Action1

2022 SMB IT Security Needs Report

June 2022

Contents

About this Report

Early in the pandemic, the need to quickly shift to remote work caused SMBs to flock to MSPs in droves. However, amidst today's rising inflation and macroeconomic crisis, SMBs will consider their choice of an IT provider more carefully, with close attention to balancing costs and benefits. Therefore, MSPs cannot expect new business opportunities to simply fall into their laps.

Accordingly, to stay competitive, MSPs should take a step back and analyze the changing needs and expectations of SMBs. What are their top cybersecurity challenges? How strong do they think their IT security is now? How satisfied are they with their current MSPs, and what issues would lead them to consider moving to another one?

To help MSPs strengthen their offerings in 2022 and beyond, we posed these and related questions to 750 SMBs from North America, Europe, and APAC, and compiled the results into this report.

Amidst today's rising inflation and macroeconomic crisis, SMBs will consider their choice of an IT provider more carefully, with close attention to balancing costs and benefits.

Key Findings

The report provides insight into SMBs that can help MSPs serve their customers more effectively. We found:

- **SMBs' lack of preparedness for cybersecurity challenges represents a huge opportunity for MSPs.** Half of SMBs (52%) acknowledge that they lack sufficient skills and technology to effectively protect their organization against escalating cyber threats. Indeed, most SMBs fail to assess their IT risks adequately and generally underestimate how heavily cybercriminals target smaller organizations. 63% of respondents think that their SMB is at less cyber risk than large enterprises — but in fact, 81% of the SMBs surveyed experienced at least one security incident during the preceding 12 months. Moreover, SMBs struggle to locate and implement effective security tools themselves. 65% of respondents said that the cost of most cybersecurity solutions prevents them from building a robust security posture, and 37% noted that their existing security controls are problematic because they hurt employee productivity. Taken together, these findings offer MSPs a solid business strategy: By providing SMBs with cost-effective technologies and expertise for protection against escalating cyberattacks, MSPs can be poised for strong growth.

- **Despite budget constraints, most SMBs plan to increase their IT security spending, which further indicates that cybersecurity is a lucrative business opportunity for MSPs.** In fact, 80% of SMBs said their IT security budget grew in 2022. Since 96% of respondents already outsource at least some of their IT security to MSPs, those budget increases are likely to go at least in part to additional MSP services.

52%

of SMBs lack sufficient skills and technology to protect their organization against cyber threats.

One in four SMB would leave their provider for IT service quality issues.

- **To attract clients, MSPs should provide a comprehensive security offering tailored to SMB needs.** The most important criterion SMBs have when choosing a new provider is whether the service is comprehensive enough. In particular, it should address the most common threat vectors for SMBs. The most common incidents the survey respondents experienced were ransomware, password-based attacks, and phishing, and the top root causes of these incidents were employees falling prey to phishing (63%) and unpatched systems (43%). Notably, these IT security challenges have been on the rise since the shift to remote work amidst the pandemic. Indeed, half of the employees at the SMBs we surveyed currently work remotely — a fact that should also be considered when developing a cybersecurity offering.

- **To improve retention and earn stronger customer loyalty, MSPs should avoid disruptions to the client's business processes.** The survey found that a quarter of SMBs are looking to change their provider due to IT service quality issues. Nearly half (48%) of respondents complained about performance issues with devices — and this problem was the top factor that would lead them to change MSPs. Respondents also complained about outages or unplanned system reboots (33%). This finding points to another core issue: SMBs expect MSPs to provide IT security services without interrupting their employees' work. This concern is understandable, since SMBs need to ensure high user productivity and business growth, given today's market volatility.

IT Security Preparedness

The survey showed SMBs' lack of preparedness for IT security challenges. In fact, more than half of SMBs (52%) acknowledge they probably or definitely lack the technology and skills required to defend against modern cyber threats.

Overall, 60% of SMBs admit that their IT security is either "very limited" or "needs improvement." The vast majority of respondents also mentioned budget constraints when talking about the limitations of their current IT security strategy.

52%

of SMBs admit that they lack the technology and skills to protect their organization against cyber threats.

Chart 1.

Do you have sufficient technology and skills to protect your organization from escalating threats?

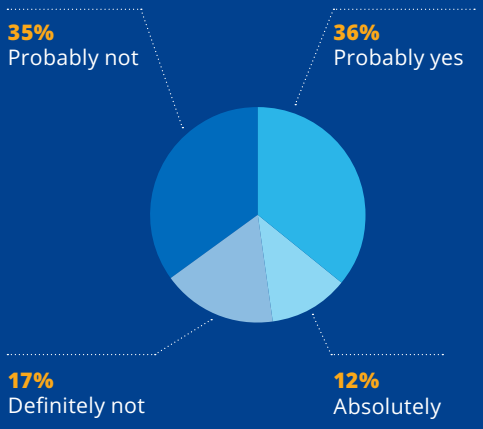
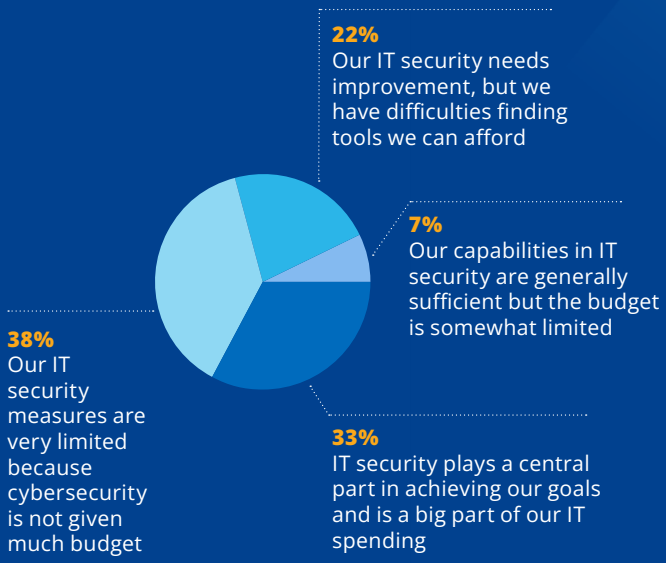


Chart 2.

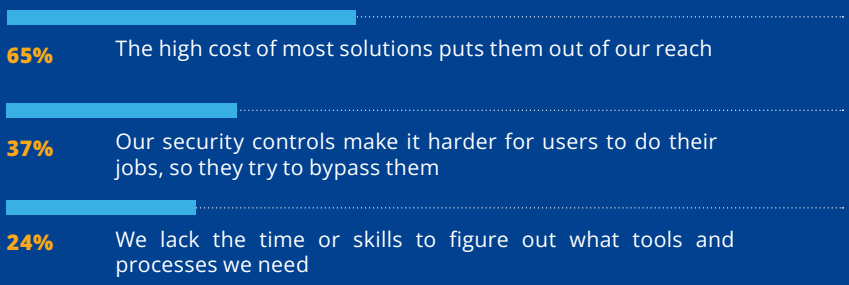
Which phrase best describes your organization's attitude towards IT security?



The most commonly cited factor that prevents SMBs from establishing truly robust cybersecurity was the high cost of most IT security offerings, which was named by 65% of respondents. Second on the list, named by 37% of SMBs, was that their security tools make it harder for users to do their jobs, so they try to bypass them.

Although there is some substance behind these reasons for lax IT security — clearly, SMBs do operate under limited budgets — the fact is, not all cybersecurity tools are expensive or complex and unwieldy. What these findings truly indicate is that SMBs desperately need help in locating and implementing effective security solutions.

Chart 3.
What prevents you from further strengthening your security posture?
(Choose all that apply.)



IT Security Budgeting

The survey revealed that, despite of budget constraints, SMBs are planning to take steps to improve their IT security. Specifically, nearly 6 in 10 organizations (57%) plan to increase their budget for IT security in 2022 by a moderate amount, and almost one-fourth (23%) plan a significant increase.

Most SMBs seem likely to be able to fund these investments in IT security, with most respondents expressing optimism about their business. Indeed, just 1 in 10 expect their revenue to drop slightly in 2022, and none are worried that it will drop significantly. Instead, 74% expect a revenue increase.

80%

of SMBs plan to increase their IT security budget in 2022.

Chart 4.
How do you expect your budget for IT security to change in 2022?

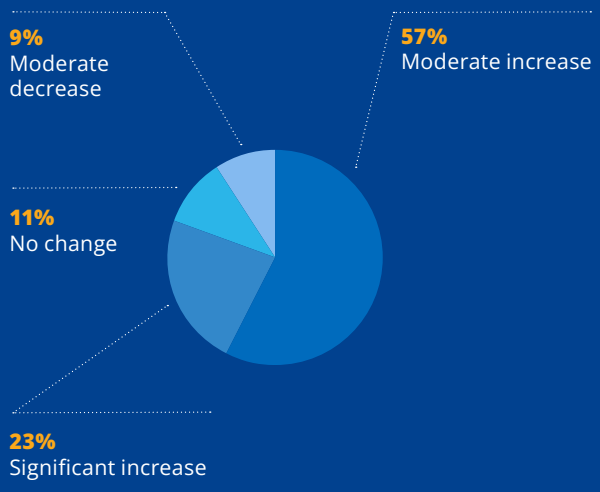
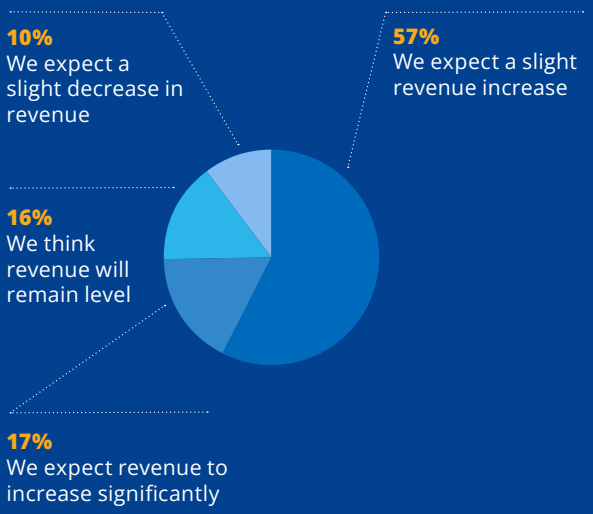


Chart 5.
What is your revenue forecast for 2022?



IT Security Concerns

63%

of SMBs consider themselves to be less at risk from cyberthreats than large enterprises.

Some of the most worrying findings of the report relate to SMBs' misconceptions about cyber risk. Nearly half (48%) of respondents said they think the threat landscape has not changed much in the past year. Actually, it has; in particular, ransomware gangs are leveraging a far more diverse toolset than before and launching more attacks than ever.

In addition, SMBs mistakenly think they are too small to be targeted. In fact, 63% of SMBs consider themselves to be less at risk from cyberthreats than large enterprises, though as we will see in a moment, most organizations surveyed suffered a cyberattack last year.

These misconceptions can give SMBs a false sense of security, which in turn can lead to decisions that increase their risk of successful cyberattacks.

Chart 6.
How concerned are you about cyberthreats?

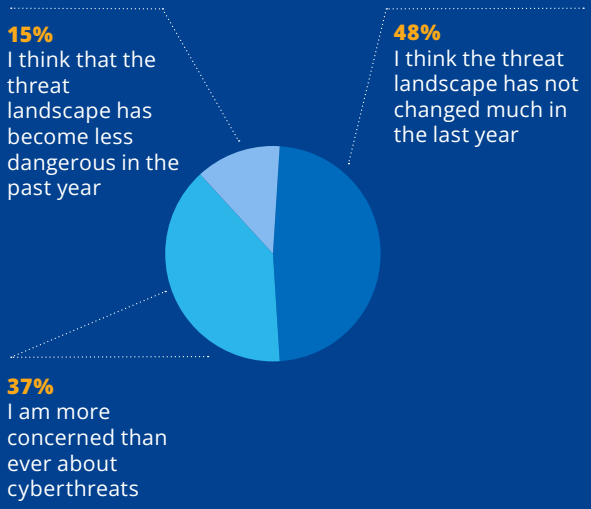
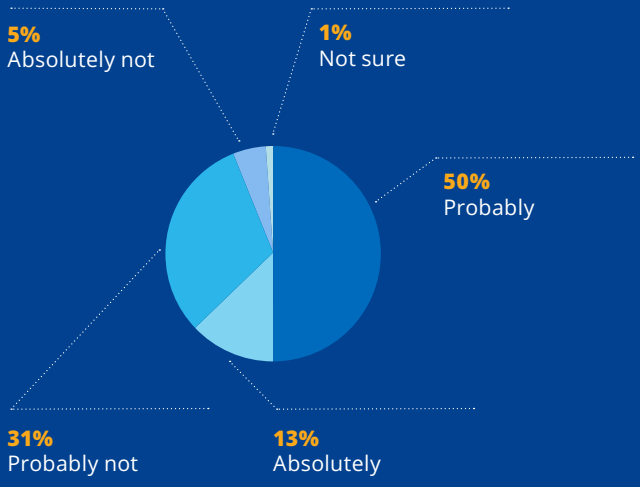


Chart 7.
Do you consider your SMB to be less at risk from cyberthreats than large enterprises?



IT Security Incidents

SMBs are experiencing security incidents at an alarming rate — 81% of respondents said their organization experienced at least one security incident during the past 12 months, and 40% said they suffered 2 or more incidents.

The most common types of incidents were:

- Password attack - 40%
- Ransomware or other malware - 39%
- Phishing - 34%

One possible reason behind the misconception that SMBs are too small to be targeted is a lack of understanding of how and why these attacks are being launched today. The reality is, more and more cybercriminals believe that it is easier for them to hack 10 or 100 SMBs than one large enterprise that is likely to have superior cyber defense, and the attacks listed above are so inexpensive to launch that targeting multiple SMBs is a cost-effective approach.

81%

of SMBs suffered at least one security incident.

Chart 8.
Did you experience any security incidents during the last 12 months?

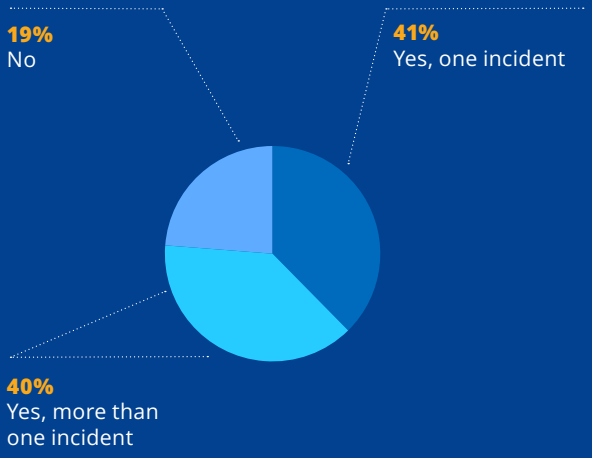
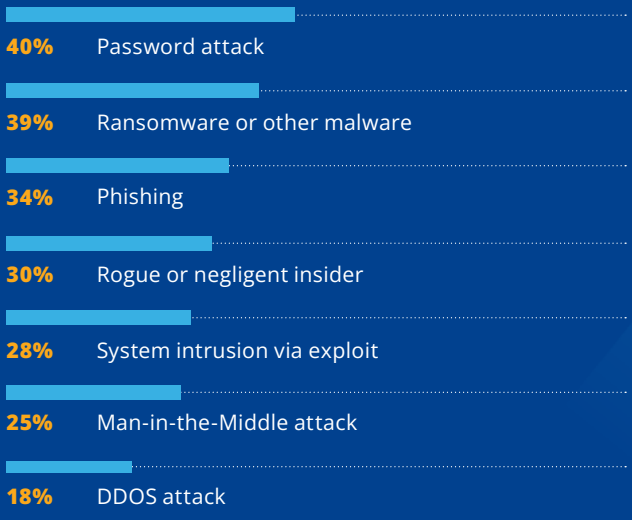


Chart 9.
What type of incident was it?
(Choose all that apply.)



50%

of employees in the surveyed organizations work remotely.

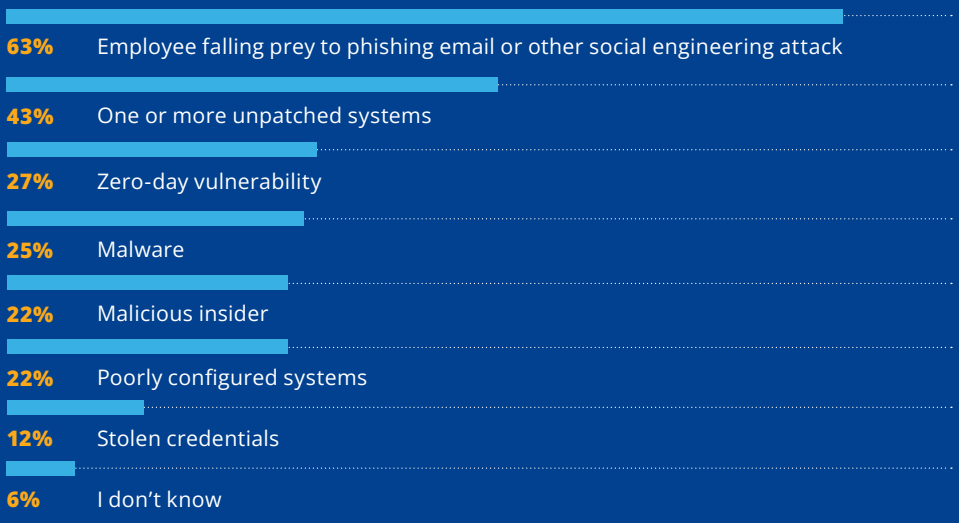
Moreover, the attacks can work together; in particular, gaining access via password attacks or phishing emails is a common way to drop ransomware into corporate systems.

In addition, as it has become easy for hackers who are not technically savvy to launch attacks using ransomware-as-service options available on the darknet, more and more cybercriminals are targeting SMBs because they are aware that SMBs are more likely to have a weak IT security posture.

The most common root cause of the security incidents was phishing and other social engineering attacks, which was blamed by 63% of respondents. The second common root cause was one or more unpatched systems (43%).

One factor that made these infection vectors so common could be the increase in remote work. On average, 50% of employees in the surveyed organizations work remotely, which expands their attack surface and makes software patching more difficult.

Chart 10.
What was the root cause?
(Choose all that apply.)



Use of MSPs

Since many SMBs acknowledge that they lack sufficient skills and technology required to efficiently defend their organizations against today's cyber threats, it's not surprising that they turn to MSPs for help. Nearly all respondents (96%) say they outsource at least some of their IT security to MSPs.

Although the majority of respondents are satisfied with their MSPs, another 23% are looking to replace their current MSP in the coming year.

One in four SMB is looking to replace its current IT provider.

Chart 11.
How much of your IT security do you outsource to an MSP?

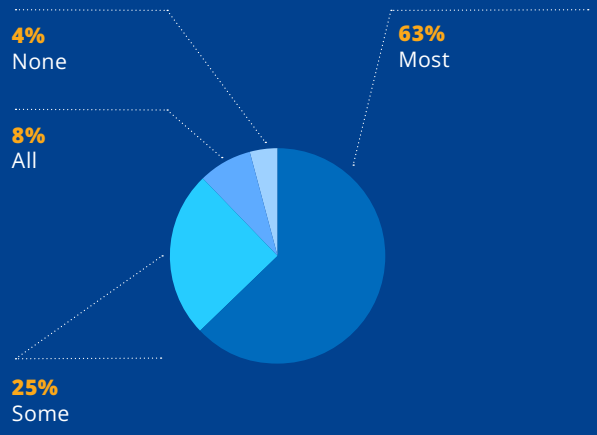
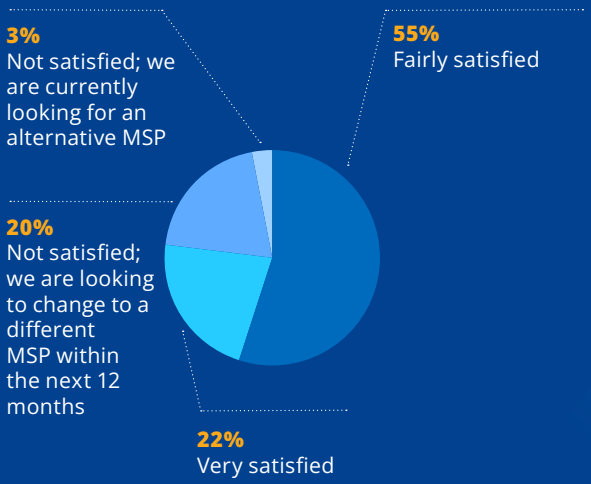


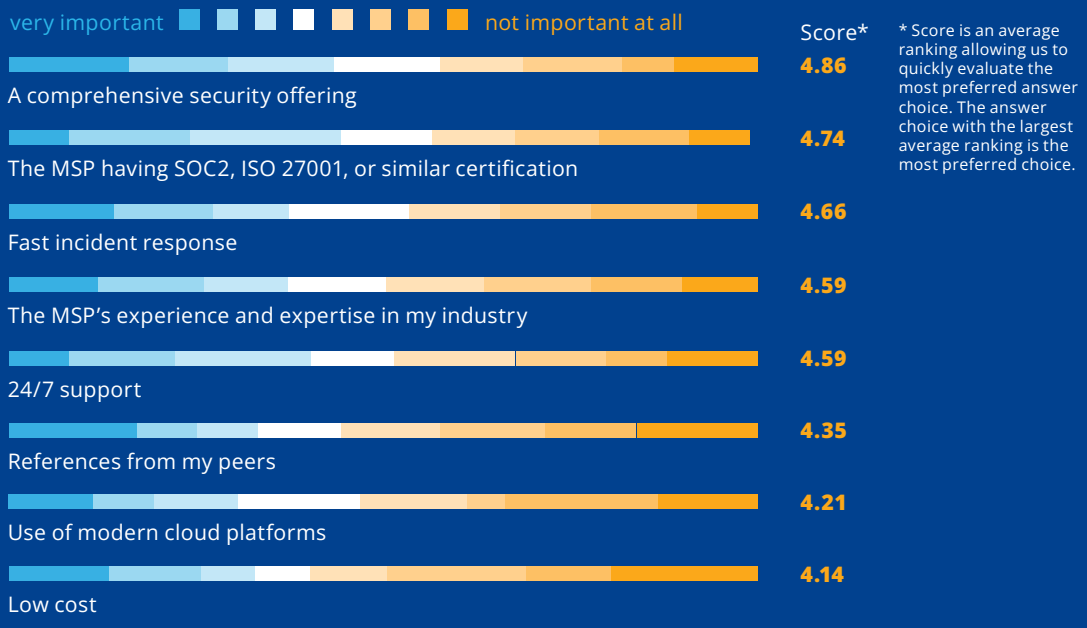
Chart 12.
How satisfied are you with your MSP?



Criteria Used when Choosing an MSP

The survey dug into what factors SMBs look at when choosing a new MSP for IT security. At first, they look to see if the provider's security offering is comprehensive. The second most important factor is availability of necessary certification. And the third most important one is the provider's ability to quickly respond to security incidents.

Chart 13.
How important are the following considerations when you're evaluating an MSP's IT security offering?



* Score is an average ranking allowing us to quickly evaluate the most preferred answer choice. The answer choice with the largest average ranking is the most preferred choice.

Top Issues with MSPs

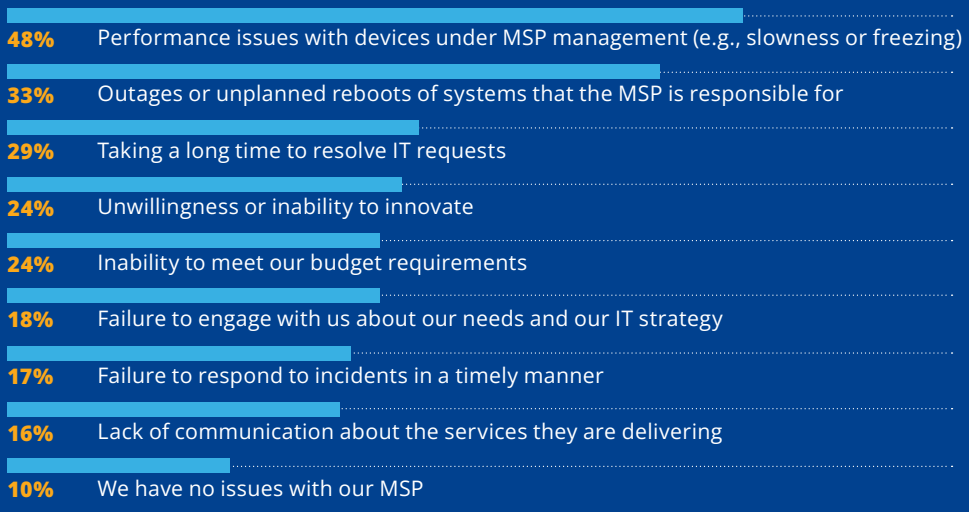
The survey findings shed light on frustrations that might lead SMBs to switch away from their current providers. The three most commonly cited issues were:

- **48%: Performance issues (e.g., slowness or freezing) with the devices under MSP management** — It is worrying that half of SMBs report this problem. Possible reasons include heavy software that requires lots of RAM or CPU, and insufficient device monitoring.
- **33%: Outages or unplanned system reboots** — While outages and system reboots are sometimes necessary, it is a problem when these events are unexpected and interfere with the customer's business operations. Possible reasons for this issue include poor communication between MSPs and their customers, and lack of patch management tools enabling the MSP technicians to schedule the deployment of updates on the convenient times and notify users before systems are rebooted.
- **29%: Long time to resolve IT requests** — Slow response to support requests frustrates customers, and if the MSP is providing IT security services, it can increase security risks. Causes of slow support by MSPs can include using a poor remote support platform or a lack of efficient processes within the MSP technicians.

48%

of respondents experienced performance issues with devices under MSP management.

Chart 14.
Have you ever experienced the following issues from your MSP? (Choose all that apply.)



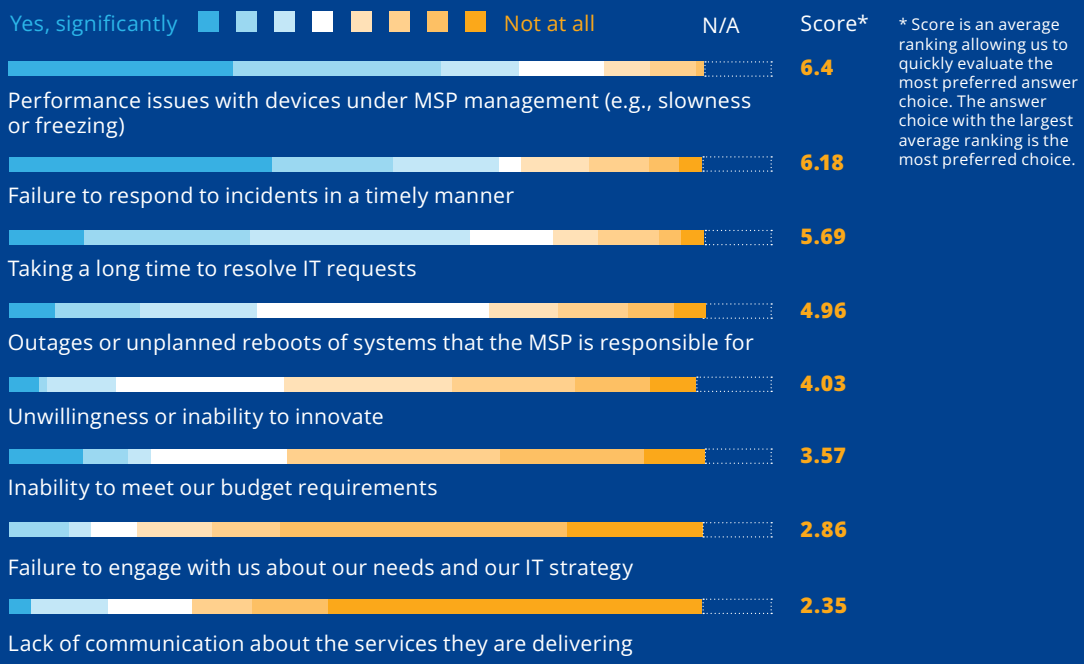
Nearly half of SMBs experienced performance issues with the devices under MSP management, and most SMBs might consider it a deal-breaker.

Taking together, these findings point to a core issue: Interruptions to client business processes caused by IT service delivery hurt customer loyalty and should be avoided. Notably, only 10% of respondents say they have no issues of this sort with their MSP.

Some of these issues were more critical than others as they caused SMBs to question their MSP's ability to secure their business effectively. The most serious ones were performance issues with the devices under MSP management, failure to respond to incidents in a timely manner, and taking a long time to resolve IT requests.

It is interesting to examine Chart 15 in light of Chart 14. In particular, performance issues with devices rank high in both charts — nearly half of SMBs experienced this issue and most SMBs might consider it a deal-breaker. But while many of SMBs say that failure to provide timely incident response made them question their MSP's competence, only 17% of SMBs actually experienced this issue.

Chart 15.
Did any of those issues make you question MSP's ability to secure your business?



* Score is an average ranking allowing us to quickly evaluate the most preferred answer choice. The answer choice with the largest average ranking is the most preferred choice.

Key Recommendations

The survey provided us with valuable insight into the IT security requirements of SMBs and what they need from MSPs. Based on our analysis, we offer the following four recommendations to help MSPs better serve their customers in 2022:

Offer security plans tailored to the attacks that SMBs most commonly experience. To help SMBs fend off ransomware, phishing and password-based attacks, consider providing robust patch management and timely software updates, password policies, multifactor authentication (MFA), Zero Trust, and secure backups and recovery. Also ensure that the client's firewalls, VPNs and other IT infrastructure has sufficient security and bandwidth to support remote workers safely. Also, do not forget about the human element: Talk with your clients about the need to raise cybersecurity awareness within their organizations, and consider adding cybersecurity awareness programs to your offerings.

Improve operational efficiency and service quality. The top issues that frustrate SMBs about their MSPs, such as performance issues with devices and unplanned outages or systems reboots, often result from legacy approaches to endpoint management and uncoordinated work. To avoid losing clients, start by improving your processes. First, upgrade to modern endpoint management tools that enable technicians to quickly troubleshoot issues by connecting to users' devices, as well as automate key IT processes like patch management, including scheduling the deployment of updates and notifying users before systems are rebooted. These tools should also empower your team to monitor the devices to ensure both high performance and security. Second, consider assigning dedicated technicians to groups of similar clients to enable them to better understand their needs and IT architectures and provide prompt and effective support.

Work closely with your customers on their IT security strategy. Most SMBs struggle to locate and implement effective security tools themselves. In particular, they admit that their employees bypass their current controls. Accordingly, MSPs need to work closely with customers to develop effective IT security policies and ensure they are properly implemented. In addition, MSPs should seek out cost-effective technologies that empower them to increase their operational effectiveness and better respond to customer needs.

Educate your customers on the nature of contemporary threats. The survey showed that many SMBs believe they are at less cyber risk than large enterprises. By disabusing them of these misconceptions and explaining why modern attackers increasingly target small and midsize companies, MSPs can help them assess their IT risks more accurately and make informed decisions about their IT security strategy.

Methodology & Demographics

To compile this report, we collected feedback from 750 SMBs in April 2022. Respondents were invited to participate in a giveaway with a chance to win a small monetary reward.

The charts below illustrate key demographics for the respondents.

Chart 16.
Location

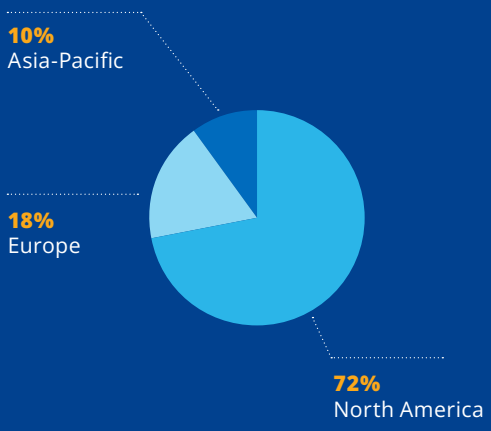
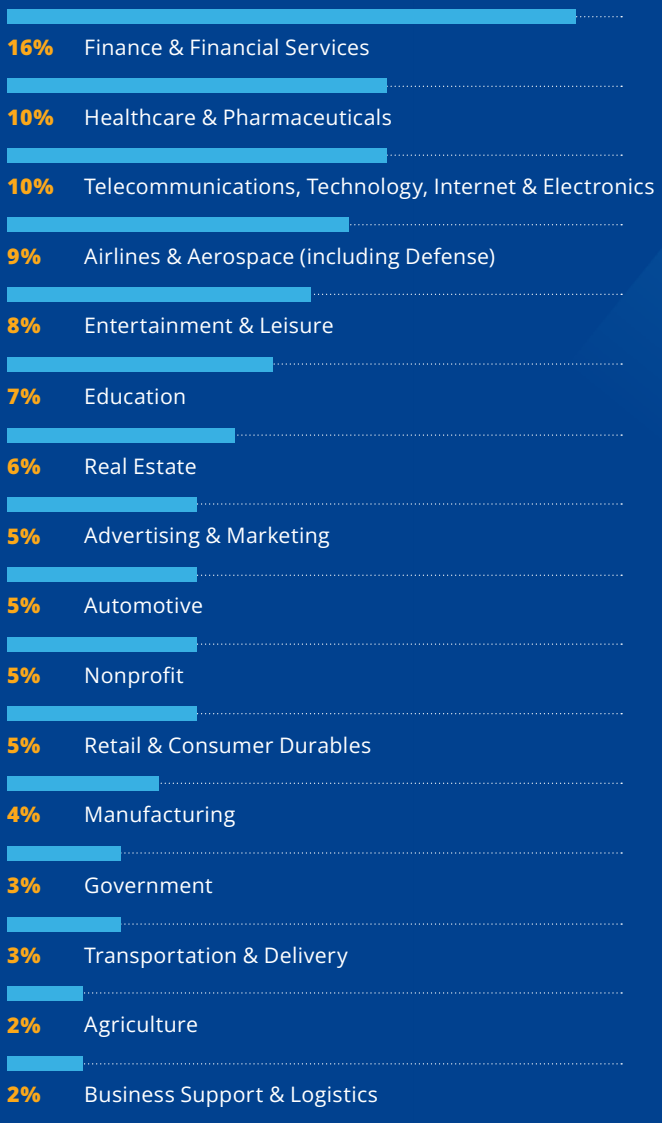


Chart 17.
Industry



About Action1 Research

The report is brought to you by Action1 Research, which conducts industry surveys among IT pros worldwide to discover trends in cybersecurity, IT operations, and the MSP industry.

For more information, please visit:

https://www.action1.com/resources/research/

About Action1 Corporation

Action1 is the provider of the #1 secure and easy-to-use cloud RMM tool that's free for the first 100 endpoints. It delivers policy-based patching and deployment of OS and third-party software, provides real-time visibility into vulnerabilities and IT assets, and includes a built-in remote desktop compliant with modern privacy laws. The company was founded by Netwrix cybersecurity veterans Alex Vovk and Mike Walters to give companies and MSPs a modern and secure alternative to legacy on-premises solutions that do not function in hybrid workforce environments.

For more information, please visit:

www.action1.com

or call 1-346-444-8530.

Corporate Headquarters:
2929 Allen Parkway,
Suite 200 Houston,
TX 77019

Action1