FORTINET

EXCLUSIVE NETWORKS

REPORT

Small and Midsize Businesses and Cybersecurity

A Report on Current Priorities and Challenges

Table of Contents

Executive Summary

The Small and Midsize Businesses and Cybersecurity Report looks closely at the challenges facing small (20-99) and midsize (100 to 249) businesses (SMBs) today and pinpoints insights showing how these organizations are responding to the challenges. Here are some key takeaways:

1. SMB leaders have diverse responsibilities that vary by organization size. While cybersecurity is a top priority for all, other areas such as finance, marketing, and sales compete for mindshare.
2. To measure security effectiveness, small businesses focus on financial metrics, while midsize firms emphasize availability and managing risk.
3. SMBs are moving to the cloud, albeit slowly. While virtually all respondents are adopting the public cloud, the majority still has more than half of their infrastructure on-premises. As they migrate, SMB leaders are split on whether to implement cloud security internally or rely on external resources such as managed service providers (MSPs) and managed security service providers (MSSPs).

Analyzing the data more deeply, the report compares the best practices of respondents who had no malicious events the past 12 months to those who were not so fortunate. SMB leaders can make use of these findings to align their security practices with proven programs.

Infographic: Key SMB Findings

61%

rate cybersecurity among their top five **job responsibilities.**

Others: 60% for operations, 54% for applications, and 52% for compliance

89%

rely on MSPs or MSSPs for **security assistance.**

64%

of presidents/CEOs/ owners rank **existing customer growth** as their top success metric.

Only 48% of CFOs agree—instead, 58% cite efficiency and productivity gains

SMBs with the fewest number of security incidents are:

51% more likely to rank **new revenue** as a top success metric

46% more likely to rank **existing customer growth** as a top success metric

36% more likely to feel comfortable protecting against **unknown threats**

28% more likely to list their **title** as president/CEO/owner

Introduction

The typical leader of an SMB must juggle responsibilities that span the organizational chart as well as the clock. On a typical day, they can find themselves dealing with cybersecurity and compliance issues in the morning, pivot to marketing presentations and attorney meetings in the afternoon, and end their day pitching potential customers or partners over dinner. The SMB environment draws leaders who are strong in key disciplines and savvy enough to deal with problems in unfamiliar parts of the business.

The digital attack surface of the SMB is much broader than it was a few years ago: brick-and-mortar operations are gone, replaced by online businesses—whether simply maintaining a website or a social media presence to full-blown ecommerce operations with a lifeline tied to connectivity and computing power. That reality puts pressure on founders, CEOs, and other executives who often excel in the nuts and bolts of running the business but may struggle when it comes to the digital aspects.

"Technology is evolving so fast that it is a real challenge to stay abreast of the latest developments and trends in cybersecurity."
– CEO, Financial Services Industry

Cybersecurity presents a major challenge for many SMB leaders. One persistent myth is that, compared to large enterprises, SMBs "fly under the radar" when it comes to cyber threats. In fact, cyberattackers see SMBs as an increasingly attractive target and are stepping up their attacks. The number of cybersecurity incidents jumped 43% for small businesses and 75% for midsize organizations in the past year.[1] Cyberattacks represent a significant risk to every business regardless of the number of employees—they are simply a fact of life for the SMB leader.

This dilemma has a silver lining. After all, SMB competitors face similar challenges, so the ability to navigate technology challenges—including cybersecurity—can be a significant differentiator. Some SMBs implement and manage security on-premises. Many SMBs, which have limited resources, turn to third-party managed service providers (MSPs) and managed security service providers (MSSPs) either for supplemental assistance or to outsource security entirely.

Methodology for This Study

This study surveyed SMB leaders for SMBs in a variety of industries across the United States.

Survey participants were all identified as key decision-makers. The largest grouping (31%) was top executives—presidents, CEOs, and owners—with IT directors and managers a close second (29%). Following these two groups were business leaders—CIOs (14%), COOs (12%), and CFOs (6%), followed by network and security administrators (4%) and other (4%) (Figure 1).

In terms of organization size, participants were almost evenly split between small organizations with 20 to 99 employees (53%) and midsize organizations with 100 to 250 employees (47%) (Figure 2).

The largest industry segment was technology (22%), followed by professional services (19%), retail/hospitality/travel (15%), and manufacturing (14%) (Figure 3).

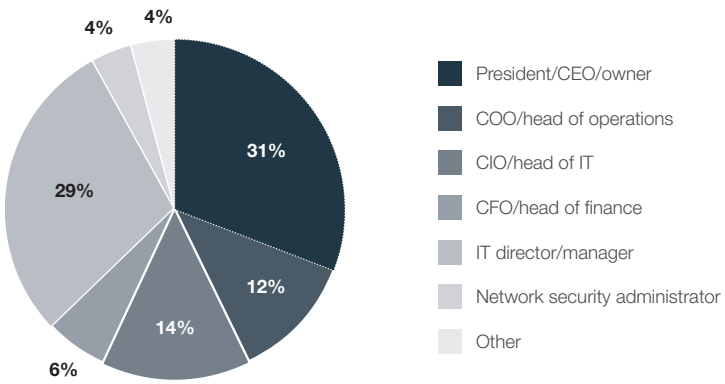

Figure 1: Survey participants by job title.

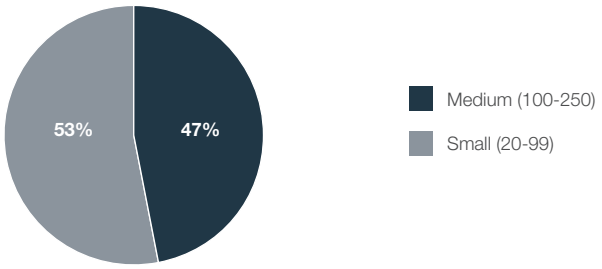

Figure 2: Survey participants by organization size.

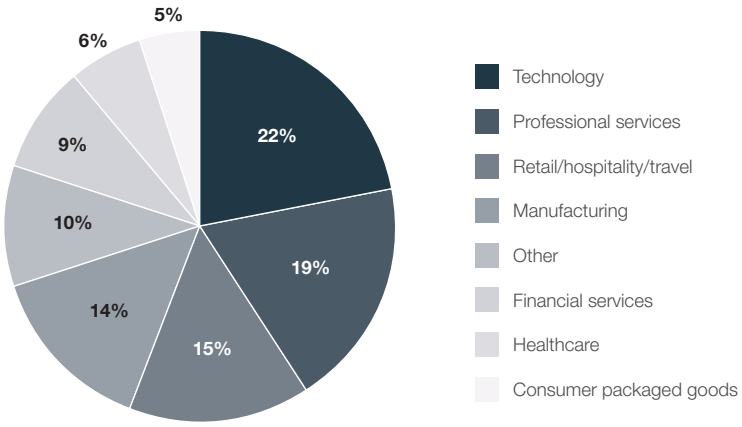

Figure 3: Survey participants by industry.

SMB Trends—Mindset

Trend: SMB leaders have diverse job responsibilities that span multiple disciplines.

The stereotypical image of the small businessperson as someone who touches virtually all aspects of the business is borne out by the survey results. Unlike the more focused charters of executives in large enterprises, the areas of responsibility for SMB leaders span multiple aspects of the business. The top five include **cybersecurity** (61%), **operations** (60%), **on-premises and cloud applications** (55%), **compliance with regulations and standards** (52%), and **product development and management** (52%) (Figure 4). It is unlikely that any one person will have expertise in all these areas, so the SMB leader must be able to effectively manage unfamiliar disciplines in support of the organization's strategic goals.

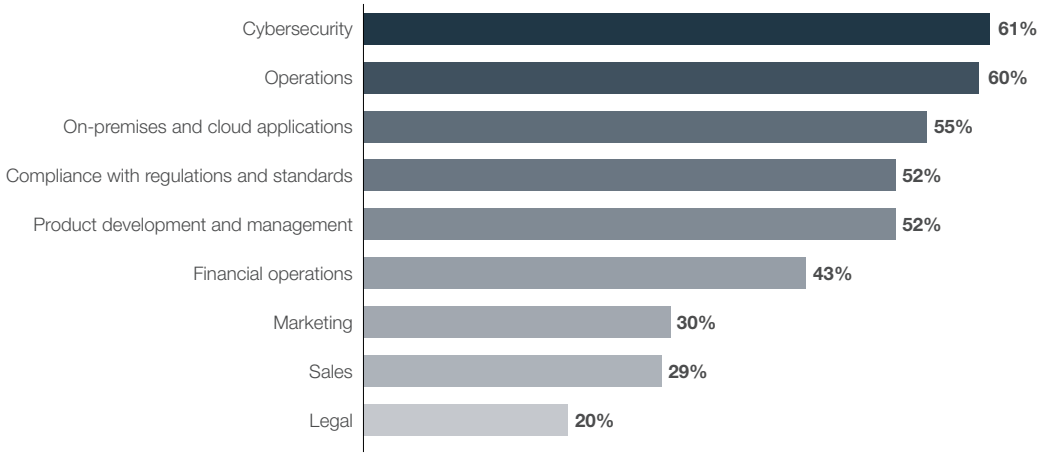

Figure 4: Job responsibilities of SMB leaders.

Trend: Growth and productivity are top success measures for SMBs.

Among all respondents, the most popular categories for measuring success were **existing customer growth** (49%)**, efficiency/productivity gains** (47%), **IT system/app availability** (43%), **cyber threats stopped/mitigated** (40%), **and new revenue** (40%). However, when responses are separated by their respective decision-making roles, the priorities for success show some interesting differences (Figure 5).

Specifically, in line with the overall results, the majority of presidents, CEOs, and owners (64%) rank **existing customer growth** as their leading measure of success. **Efficiency/productivity gains** and **new revenue** rank toward the top for CEOs (49% and 48%, respectively). Nearly half of all small business failures are due to lack of working capital, so it makes sense that owners judge success by increasing revenues from existing customers and developing new revenue streams.[2]

COOs and CFOs report the same three top measures as CEOs but in a different order. **Efficiency/productivity** gains was the top success measure for both COOs (69%) and CFOs (56%), followed by **new revenue** (50% and 44%, respectively) and **existing customer growth** (50% and 44%, respectively). The fact that the COO and CFO are more directly focused on productivity suggests that CEOs are willing to delegate operational responsibilities but prefer to own the customer relationship themselves.

For directors of IT, CIOs, and network/security administrators, however, measurement of operational uptime and security were top critical concerns. **IT system/app availability** was favored as an important success metric by 64% of these respondents. Their next highest-ranking success factor was **cyber threats stopped/mitigated** (a top-three choice by 60% of those surveyed). This finding likely reflects the fact that CIOs and IT leaders tend to be evaluated on their ability to keep the infrastructure running and free of malicious threats.

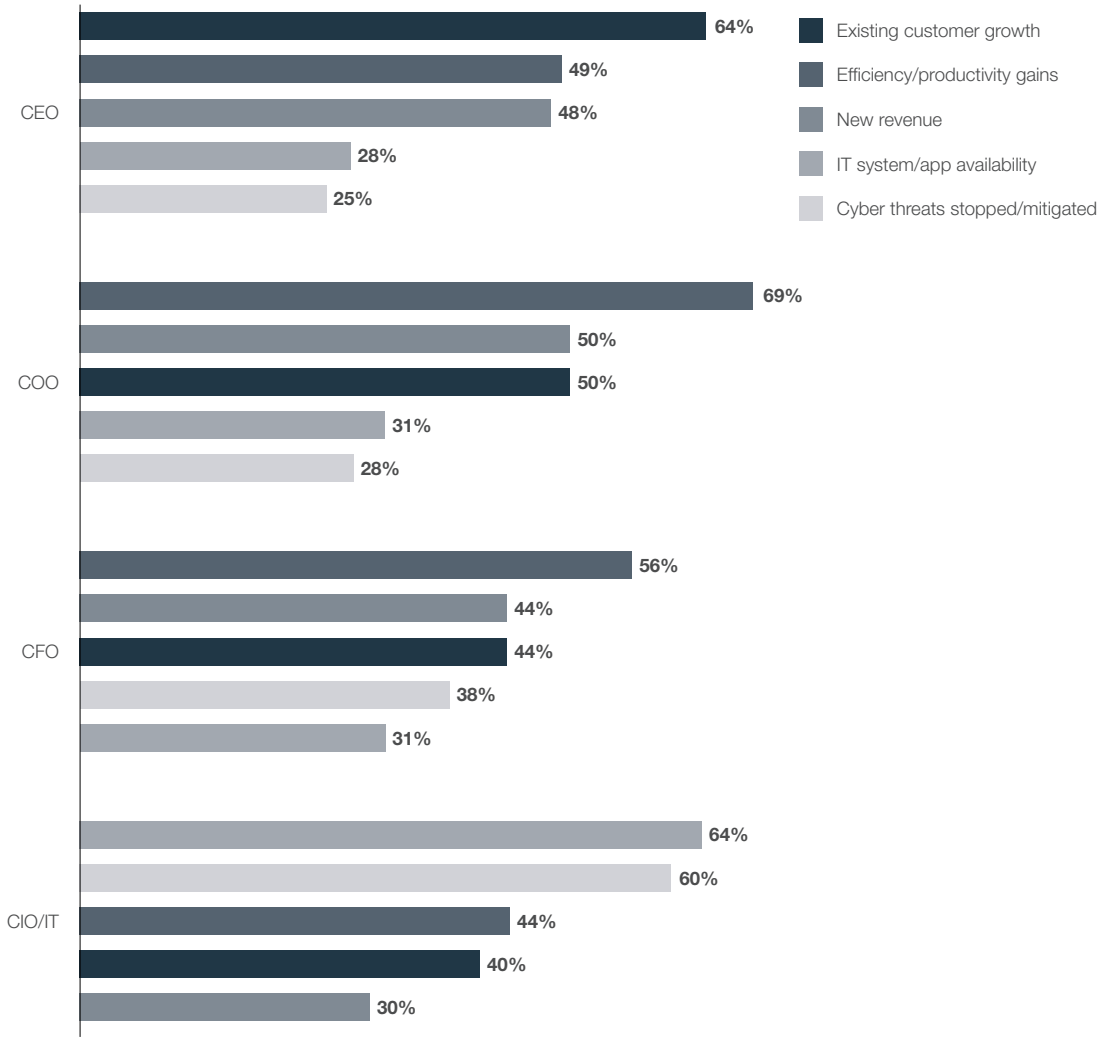

Figure 5: Success metrics by organizational role.

Trend: SMBs show high levels of confidence in their current security posture.

The survey showed high levels of confidence in four aspects of security: **cloud service provider (CSP) baseline security** (78%), **SaaS provider baseline security** (77%), **remote access security** (75%), and **mobile device security** (70%) (Figure 6). However, findings in the next section (SMB Trends—Security Posture) regarding security features, risk management best practices, and lack of automation suggest a degree of over-optimism in their self-evaluations—a not uncommon occurrence in any size organization.

Figure 6: Confidence level in four key aspects of security posture.

"Our biggest challenge is maintaining a secure system while still interacting effectively with potential customers and revenue opportunities."
– CFO, Transportation Industry

SMB Trends—Security Posture

Trend: Many SMBs lack critical security features for threat prevention and access control.

The top two security features deployed by SMBs include **network firewalls** (71%) and **data loss prevention** (68%)—certainly the bare minimum level of security that every SMB needs. The next two features—**web application firewalls** (59%) and **mail security** (58%)—offer additional protection for traffic entering and leaving the SMB infrastructure. These four features together can be viewed as a baseline security package that every SMB should deploy (Figure 7).

However, the advancing threat landscape and expanding attack surface pose risks that call for additional security capabilities for threat detection and prevention and access control that require other security features. Nearly half (46%) of SMBs lack **security information and event management (SIEM), endpoint protection,** and **identity management/authentication.** SMBs should carefully evaluate their level of vulnerability—ideally with the help of a trusted vendor or security consultant—to identify gaps in the organization's security posture and the steps needed to fix them.

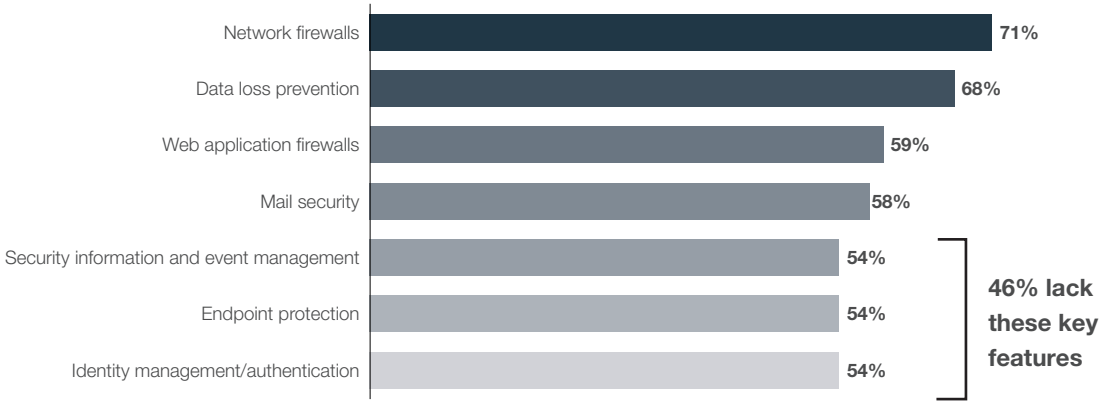

Figure 7: Security features deployed by company size.

Trend: SMBs have important risk factors—and gaps in their risk management strategies.

The survey uncovered several key risk factors facing SMB leaders: **use of contractors** (86%), **increased regulatory requirements** (89%), and **remote employees** (86%). As expected, midsize businesses have more exposure than small organizations in all three categories: contractors (95% versus 79%), compliance (96% versus 82%), and remote workers (90% versus 83%) (Figure 8).

When it comes to risk management factors, 73% of SMB organizations believe they can balance risk against risk tolerance based on metrics. A dominant percentage (72%) also report that they have full visibility and control into their network, a prerequisite for effective risk management (Figure 9). This number is almost directly inverse to responses from large enterprise organizations, where 70% of decision-makers feel they lack full visibility of their infrastructure.[3]

At the same time, nearly half have challenges with unknown threats (47%) or are too reactive (41%). These findings are early warning signs: SMB leaders would do well to up-level their risk management strategies. A good first step is to seek expert help to conduct a thorough risk management assessment.[3]

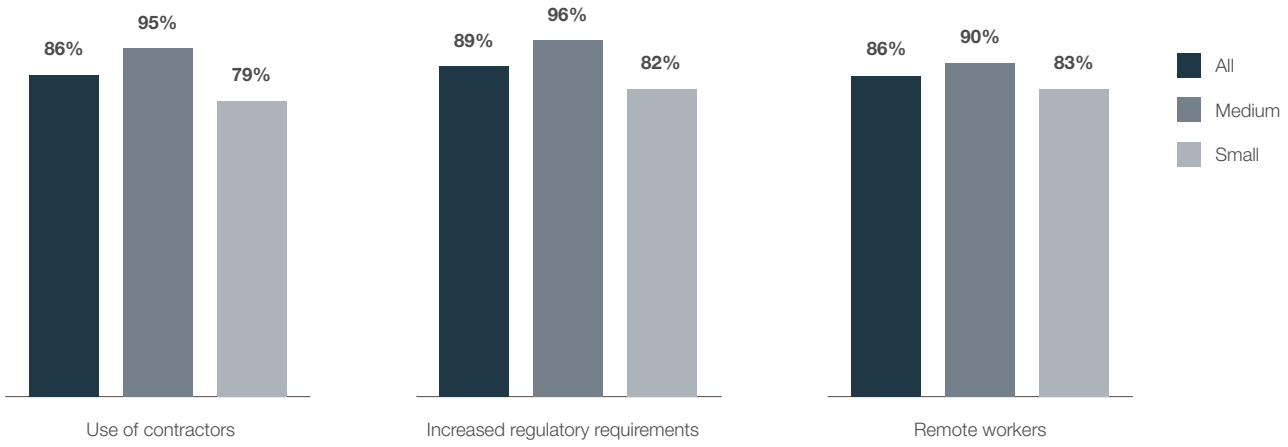

Figure 8: Risk factors by company size.

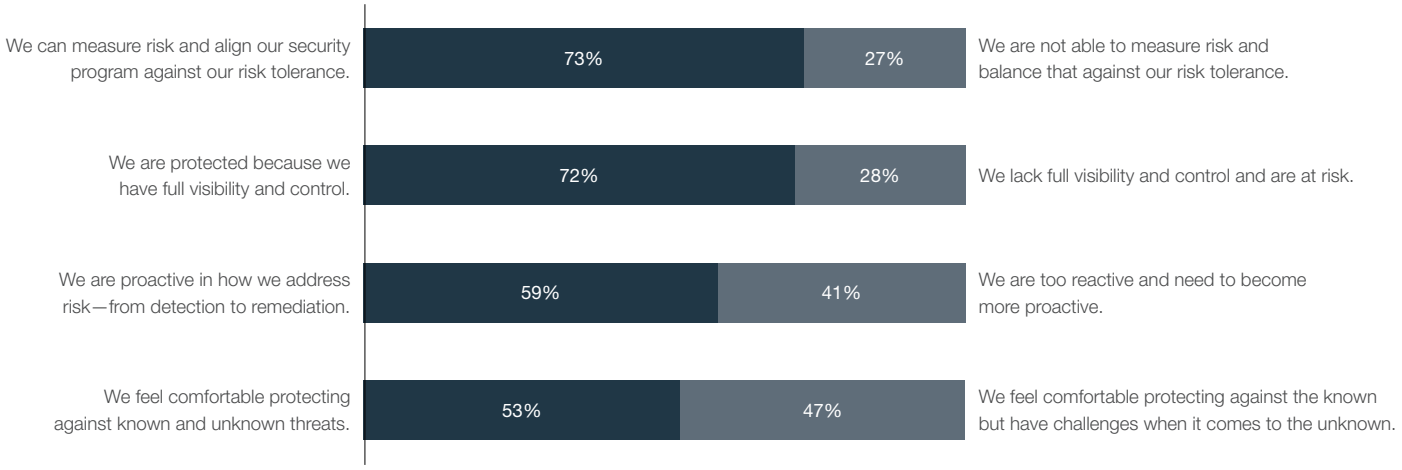

Figure 9: Adherence to risk management best practices.

Trend: SMB obstacles to cybersecurity point to a need for security automation.

The top issues that SMB organizations face with security include **lack of expertise/knowledge** (37%), **lack of end-to-end integration** (35%), and **missing malware and attacks** (34%) (Figure 10).

The first of these reported problems is supported by the worldwide shortage of skilled security staff—for example, cybersecurity professionals in a recent cloud security survey sponsored by (ISC)[2] listed **lack of qualified security staff** as one of their biggest operational headaches.[4] SMBs are certainly not immune, and perhaps the problem is even exacerbated for them because it is hard for them to compete for security talent against larger enterprises.

"Ransomware is the bane of our IT staff, data scientists, and executives."
– IT Director, Technology Industry

The next four issues—**too many manual processes** (34%), **lack of visibility** (30%), **too many false positives** (27%), and **difficult to manage** (27%)—speak to the subsequent need for automated defenses to compensate the lack of skilled security expertise. Security integration enables automation. Automated detection and response capabilities can significantly reduce threat intrusion rates while easing the burdens of manual workflows on limited staff.

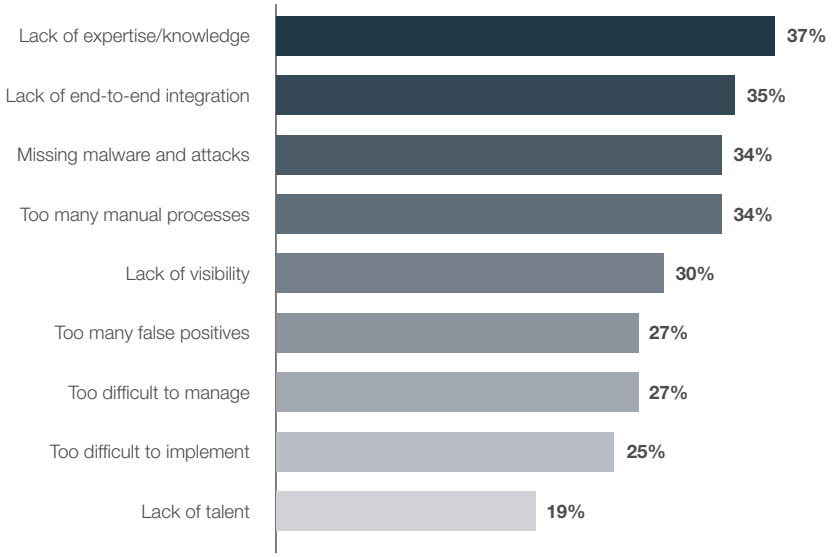

Figure 10: Obstacles to cybersecurity.

SMB Trends—Strategies

Trend: Most SMBs partner with MSPs for both security and other IT services.

The survey data clearly shows that a large majority of SMBs rely on managed service providers for both security (89%) and other IT services (75%) (Figure 11).

A breakdown shows that the top reason for using outside services is **implementation consulting** (35%), followed by **ongoing outsourcing** to MSPs (30%) and assistance with **public cloud security solutions** (24%) (Figure 12).

Midsize companies are far more likely to turn to an MSP for public cloud security (31% versus 18%) while the smaller firms are more than three times as likely to handle security internally (16% versus 5%) and somewhat more likely to outsource security on a continuing basis (32% versus 28%).

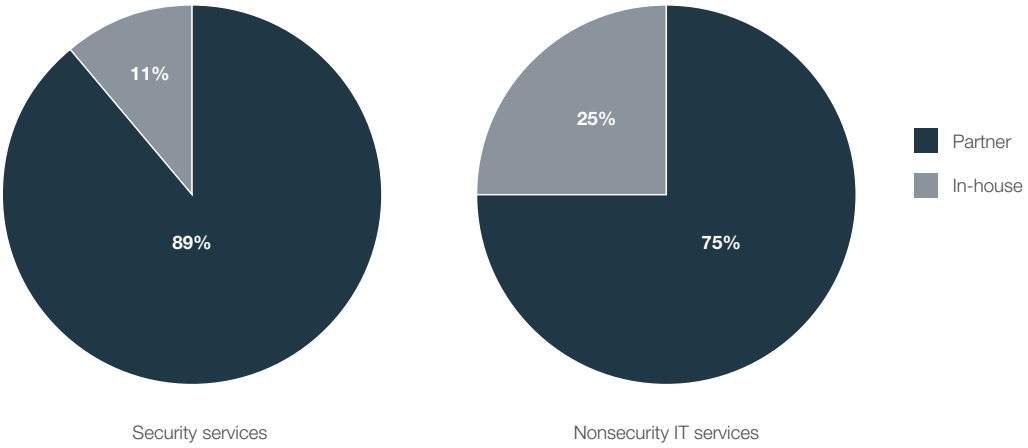

Figure 11: MSP usage for security and nonsecurity services.

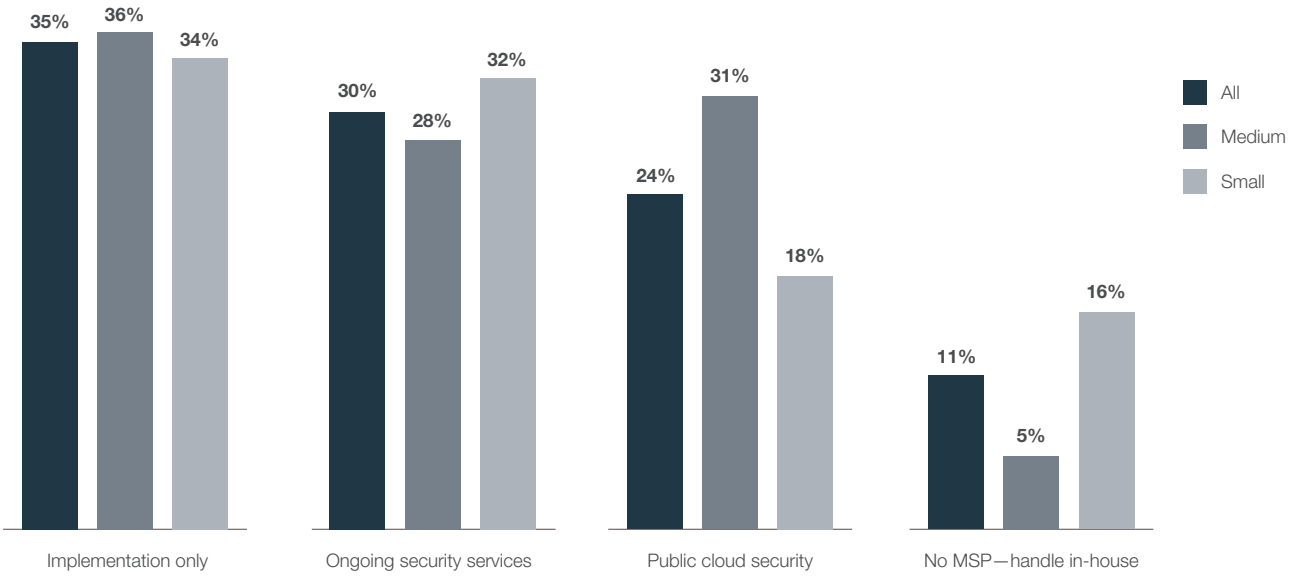

Figure 12: Breakdown of MSP usage.

Trend: SMBs are moving to the cloud but still have most of their infrastructure on-premises.

Without question, moving to the cloud requires a substantial readjustment to any organization's security strategy. Despite significant investments in baseline security by major cloud service providers, cybersecurity professionals are skeptical: A recent study reported that 93% of organizations are moderately to extremely concerned about cloud security, a small increase from the year before.[5]

This anxiety could be one reason why SMBs—many of whom struggle to secure their on-premises deployments—have been slow to take on the challenges of the public cloud. The Fortinet survey found that only 39% of SMBs have migrated at least half their infrastructures to the cloud, with little variation by company size (Figure 13). However, three-quarters (75%) have some level of cloud deployment, an indication that SMBs are adopting cloud services into their business strategies.

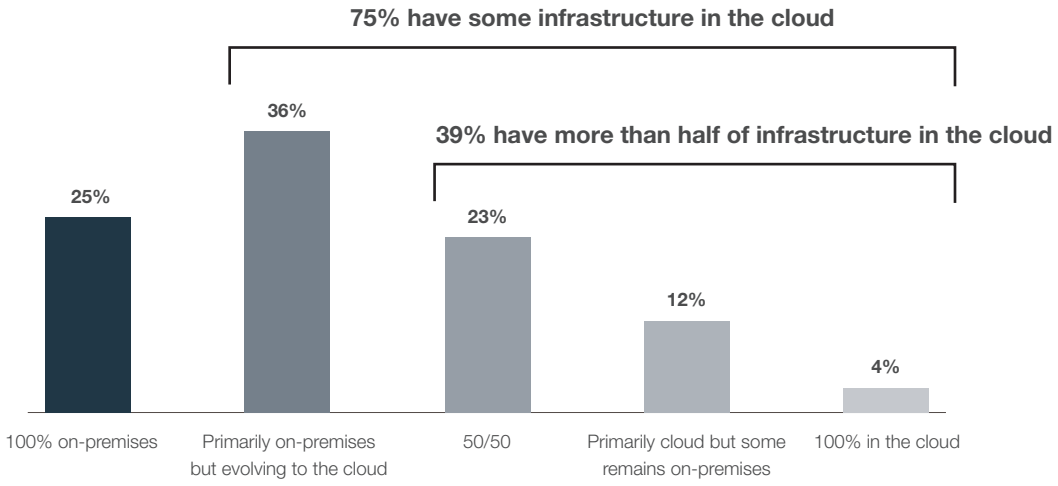

Figure 13: Level of cloud adoption by SMBs.

Trend: Virtually all SMBs have a strategic plan for cloud security but differ on the best way to resource.

As their cloud deployments continue to grow, SMBs are divided on the best way to provide security. More than one-third (36%) of respondents will partner with an MSP/MSSP, but another one-third (33%) plan to hire more staff and handle the increased security requirements internally. Of the rest, 16% look to purchase an off-the-shelf software solution. Just 10% plan to outsource to an MSSP. A mere 5% do not yet have a plan in place (Figure 14).

For the most part, small and midsize organizations have similar strategies, although there are a few noteworthy differences. For one thing, 8% of small companies lack a plan for cloud security compared to just 1% of their larger counterparts. On the flip side, midsize firms are more likely to rely entirely on internal resources (36% versus 30%), while smaller organizations have a slight preference for purchasing a turnkey solution (17% versus 15%). Larger firms are 50% more likely to outsource to an MSP/MSSP (12% versus 8%).

"We're having security issues moving legacy applications to the cloud."
– CIO, Consumer Packaged Goods Industry

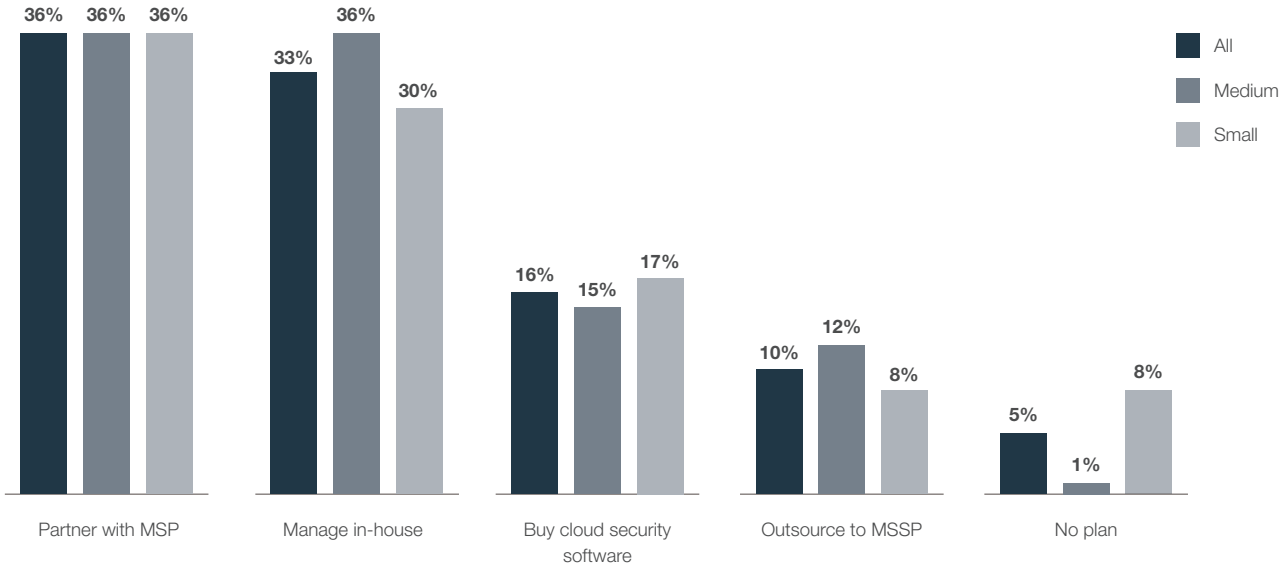

Figure 14: Cloud security plans by company size.

Trend: Small businesses focus on financial metrics, while midsize firms emphasize availability and cybersecurity.

One of the more striking findings of this survey concerns the differences in success metrics between small (less than 100 employees) and midsize (100 to 250 employees) organizations (Figure 15). Compared to their smaller counterparts, midsize businesses put far more emphasis on **system availability** (51% versus 36%) and **cyber threats stopped or mitigated** (46% versus 34%).

Here is one plausible explanation for the discrepancy: Since larger businesses tend to have more customers, they have more customer information at risk and thus could be expected to track their performance in stopping and mitigating breaches more than smaller companies. An earlier survey finding offers an alternate explanation. As midsize businesses are more likely to use contractors, deal with regulatory challenges, and have remote workforces, they may place more emphasis on cybersecurity because they have a larger attack surface and more regulatory scrutiny—the job is just bigger for them.

"My organization lacks clear visibility of which workloads are the most sensitive and the policies in place to protect them."
– IT Director, Retail Industry

The tables turn in favor of the small businesses when it comes to **new revenue** (43% versus 33%) and **cost reduction/avoidance** (53% versus 45%). These findings suggest that the smaller businesses are more focused on **profit margins** due to the increased risk of failure that comes with lower revenues and less robust cash flows. These financial, time, and resource pressures thwart the attention they can spend on cybersecurity, which becomes a checkbox.

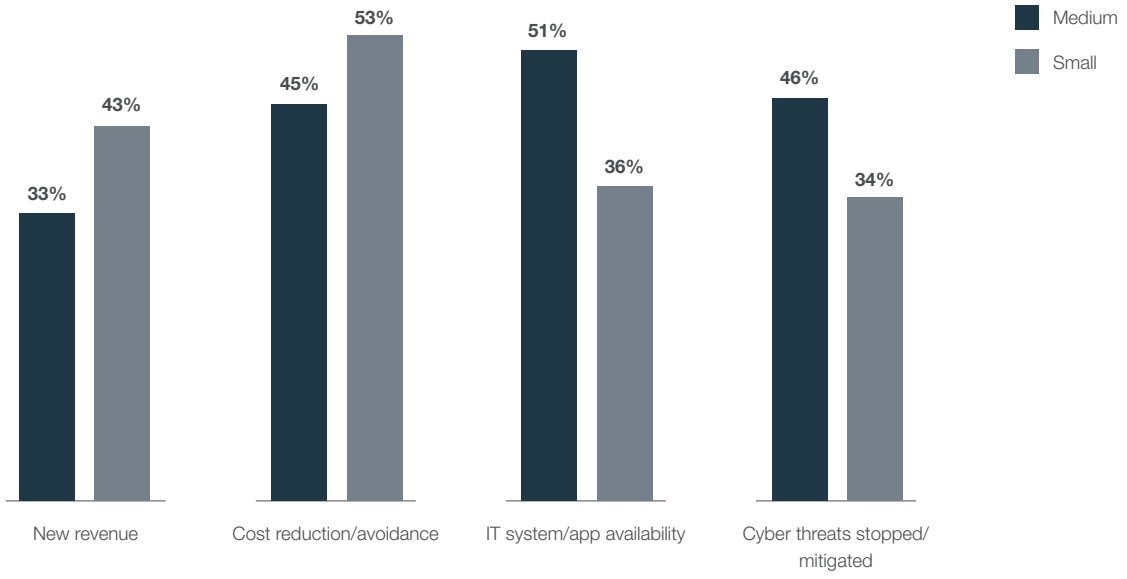

Figure 15: Success metrics by company size.

Key Challenges for SMB Leaders

The survey asked participants to describe their biggest cybersecurity challenges verbatim, then sorted their answers into the following three categories:

- **Expanding attack surface.** Public cloud, mobile, Internet of Things (IoT), and other technologies driven by digital innovation increase the number of possible attack points and therefore the associated risks.
- **Complexity.** The breadth of point security products and general lack of integration make it difficult for lightly staffed businesses to effectively manage cybersecurity.
- **Advanced threat landscape.** Increasingly sophisticated threats—and far more of them—challenge SMB leaders who often have little formal cybersecurity training.

"Customer information is particularly at risk when users access applications from their mobile devices."
– CFO, Financial Services Industry

Of the above three categories, respondents cite the **advanced threat landscape** as the biggest challenge, comprising nearly half (48%) of all respondents, followed by **complexity** (38%) and the **expanding attack surface** (13%) (Figure 16). These findings make sense in light of what we know about SMBs. The typical SMB leader has little formal cybersecurity training, so advanced threats—a challenge to any IT professional—can be expected to be a major concern. The same logic applies to complexity: Even if SMB leaders can procure and deploy effective security solutions, they lack the ability to integrate and optimize multiple tools. Finally, SMBs tend to lag large enterprises in their adoption of new technologies and therefore the expanded attack surface is a lesser concern for them.

Breaking down the findings by organizational size expands the understanding of SMB challenges. To begin, a larger percentage of midsize companies see the **advanced threat landscape** as their biggest challenge (57% versus 42%). With more valuable information stored in their infrastructures, midsize companies often make a more inviting target for cyberattackers than the smaller businesses. In contrast, small businesses are more likely to cite **complexity** as their top challenge (43% versus 32%), probably reflecting their relative lack of formal cybersecurity training and resources compared to the larger organizations.

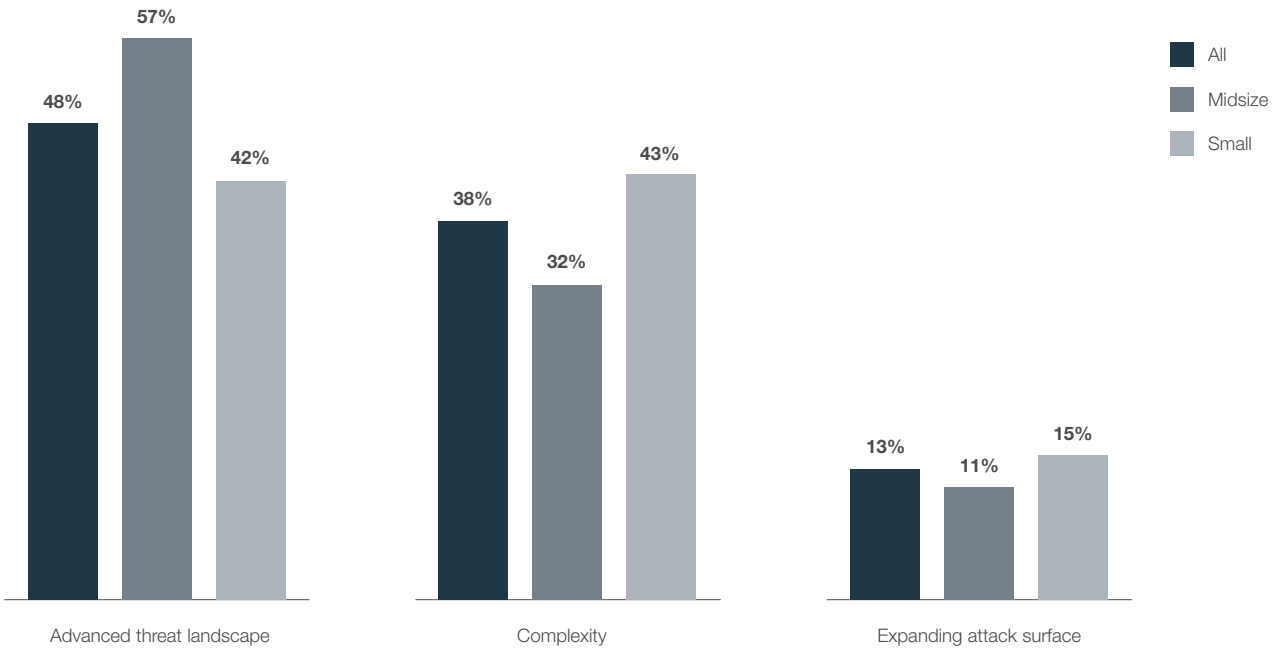

Figure 16: Top cybersecurity challenge categories by size.

Best Practices of Top-tier SMB Leaders

Fortinet compared the survey responses from respondents reporting no malicious events in the past year with those who had experienced at least one such incident. This analysis identified a number of best practices that top-tier SMB leaders were more likely to employ:

1. Top-tier SMB leaders are 86% more likely to use cloud security software.

Cloud service providers deploy baseline security to protect their infrastructure. However, SMBs must secure their own data and applications. This finding shows that cloud security is not a do-it-yourself activity—namely, success is more likely for those who invest in proven solutions.

2. Top-tier SMB leaders are 51% more likely to rank new revenue and 46% more likely to rank existing customer growth as top success metrics.

All successful business leaders know the equation: Profit = Income – Expenses. The more successful SMB leaders focus on the income side, both by gaining new sources of revenues and maximizing wallet share for existing customers.

3. Top-tier SMB leaders are 36% more likely to feel comfortable protecting against unknown threats.

All survey respondents were understandably comfortable dealing with known threats—signature-based solutions are highly effective. However, top-tier SMBs understand the risks associated with the advanced threat landscape and have taken steps to mitigate those risks.

4. Top-tier SMB leaders are 28% more likely to be the president/CEO/owner.

Numerous studies have shown that the higher the level of executive sponsorship, the more likely an initiative is to receive the necessary resources. This finding demonstrates that cybersecurity needs to be top of mind for the leader at the top.

5. Top-tier SMB leaders are 27% more likely to say that they are protected because they have full visibility and control.

A prerequisite for effective security is end-to-end visibility and control of the security apparatus, a fact that the top-tier leaders have turned to their advantage.

Conclusion

SMB leaders face unique challenges in securing their business assets from cyberattacks. This report shows a growing awareness of the importance of cybersecurity and a fairly realistic understanding of the risks associated with the advanced threat landscape and complexity of the security infrastructure.

SMB leaders would do well to implement these best practices:

Augment the baseline security provided by cloud service providers and SaaS providers with proven solutions from a trusted vendor

Deploy an end-to-end integrated security architecture with full visibility and protection against unknown threats

Vest ultimate responsibility for cybersecurity in the president/CEO/owner

Procure security solutions that can scale easily to accommodate growth

References

1 "Hiscox Cyber Readiness Report 2019," Hiscox, April 2019.

2 Melissa Horton, "The 4 Most Common Reasons a Small Business Fails," Investopedia, August 12, 2019.

3 "Security Implications of Digital Transformation Report," Fortinet, July 26, 2018.

4 "2019 Cloud Security Report," Cybersecurity Insiders, 2019.

5 Ibid.

FORTINET

www.fortinet.com

January 7, 2020 9:00 AM

D:\Fortinet\Work\2020\January\010720\report-small-midsize-businesses-cybersecurity

368323-0-0-EN