Guardz.

2025 State of SMB Cybersecurity Report

Real world insights from 800 small and mid size businesses, outlining the changing risk & operations landscape for MSPs

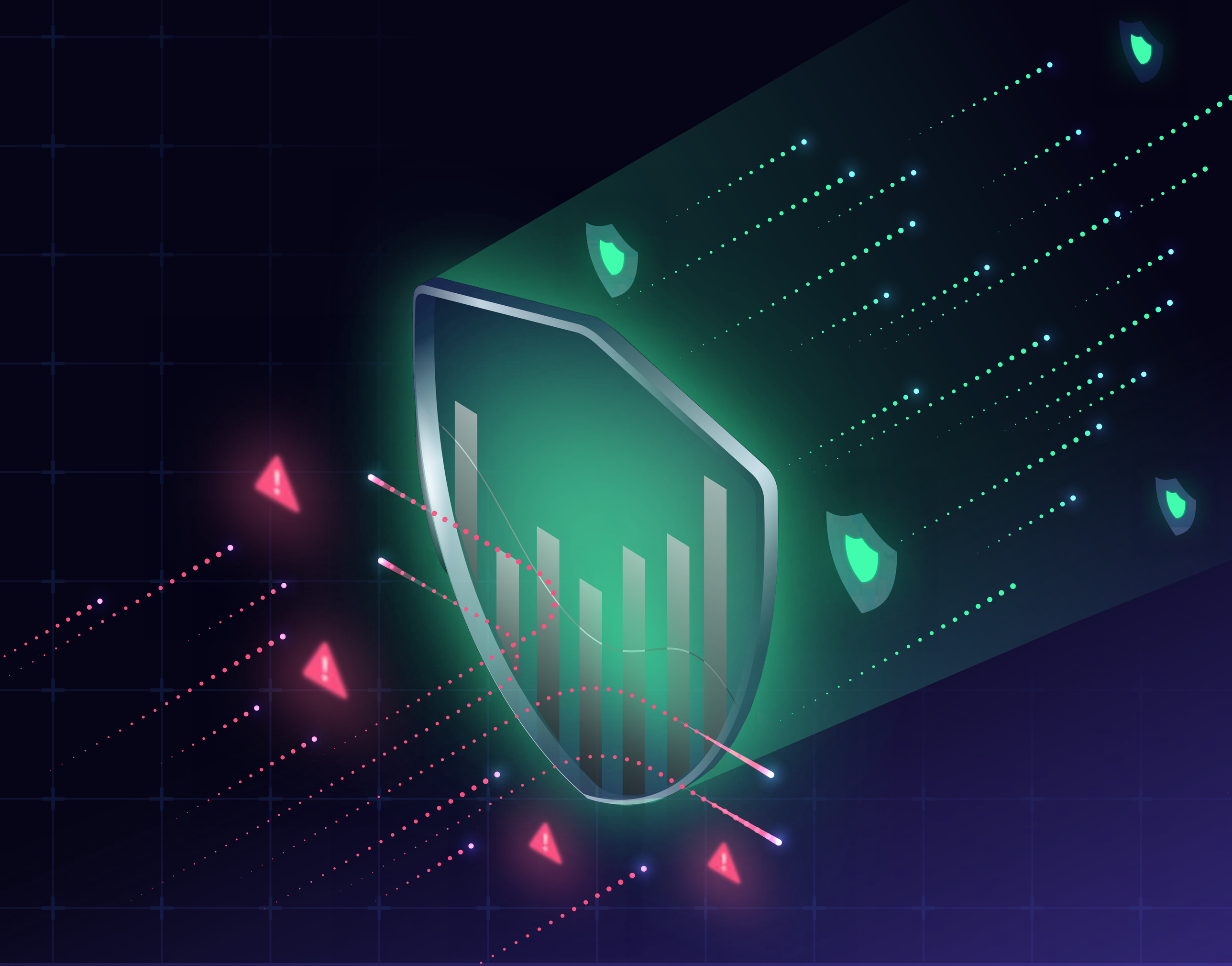


Table of Contents

Executive Summary 3

Preface From the Head of Security Research at Guardz 4

Introduction 5

Clear and Present Danger: 1 in 2 SMBs Targeted Already 5

Healthy Cyber Awareness, Weak Preparedness 6

Where SMBs Are Struggling Most and What’s Coming Next 7

The Reality of SMB Cyber Operations: Fragmented, Exhausted, and Overextended 8

The Opportunity for MSPs Has Never Been Clearer 9

Key Takeaways 10

Executive Summary

Small businesses are facing more cyber pressure than ever. About half of SMBs have already experienced a cyber incident. **A full 61% believe the future holds even greater cyber risk.** Budgets are rising, concerns are escalating, and threats are increasing faster than most businesses can keep pace. The reality is that **only 34% have a professionally built incident response plan**.

Yet there is a positive takeaway. 80% of SMBs that had an incident plan in place were able to avoid significant damage. That number highlights what MSPs already know: preparation is everything.

This benchmark report translates survey data into a clear, actionable view of SMB risk, readiness, and the growing demand for trusted cybersecurity partners.

Key Takeaways

- **50%** of SMBs have already experienced a cyber incident
- **80%** of impacted SMBs avoided major damage because they had an incident plan
- **45%** say human error is their top vulnerability
- **61%** believe cyber risk will increase
- **52%** would work with an MSP due to fear of attacks

Methodology

The study gathered responses from 800 U.S.–based SMB owners, each representing businesses with more than ten employees, across a diverse range of industries, including retail, healthcare, finance, manufacturing, education, and technology. Respondents completed the survey answering a combination of single-selection, multi-selection, and matrix-style questions designed to measure cybersecurity readiness, perceived risks, incident experience, and engagement with MSPs. Results were provided with both raw counts and stratified weighting to ensure proportional representation of industries.

Preface From the Head of Security Research at Guardz

I'm pleased to introduce this year's Guardz State of SMB Cybersecurity Report. Over the past year, our research team has observed a rapid shift in threat patterns, particularly in areas such as identity misuse, automation, and the widening gap between attacker capabilities and SMB defenses. The findings from a survey of 800 SMBs echo what we see every day and bring the SMB experience into the trends shaping the year ahead.

Our goal is straightforward. Turn what we learn from real incidents, telemetry, and daily investigations into clear guidance MSPs can use to protect the businesses that rely on them.

The following two points highlight the most significant shifts we saw in 2025

1. AI-powered attacks are expected to hit SMBs with unprecedented force in 2025. Automated phishing farms, synthetic identities, and machine-speed reconnaissance turned small businesses into high-yield targets. Most SMBs admitted their exposure jumped, while true security controls remained largely absent.
2. The financial blast radius of breaches expanded. A single compromise in 2025 often triggered operational paralysis, deep forensic work, and expensive recovery cycles. For many SMBs, the real cost of an incident now lands well into six and seven-figure territory.

Predictions for 2026

2026 is shaping up to be the year identity becomes the frontline. Adversaries are expected to bypass endpoints and email entirely, targeting cloud identities, session tokens, and misconfigured access paths. At the same time, workspace security is evolving from device-centric controls to continuous identity validation, application trust, and real-time context checks. SMBs will need to reinforce identity governance, tighten control over automated workflows, and rebuild trust models across their supply chain to withstand the next wave of attacks.





Elli Shlomo

Head of Security Research

Security Researcher and Microsoft Security MVP who turns complex threats into practical defense tactics for modern security teams.

Introduction

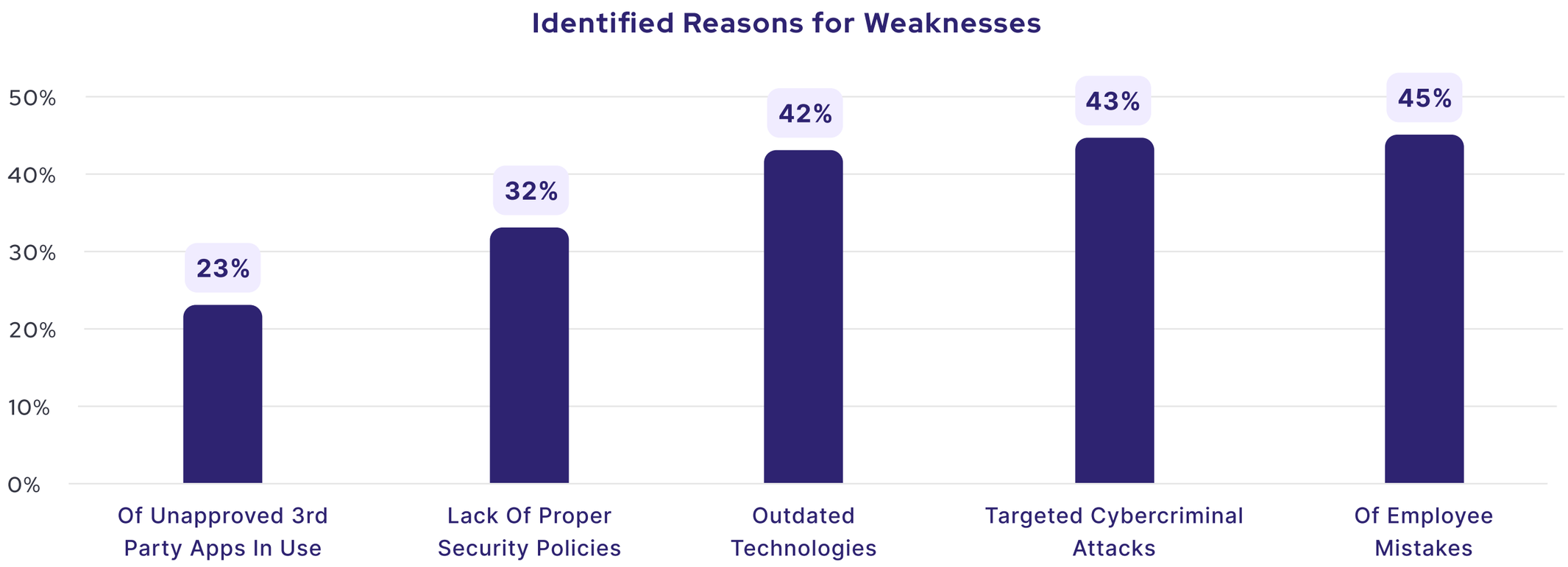
In 2025, SMBs find themselves operating in a threat landscape that moves faster than their defenses. AI-powered attacks are becoming increasingly mainstream, and many SMBs still underestimate how disruptive a real attack can be. They assume they're too small to be targeted, and by the time they realize otherwise, the damage is already in motion.

To understand the real challenges SMBs face, Guardz surveyed 800 SMB leaders across industries. This report highlights the most pressing risks, where SMBs are struggling, and the key opportunities for MSPs to provide real, measurable protection.

1 Clear And Present Danger: 1 In 2 SMBs Targeted Already

According to the survey, about 50% of SMBs have already been breached or attacked.
That means 1 out of every 2 is dealing with real fallout, not hypothetical scenarios.

All identified weaknesses by SMBs are solvable



These figures underscore a significant reality: SMBs are not compromised by a lack of will, but rather by operational limitations. The identified weaknesses represent preventable vectors that persist due to insufficient time, inadequate policy enforcement, and a lack of subject-matter expertise.

Why This Matters - Limited Time And Expertise Keep SMBs Vulnerable

The diversity of weaknesses highlights a need for a depth of specialization that often extends beyond the scope of traditional in-house SMB IT, underscoring the importance of a managed service provider in effectively addressing these vulnerabilities.



2 Healthy Cyber Awareness, Weak Preparedness

Half of SMBs believe that their cybersecurity needs are increasing, and many have raised budgets accordingly. However, one in three SMBs operates with a financial blind spot, unable to quantify per-employee security investment.

Money is being invested in cybersecurity, but not necessarily in the right places. As a result, Incident preparedness is critically underdeveloped

34%
have a formal incident response plan

28%
rely on informal processes

15%
have no plan at all

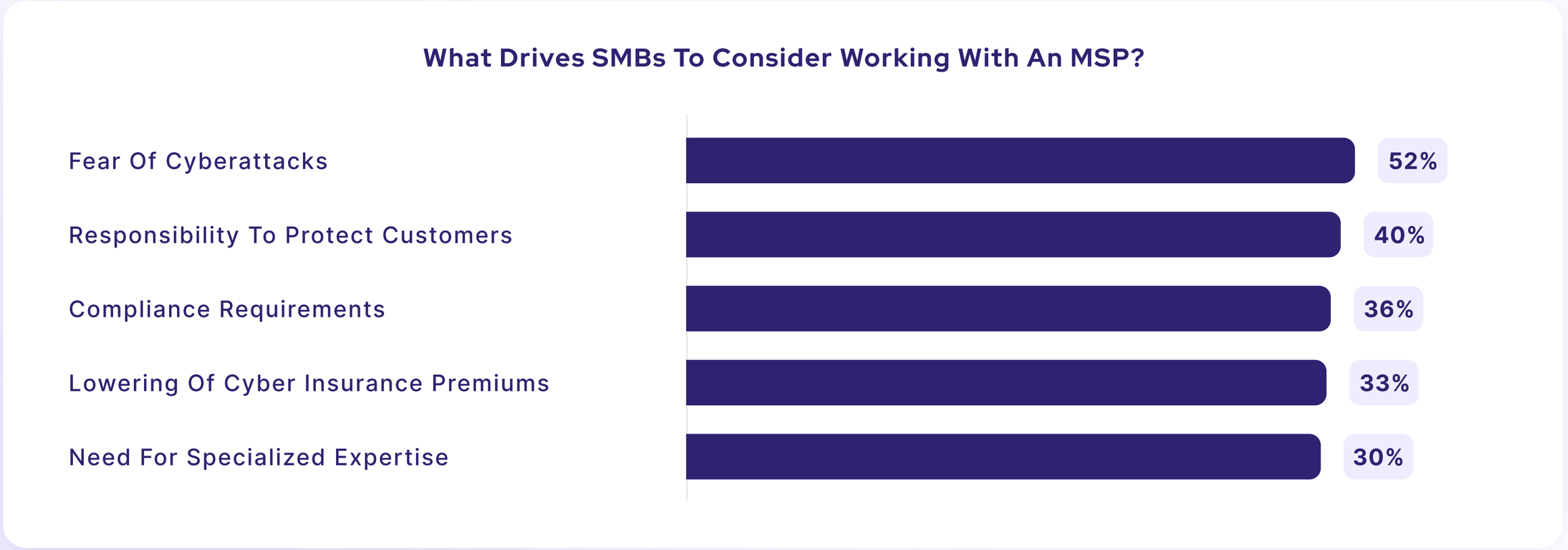
42%
of SMBs are reacting to incidents, rather than preparing for them

Who handles incidents when something goes wrong?

- **33%** of business owners handle alerts themselves
- **13%** offload alerts to untrained employees
- **Only 14%** rely on an external cybersecurity provider

When untrained staff or busy owners manage incidents, attackers gain time and leverage. Organizations with defined processes perform dramatically better. In fact, **80% of SMBs with an incident plan avoided major damage**, reinforcing the value MSPs bring in building and managing those plans.

Motivations to partner with MSPs



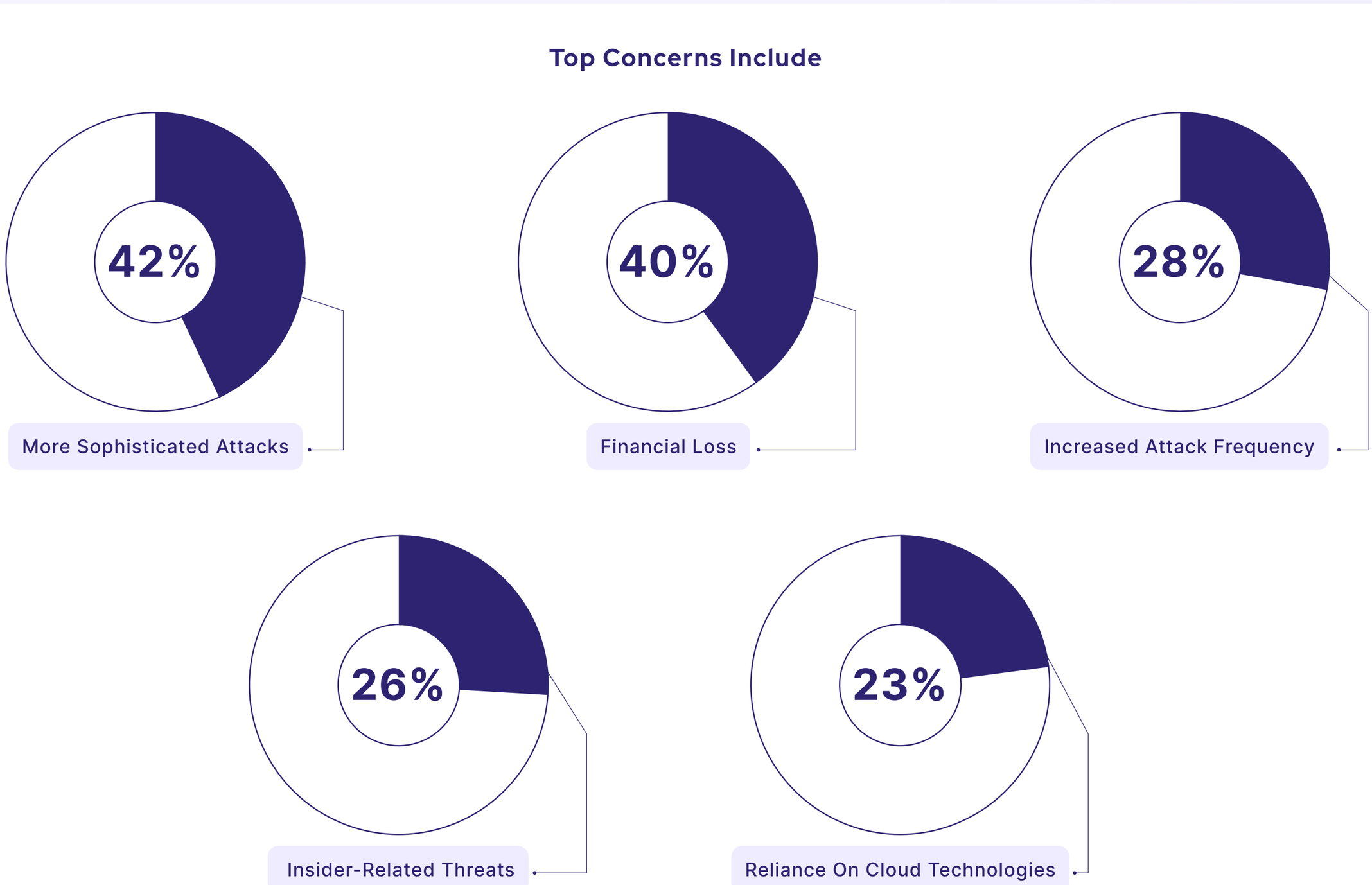
Why this matters - Awareness Strengthens, Readiness Falls Short

Processes and preparation are no longer optional. SMBs are aware of the risks, but without a structured defense plan, they can't convert awareness into protection. MSPs fill that exact gap.



3 Where SMBs Are Struggling Most and What's Coming Next

There is a prevailing consensus regarding the trajectory of the threat landscape: **61% of SMBs acknowledge that the future will be characterized by escalating cybersecurity risks.**



Why this matters - Bigger Threats Ahead, Bigger Need for MSPs

SMBs are worried about exactly the problems MSPs are built to solve.

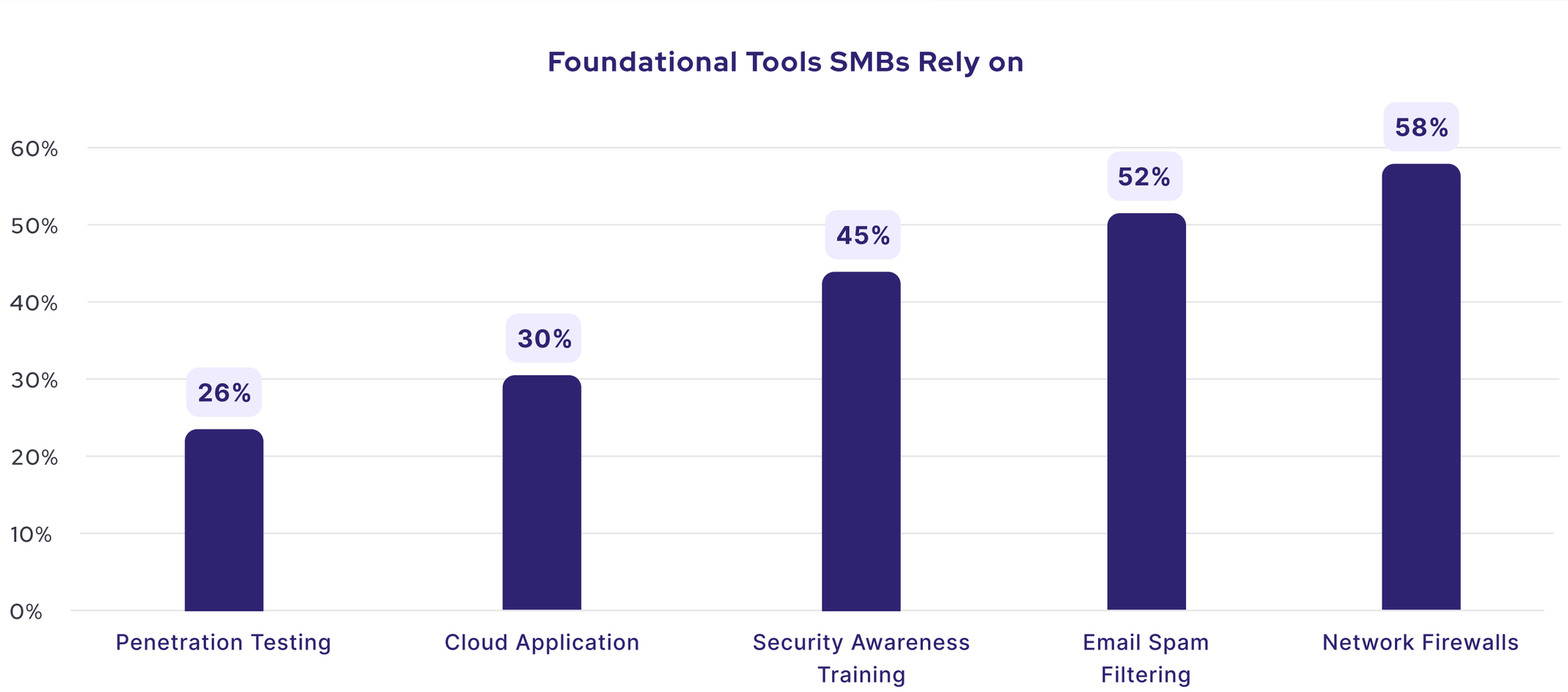
Demand is strong. SMBs are simply searching for the right partner.



4 The Reality Of SMB Cyber Operations: Fragmented, Exhausted, And Overextended

While many SMBs rely on foundational tools like network firewalls (58%) and email spam filtering (52%), adoption drops sharply for more advanced measures. **Fewer than half provide employee security awareness training (45%)**, less than a third use cloud application security tools (30%), and only a quarter conduct regular security assessments or penetration testing (26%).

In summary, the necessary toolsets are present, but coverage remains uneven, and integration is limited. Operational responsibility is dispersed across too many stakeholders, reducing overall effectiveness.



Business owners managing alerts, employees making policy decisions on the fly, and scattered security tools create operational drag and invite risk.

Why This Matters - Too Many Tools, Too Little Protection

Fragmentation leads to blind spots. Blind spots lead to breaches.
SMB security ecosystems are too scattered to defend against the complexity of modern cyber threats.



5 The Opportunity for MSPs Has Never Been Clearer

The SMB ecosystem recognizes the gaps and seems to be making somewhat of a change as engagement with MSPs increases. And the data makes it clear that SMBs are looking for that support.

MSPs can close every major gap revealed in this survey

- ✓ Policy Development & Enforcement
- ✓ Consolidated Technology Stacks
- ✓ Incident Response Planning
- ✓ Faster Detection & Resolution
- ✓ Employee Training & Awareness
- ✓ Insurance Readiness
- ✓ Dedicated Monitoring
- ✓ Regulatory Alignment

Why This Matters - A Turning Point For MSP Driven Security

This shift in SMB mindset signals a turning point for the industry. As businesses reassess their security posture, MSPs have a rare chance to reshape how cybersecurity is delivered, moving from ad hoc support to long term strategic partnership.



What the Data Really Tells Us

> The biggest gap we see is not awareness, it's operational limitations. SMBs seem to be struggling to keep pace with modern threats. MSPs equipped with AI augmented protection are becoming the essential security backbone that keeps these businesses operational, resilient, and ready to scale.

Elli Shlomo

Head of Security Research

Takeaways from the 2025 State of SMB Cybersecurity Report

Awareness vs. Readiness Gap

The findings from this year's survey reveal a widening divide between SMBs' awareness of cyber risk and their ability to manage it effectively. While budgets are rising and concern is at an all-time high, most SMBs continue to operate without the structure, expertise, or protections required to defend against modern threats, painting a clear picture of where support is most urgently needed.

Recognizing the Stakes but Lacking Capability

SMBs are signaling that they understand the stakes. They anticipate greater risk in the year ahead and acknowledge that their existing tools, training, and internal processes are insufficient. Yet many still rely on business owners or untrained staff to oversee complex security responsibilities. This disconnect leaves organizations vulnerable to preventable incidents stemming from human error.

Systemic Barriers to Resilience

The data also highlights systemic challenges that make it difficult for SMBs to close these gaps alone. Low per-employee investment, limited visibility into actual spend, inconsistent use of foundational security controls, and the absence of incident response plans collectively hinder resilience. Even when attacks occur, many organizations lack the resources to determine root causes, implement improvements, or prevent future recurrence.

Growing Openness to External Support

At the same time, the survey underscores growing openness among SMBs to external support. Fear of cyberattacks and a sense of duty to protect customers and partners are key motivators driving interest in managed security services. These findings illustrate a pivotal moment where rising pressure meets a clear demand for capable, specialized guidance.

A Strategic Opportunity for MSPs

For MSPs, these insights validate what many already observe in the field: SMBs recognize the risks but remain under protected, overwhelmed, and underserved. The vulnerabilities outlined in this survey demonstrate why comprehensive, identity-aware, AI-enabled protection is no longer optional for businesses operating in today's threat landscape. MSPs equipped with modern security platforms are uniquely positioned to help organizations close critical gaps, strengthen resilience, and confidently navigate the year ahead.

Discover the power of the Guardz platform for your MSP business.

Book a Demo

Watch On Demand Demo