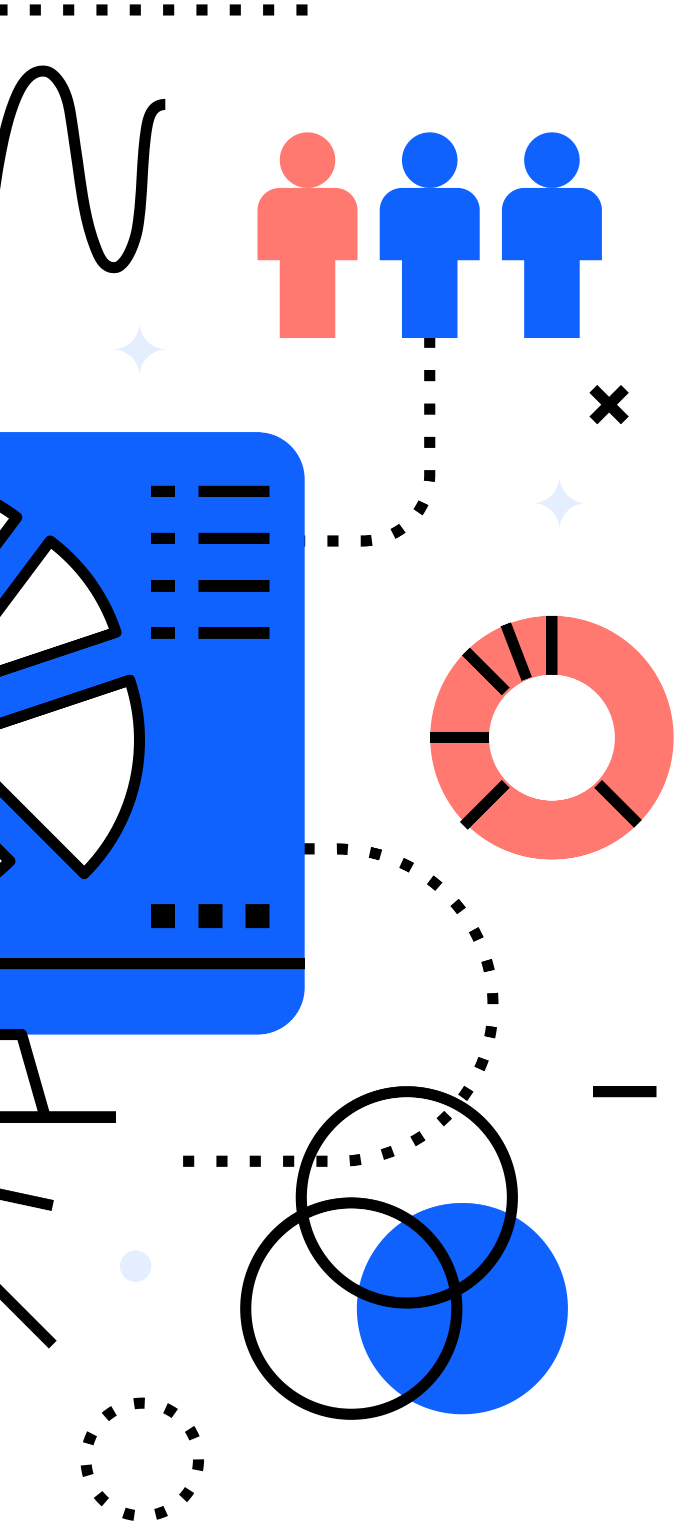
2025 SMB IT Security Insights Survey

Information Technology Security Trends for SMBs

Tech Research
a TSL Division



Introduction

Recently, TSL Marketing surveyed more than 1200 business leaders at small and medium-sized businesses (SMBs). We asked questions about IT security trends, including AI, and what they want from cybersecurity service providers.

The TSL 2024 SMB IT Security Insights Survey revealed valuable information that managed security service providers (MSSPs) can use to market IT security services to SMBs.

Table of Contents

Chapter 1......... **How SMBs Are Using IT Security**

Chapter 2......... **IT Security in the Today's Workplace**

Chapter 3......... **What Companies Want from IT Security Service Providers**

Chapter 4......... **Top IT Security Concerns**

Chapter 5......... **State of the Cybersecurity Technology Market for SMBs**

Chapter 6......... **AI Adoption and IT Security**

Chapter 7......... **State of the Infrastructure Provider Market for SMBs**

Chapter 8......... **State of the Cloud Provider Market for SMBs**

Chapter 9......... **Must-Have Security Services for SMBs**

Chapter 10........ **Conclusion: TSL's Methodology**

Chapter 1:

How SMBs Are Using IT Security

According to our research, cybersecurity is the top area of investment for today's small and medium-sized businesses (SMBs). We found that SMBs are concerned about both internal and external threats. Ransomware is the #1 security concern for mid-sized businesses.

Out of the companies surveyed, three-quarters of them plan to make annual IT security awareness training a priority. This finding aligns with ongoing concerns about ransomware, a type of attack that can be prevented through employee education.

Of the 1,285 companies we surveyed:

60%

Plan to invest in cybersecurity in the next 12 months

48%

Identified ransomware as a top 3 IT security concern

75%

Think mandatory annual employee IT security training is important

The good news for IT security service providers is that they can benefit from a thriving cybersecurity market if they target the right customers. MSSPs can capitalize on these survey findings by developing marketing campaigns that promote their ransomware prevention and security awareness training services.

Chapter 2:

IT Security in Today's Workplace

Our findings show that SMBs are using a variety of workplace environments, including remote, in-office, and hybrid workplaces that balance work from home with working from the office. Of the SMBs surveyed:

36% < 50%

work in office, with the rest working remotely

33%

Have most employees working in office

20% > 50%

work in office, with the rest working remotely

11%

Have a mostly remote workplace

With more than half of companies continuing to use hybrid workplaces, SMBs are investing in security technologies related to remote work:

56%

Plan on investing in Endpoint/Device Security

45%

Have plans to invest in Identity and Access Management (IAM)

43%

Are looking to invest in Email Threat Defense

MSSPs should keep the technology priorities of companies with different types of workplaces in mind when promoting their IT security services. IT security providers should emphasize the importance of Endpoint Detection and Response (EDR), IAM, and email security.

Technology Investments for Remote and In-Office Workplaces

When we compared our findings on work arrangements with technology investments, we found that cybersecurity is the most common investment across all work arrangements, with a higher adoption rate among remote-first firms, probably due to the risk created by distributed environments.

63%

of "Mostly all remote" firms plan on investing in cybersecurity

56%

of "Mostly all in office" firms plan on investing in cybersecurity

We also saw that firms that relied on an entirely remote workforce were more invested in cloud than those with an in-office workforce.

54%

of "Mostly all remote" companies plan on investing in cloud

32%

of "Mostly all in office" companies plan on investing in cloud

Remote companies care more about endpoint security, collaboration, and AI solutions than in-office companies.

16%

of "Mostly all remote" workplaces prioritize Endpoint/Device Security

12%

of "Mostly in-office" workplaces prioritize Endpoint/Device Security

These findings suggest that fully remote work environments prioritize securing devices to mitigate risks associated with remote access, a critical consideration for distributed workforces.

Companies with remote workplace invest in AI at a faster rate than in-office companies, while In-office teams care more about IT infrastructure, upgrading software, and networking.

IT security service firms can use this information to tailor their messaging to appeal to companies with different work arrangements. For example, marketing campaigns can target remote workplaces with AI-powered security and EDR services.

Chapter 3:

What Companies Want from IT Security Service Providers

When SMBs were asked how they would like to see IT security service providers improve their services, they responded that they want managed security services to be more affordable, responsive, and proactive. Companies expected the same things from an IT security service provider whether they used an in-office, remote, or hybrid workplace.

Companies surveyed wanted their IT security service providers to:

56%

Decrease costs

46%

Be more proactive

44%

Improve responsiveness

37%

Improve technical expertise

SMBs ask that their IT security service firms be more proactive but are not as concerned about an managed service provider's IT planning or business acumen.

Key Takeaways

In promoting their services, MSSPs should emphasize cost efficiency, as well as their ability to deliver support quickly and to anticipate and prevent problems for their customers. IT security service providers may also want to emphasize the advantages of working with a local MSSP that can respond to issues quickly both remotely and on-site.

While expertise doesn't rank as highly as cost or responsiveness, SMBs still want to work with an IT security services provider that has experience and know-how that might be lacking in an internal IT staff, such as specializations in endpoint and AI-powered security. Many SMBs have IT security skills gaps that can be bridged by outsourcing security services.

Chapter 4:

Top IT Security Concerns

When we asked the companies that participated in our survey to identify the top 3 security concerns for mid-sized businesses, ransomware came out on top, followed by data breaches and employee negligence.

48%

Ransomware

42%

Data Breaches

39%

Employee Negligence

Employee training was a close fourth at 35%, emphasizing concern with internal threats. Ransomware is related to internal security threats because attacks are often triggered by an employee opening and engaging with an infected email. Employee security awareness training can prevent ransomware attacks.

Internal threats was near the bottom of the list with 15%, indicating that companies distinguish between internal risk due to employee error versus malicious intent that would motivate an employee to steal data or sabotage systems.

Chapter 5:

State of the Cybersecurity Technology Market for SMBs

Understanding the cybersecurity technology market is crucial for MSSPs that want to reach a target audience with messaging related to the right services. To track market trends for IT security solutions, we asked the SMBs to identify which solutions they have in their infrastructure.

Of the companies surveyed:

vmware by Broadcom

42%

use VMware

FORTINET

31%

use Fortinet

paloalto NETWORKS

23%

use Palo Alto

CROWDSTRIKE

15%

use CrowdStrike

We wanted to find out more about how companies are using technology overall, so we asked what IT areas companies planned on investing in over the next 12 months. Cybersecurity ranked first by a good margin. IT infrastructure hardware and cloud computing ranked second and third respectively. AI solutions was a close fourth.

Of the companies surveyed:

60%

Cybersecurity

44%

IT Infrastructure Hardware

41%

Cloud Computing

39%

AI Solutions

IT security service firms should keep this picture of the technology market in mind while marketing their cybersecurity services.

Chapter 6:

AI Adoption and IT Security

AI is a significant technology trend that can enhance IT security, so we asked SMBs about their use of AI and Robotic Process Automation (RPA). While RPA adoption is low, many SMBs are progressing in their AI journey.

Of the SMBs surveyed:

68%

Don't have any plans to adopt RPA

46%

Have started to explore how AI can help their businesses

28%

Have some light AI implementations

15%

Have implemented at least one RPA solution

In response to these findings, IT security services firms can position themselves as experts that can help create AI roadmaps and strategies for AI-powered cybersecurity and the automation of IT security controls. Top security technology companies, such as Fortinet and Palo Alto, offer AI-powered solutions. MSSPs should promote their partnerships with these companies.

AI Adoption by Industry

The industry that a company operates in seems to affect the rate of AI adoption. For example, companies in industries with strict compliance standards, such as Finance and Healthcare, seem to adopt AI at a faster pace than other industries.

Of Finance firms surveyed:

45%

Have started to explore the benefits of AI

35%

Have some light AI implementation

Of Healthcare providers surveyed:

39%

Have started to explore the benefits of AI

31%

Have some light AI implementation

Work Arrangement and AI Adoption

Mid-sized companies with mostly remote workforces and hybrid workplaces show a higher proportion of light AI implementations than those with in-office workforces, suggesting greater agility in adopting AI technologies.

32%

of "Mostly all remote" companies have some light AI implementations

32%

of companies with Less than 50% in-office workers have some light AI implementations

22%

of "Mostly in-office" companies have some light AI implementations

Considering this information, MSSPs may want to target companies with remote and hybrid workplaces for AI-powered cybersecurity services, such as threat detection and identification.

Cloud and AI Adoption

Overall, companies that planned to invest in cloud computing technology were further along in their AI journey than companies that invest in on-premises infrastructure.

When we examined the cloud market, we learned that, while IBM Cloud captures a small share of the mid-sized market, their customers are further ahead in AI adoption than companies that go with their competitors.

Of IBM Cloud users:

38%

Have started to explore AI

20%

Have a detailed AI roadmap

18%

Have light AI implementations

The number three player Google Cloud has customers that are further ahead in AI adoption than Azure and AWS users. This difference may be due to the market dominance of Azure and AWS. Customers that are more adventurous may be willing to explore less dominant cloud providers.

20%

of Google Cloud customers have detailed AI roadmaps

12%

of AWS customers have detailed AI roadmaps

8%

of Azure customers have detailed AI roadmaps

MSSPs need to take into account the AI maturity of companies that work with specific cloud providers when promoting AI-powered security. IBM Cloud shops may be more receptive to AI security while Azure and AWS shops may need help starting or progressing in their AI and automation journey.

Chapter 7:

State of the Infrastructure Provider Market for SMBs

We wanted to track trends in the infrastructure provider market for SMBs to give IT security service providers an idea of how infrastructures are evolving and what types of environments companies need to protect.

When we asked SMBs to indicate which infrastructure providers they use, Cisco, VMware, and Dell /EMC commanded the highest market shares.

59% CISCO

53% vmware by Broadcom

45% DELL EMC

The popularity of Cisco and VMware shows that SMBs are focusing on network security and infrastructure, as well as virtual and software-defined infrastructure.

We looked at how choice of infrastructure provider aligned with an interest in cybersecurity and found that:

24%

of Cisco users plan to invest in cybersecurity

22%

of VMware users plan to invest in cybersecurity

18%

of Dell/EMC users plan to invest in cybersecurity

When marketing their infrastructure security services, IT security service firms should emphasize their partnerships with the top infrastructure security providers and the certified expertise they can offer.

Infrastructure and Cloud Providers Alignment

For IT service firms targeting prospects with a combination of tech stacks, it's useful to understand how companies align infrastructure technology with cloud.

Cloud providers Microsoft Azure and AWS and infrastructure providers Cisco, Dell/EMC, and VMware dominate the mid-market. Companies that use Azure frequently adopt VMware, suggesting a preference for virtualized environments. Azure and AWS users show a preference for Cisco solutions, indicating an interest in network security.

58%

of Azure users are VMware shops

64%

of Azure users are Cisco shops

62%

of AWS users are Cisco shops

These insights into cloud and infrastructure technology alignment can guide MSSPs in making strategic decisions when marketing infrastructure planning services for cloud and IT security technology adoption.

How Workplace Model Impacts Infrastructure Technology

Companies that have mostly remote workplaces favor Cisco infrastructure, showing a steep drop-off in use of other infrastructure providers.

Of the companies with mostly remote workplaces:

51%

use Cisco

39%

use VMware

24%

use Dell/EMC

These findings make sense due to network security challenges created by remote workplaces.

Companies that work mostly in-office use Cisco infrastructure at a similar rate to mostly remote offices but without the drop-off for the other top infrastructure providers.

54%

use Cisco

51%

use VMware

47%

use Dell/EMC

MSSPs with certified Cisco expertise can differentiate themselves when marketing their network security services to companies with either remote or in-office workplaces.

Chapter 8:

State of the Cloud Provider Market for SMBs

As cloud adoption becomes commonplace, and companies embrace more complex cloud models, such as hybrid and multicloud, we wanted to look at how the cloud provider market for SMBs is evolving.

Once again, Microsoft Azure and Amazon Web Services (AWS) dominated the cloud market for SMBs. Microsoft is still the leading cloud provider for SMBs by far, capturing over three-fourths of the market, with AWS coming in as a strong second.

Of companies surveyed:

76% Microsoft Azure

45% aws

19% Google Cloud

Google Cloud earned a respectable share of the cloud market, with other providers taking a sliver of the pie.

10%

Chose "Other"

5%

Don't use a cloud provider

3%

Use IBM Cloud

This picture of the cloud provider market should help IT security service providers create marketing strategies that play to their certified expertise in delivering leading cloud security services.

Cloud Market by Industry

When we compared AWS and Azure adoption by industry for 12 key verticals, we saw some separation between these top cloud providers and the others as they perform particularly well in the Retail, Financial, and IT industries.

Of the companies surveyed:

73%

of Finance firms use Azure

71%

of IT companies use Azure

64%

of Retailers use Azure

Of the companies surveyed:

52%

of Retailers use AWS

60%

of Finance firms use AWS

57%

of IT companies use AWS

When developing marketing strategies, MSSPs that have experience working with these key industries should promote their expertise in Azure and AWS security and compliance.

Cybersecurity Measures for Cloud Users

When we looked at what security measures SMBs that are adopting the cloud plan to prioritize, we found that they are likely to invest in cloud security with almost half choosing Cloud Application Security.

48%

Cloud Application Security

13%

Multicloud Defense

While the top security measures chosen by cloud users aligned with our overall findings, MSSPs should remember to promote cloud security services to companies that have adopted the cloud.

Chapter 9:

Must-Have Security Services for SMBs

When asked which security measures were important for companies of their size and industry, SMBs put IT security training at the top of the list. A formal incident response plan and annual security audits were neck-and-neck at second place.

75%

Mandatory Annual Employee IT Security Training

68%

Comprehensive and Documented Incident Response Plan

68%

Annual Security Audit

Security Measures and Technology Adoption

We compared our findings regarding preferred security measures to technology adoption and discovered that cybersecurity adoption is strongly correlated with a focus on proactive security measures, such as Endpoint/Device Security and Employee IT Security Training.

Of companies that prioritize cybersecurity technology adoption:

82%

chose Mandatory Annual Employee IT Security Training

75%

chose Annual Security Audit

61%

chose Endpoint/Device Security

These priorities are important for MSSPs to keep in mind when marketing their cybersecurity services. Offering security awareness training, incident response plans, and security audits could be an important differentiator for an IT security firm.

TSL's Methodology

In conducting the IT security survey, TSL targeted small and medium-sized businesses, surveying 1,285 respondents. The businesses surveyed had between 500 and 1,000 employees.

SMBs in 12 traditional industries, including healthcare, finance, and information technology, were surveyed, as well as those in a wide variety of niche industries.

Get expert advice on how to tailor your marketing strategy to the needs of SMBs. Request a proposal from TSL Marketing.

Ask for a Proposal

Tech Research
a TSL Division