization: over half (59%) strongly agree that cybersecurity should encompass all aspects of their organization, compared to 46% strongly agreeing with that claim last year. *

As a result, SMB cybersecurity investment plans have remained broadly unchanged, despite the wider economic challenges brought about by the COVID-19 pandemic. Specifically, 74% of SMBs are planning to invest more or much more in cybersecurity in the next 12 months, and 23% say they will invest the same in cybersecurity this year. When compared with last year, we saw a higher percentage of SMBs wanting to invest more and much more in cybersecurity in 2019. This tapering off might suggest that SMBs are becoming more satisfied with the cybersecurity investments they have made in the past year, therefore more will retain their current level of investment.

Cybersecurity investment planning for the next 12 months

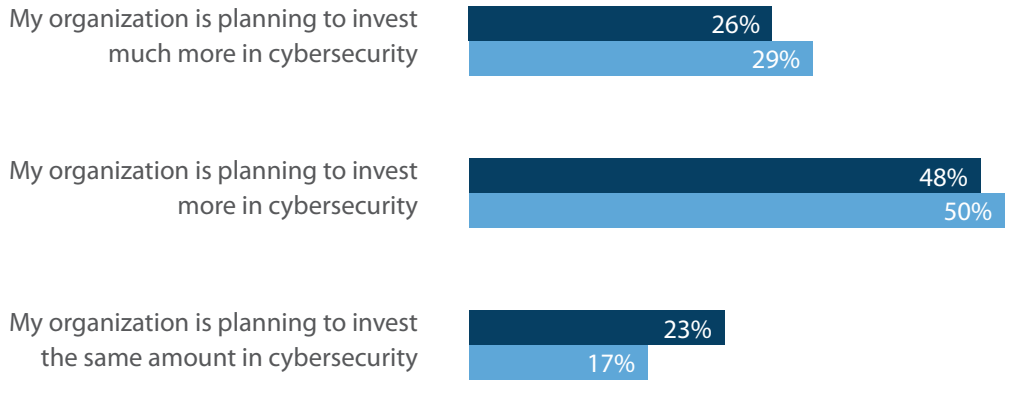


Figure 1: Analysis of respondents' organizations level of investment in cybersecurity for the next 12 months, not showing all answer options, split by year, asked to all respondents (base: 700)

Despite the importance attached to cybersecurity, the investments that SMBs are making are mostly at a basic, foundational level. 71% of SMBs have only foundational cybersecurity protections (such as firewall, antivirus, etc.). When asked if they currently have advanced endpoint protection and advanced network protection, that percentage drops to 47% and 53%, respectively.

Foundational protections are more common for SMBs who are not currently working with an MSP compared to those who are (77% vs. 69%, respectively). In addition, those SMBs that use an MSP are much more likely to have these advanced protections in place than SMBs that do not use an MSP.

What's more, there remains a perennial underlying problem that, arguably, only MSPs are able to address: **52% of SMBs say they lack the in-house skills needed to properly deal with security issues,** and only 41% of SMBs have specific cybersecurity experts in their organization yet still struggle with the cybersecurity skills gap.

So how can MSPs address this? The research reveals that 62% of SMBs expect increased security as a benefit of working with an MSP. And 49% of SMBs find more expertise as an added benefit of working with an MSP—hinting at how SMBs are seeking out MSPs to help close the skills gap. Additionally, MSPs can help SMBs deepen their cybersecurity protections. The respondents that use an MSP are much more likely to have deeper, more advanced protections in place than SMBs that do not use an MSP.

However, MSPs also need to be aware that increasing costs are a greater challenge for SMBs compared to last year. Thirty-six percent of SMBs see increased costs as a challenge of using an MSP, compared to 30% saying the same last year. *

Assessing the Impact of COVID-19 on SMB Cybersecurity

26% of respondents have experienced a positive business impact as a result of COVID-19, while 70% have experienced a negative impact. But regardless of its effect, COVID-19 has made little impact on the value SMBs place on cybersecurity, and it remains in the top five priorities for nearly all respondents. Of the SMBs who have experienced a negative impact from COVID-19, 86% list cybersecurity as a top or top five priority for their organization. This is similar for SMBs who have reported a positive impact.

Yet COVID-19 has brought new concerns for SMBs, particularly as it relates to remote environments. **79% of SMBs are worried about their remote devices or remote employees being breached**. And 42% of SMBs claim to be investing more in cybersecurity due to the fact that they have more employees working remotely. While remote work may be a new frontier for SMBs, respondents expect that, on average, 33% of their workforce will be fully remote in 12 months' time—presenting a new opportunity for MSPs.

The Impact of Security Incidents on SMBs

55% of SMBs have reported suffering a cyberattack, and the impact is considerable. The average cost of an attack has grown from last year, when it stood at $50,865, compared to this year where it has risen to $58,902—an increase of nearly 16%. * And the larger the size of the SMB, the more significant this cost becomes.

Total business cost of cyberattack(s)

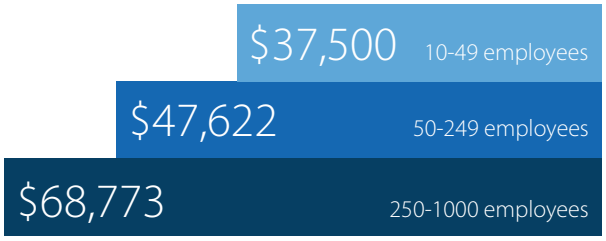


Figure 2: "What is the total business cost of cybersecurity attack(s) that your organization has experienced in the last two years?", showing averages (excluding outliers) in USD split by organization size, asked to respondents whose organization experienced a cost-associated impact from a cybersecurity incident (base: 247)

The cost of a cyberattack is the most common impact across SMBs in all regions, except when it comes to those in the US. These respondents are more likely to cite data loss as the most common impact from a security incident. The same goes when looking at size of the SMB: larger SMBs are more likely to cite data loss as the most common impact of a cybersecurity incident, compared to smaller and mid-sized SMBs who say cost was the most common impact.

When it comes to concerns that respondents have in the event of a cyberattack, these vary depending on geo-location and respondent type. For example, SMBs in the UK say damage to company reputation is their biggest concern in the event of a cyberattack, whereas all other regions cite data loss as the key concern. Additionally, IT decision-makers are more likely to cite damage to company reputation and bad press/publicity as concerns compared to business decision-makers. This highlights the individual differences that factor into fear.

Another growing trend is the importance SMBs attach to the possibility and impact of being breached. This year, 44% of SMBs respondents say they are extremely worried about customer data being breached, compared to only 29% last year; 34% are extremely worried about internal data being breached, compared to 22% last year; 31% are extremely worried about the increased cost of a cyberattack, compared to 24% last year; and 33% are extremely worried about the legal ramifications of a cyberattack, compared to 29% last year. *

Consequences for Incumbent MSPs

Accountability for cyberattacks has become more balanced compared to 12 months ago. This year, 56% of SMBs would hold both their provider and themselves accountable in the event of a cyberattack, compared to 39% saying so last year. What's more, last year 33% of SMBs said they would hold their MSP solely accountable, whereas that has dropped slightly to 24% this year. *

However, 62% of SMBs would still take legal action against their MSP in the event of a cyberattack, compared to 66% last year. * Whatever the concerns and real-world impact of security incidents, the bottom line for MSPs is that 27% of SMBs have fired their security provider after suffering a cyberattack. **Cybersecurity expertise—or more importantly, the lack of it—can have serious consequences for MSPs in an increasingly competitive market.**

The Opportunity for MSPs: Being the 'Right' Provider

SMBs retain a strong commitment towards cybersecurity, offering a clear and growing market opportunity for MSPs to build or expand their cybersecurity practices.

50% of respondents are investing more in cybersecurity because they see its value. What's more, **SMBs clearly believe in the current and future importance of managed services**, with 59% of them predicting that all or the majority of cybersecurity activities will be outsourced in five years. Yet only 43% of SMBs are currently outsourcing all or the majority of their cybersecurity to a third party, giving MSPs considerable opportunities to build additional market presence.

There is also considerable scope for MSPs to provide more comprehensive cybersecurity solutions to the SMB market. SMBs who do not currently partner with an MSP are less likely to have advanced endpoint protection, advanced network protection, security awareness training, and a security incident response plan—all of which are services MSPs can and should provide.

Partnering with an MSP makes SMBs feel more confident that they are protected. SMBs who partner with an MSP are more likely to feel very well protected against customer data being breached, internal data being breached, as well as remote devices/employees being breached. Without the expertise of an MSP, SMBs feel the limit of their own abilities. Of SMBs who do not use an MSP, only 6% feel confident in all cases that they would be able to defend themselves during a cyberattack. Furthermore, confidence in an MSP is a key factor in an SMB's decision to continue working with their provider. Of those who are working with an MSP but plan to change their provider, only 9% feel confident in their provider's ability to protect them against cyberattacks in all cases, compared to almost 30% for those who plan to stay with their current provider.

It's clear that MSPs must work to reinforce that confidence and build closer relationships with their cybersecurity clients. **Only 13% of SMBs are having regular cybersecurity-related conversations with their MSP**. For 38% of SMBs, these conversations are triggered only by a quarterly review, and a further 35% of SMBs only have these conversations during an annual review. Even more worrisome is that fact that 29% of SMBs talk to their MSP about cybersecurity only after they have suffered an incident.

What Do SMBs Look for in the 'Right' Cybersecurity Solution?

Nine in ten (91%) SMBs would consider using or moving to a new MSP if they had the 'right' cybersecurity offering. But what does that 'right' cybersecurity solution look like to SMBs?

The most important factor that SMBs weigh when looking at a cybersecurity offering is confidence in its ability to respond to security incidents. Other influential factors include the confidence in its ability to minimize damage, price of offering and certifications of resources—proving that SMBs are looking beyond the mere tools of an offering, and instead to an MSP's ability, expertise, and trust factor.

Wherever individual priorities lie, SMBs that use an MSP would be willing to pay a new provider, 30% more on average for the 'right' cybersecurity offering. This has increased compared to last year when SMBs were willing to pay an average of 26% more. *

The larger the organization, the less important the price of the offering becomes. For larger SMBs (250-1000 employees), capabilities/certifications of resources is more commonly considered an important factor in the 'right' solution than the price of offering (52% vs. 44%). There are also slight differences based on geographical location.

Conclusion

The context of this annual study typically sets out key economic, business and technology trends, their impact on SMBs, and the cybersecurity choices they make. But this year is unique in the experience of anyone taking part or studying the findings.

COVID-19 has brought huge disruption and uncertainty to every country, industry, business, and many millions of hard-working people. Many important issues have taken a back seat as society works through its current challenges and looks more positively to the future.

But in the case of cybersecurity, what we have seen is a discipline that has become truly strategic across the SMB landscape. It has proven resilient to global economic downturn, retaining the support, commitment, and investment of business and IT leaders.

MSPs are uniquely positioned to protect these businesses against the growing sophistication, volume, and impact of today's cybersecurity threats. There is considerable opportunity for growth among both existing and new customers for those who can shape their proposition and service delivery to the evolving needs of SMBs.

However, customer expectations are growing, and MSPs would be naive to assume that standard, 'off-the-shelf' cybersecurity services will satisfy the requirements of increasingly sophisticated SMBs. Deep expertise and tailored products backed by attentive customer service hold the key to building confidence in SMBs in the years to come.

About ConnectWise

ConnectWise is an IT software company empowering Technology Solution Providers to achieve their vision of 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. Visit ConnectWise.com.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis, is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets.

ConnectWise ® I 4110 George Rd., Suite 200, Tampa, FL 33634, USA

Research Conducted By: Vanson Bourne