SOPHOS

Addressing the cybersecurity skills shortage in SMBs

Exploring the frontline impact of the cybersecurity skills shortage on small and mid-sized businesses and how to address these challenges within resource and budget constraints.

A Sophos Whitepaper. October 2024

Introduction

The global shortage of cybersecurity skills is well known and well documented. It's also not going away any time soon, making it essential that small and medium-sized organizations take steps to address its impacts.

Understanding the challenge is the first step to addressing it. This report shares findings from an independent survey of frontline practitioners around the globe, revealing how the skills shortage impacts small and medium-sized organizations on a day-to-day basis. Based on these insights, it provides practical guidance for addressing these challenges within existing resource and budget constraints. It also explores the Sophos solutions that enable smaller organizations to achieve better cybersecurity outcomes.

About the survey

Sophos commissioned an independent, vendor-agnostic survey of 5,000 frontline IT/cybersecurity professionals across 14 countries. 1,402 respondents work in organizations with between 100 and 500 employees, the segment considered small and medium-sized businesses (SMBs) in this report. The research was conducted in the first quarter of 2024.

Smaller organizations are disproportionately impacted by the skills shortage

The skills shortage weighs heavily – and disproportionately – on SMBs. The survey reveals that **organizations with fewer than 500 employees perceive a shortage of in-house cybersecurity skills/expertise as their second biggest single cybersecurity risk**, topped only by zero-day threats. In contrast, for those with more than 500 employees, it ranks seventh.

Relative ranking of "shortage of in-house cybersecurity skills/expertise" as a cybersecurity risk to the business

SMBs (n=1,402)	LARGER ORGANIZATIONS (n=3,598)	
100 – 500 EMPLOYEES	501 – 1000 EMPLOYEES	1001 – 5000 EMPLOYEES
#2	#7	#7

Who/what do you consider to be your organization's top three cybersecurity risks? Relative positioning of "shortage of in-house cybersecurity skills/expertise" among the responses ranked first (base numbers in the chart)

While organizations of all sizes are impacted by the skills shortage, it's clear that SMBs feel its impact most sharply. Risks that rank highly for larger organizations, such as a shortage of cybersecurity tools (#2 perceived risk for those with 501-1,000 employees) and stolen access data and credentials (#2 perceived risk for those with 1,001-5,000 employees), are secondary concerns for smaller businesses that are struggling with the more foundational challenge of having people to operate their existing investments.

Skills shortage: a two-headed challenge

The simple truth behind the skills shortage is that there are insufficient skilled cybersecurity professionals. This impacts SMBs in two ways: lack of expertise and lack of capacity. The exact balance between the two will vary from organization to organization.

Lack of expertise

Cyber threats and security technology are complex. Doing cybersecurity well is an advanced skill that requires high degrees of expertise – and the bar keeps getting higher and higher. As cyberattacks continue to get more complex, a greater level of expertise is needed to stop them.

The survey reveals that **96% of those in smaller businesses find at least one aspect of investigating suspicious alerts challenging**. While larger organizations also often struggle with security operations, the challenge is greatest in SMBs, as illustrated in the chart below.

Percentage of organizations that find security operations tasks challenging

SECURITY OPERATIONS TASKS	SMBs (n=1,402)	LARGER ORGANIZATIONS (n=3,598)	
	100 – 500 EMPLOYEES	501 – 1000 EMPLOYEES	1001 – 5000 EMPLOYEES
Identifying which signals/ alerts to investigate	74%	67%	65%
Prioritizing which signals/ alerts to investigate	71%	67%	66%
Getting sufficient data to identify if a signal is malicious or benign	73%	66%	67%
Keeping accurate records of investigations	72%	62%	64%
Remediating malicious alerts or incidents in a timely way	75%	68%	67%
Identifying the root cause of the incident i.e. how the adversary entered the organization	73%	68%	69%
Organizations that find at least one aspect of security operations challenging	96%	95%	94%

If your organization investigates security alerts in-house, how challenging are the following steps for your organization when investigating suspicious alerts? "Very challenging" and "Somewhat challenging" (base numbers in chart)

The practicality of developing cybersecurity expertise presents a particular challenge for those working in SMBs. When only a handful of people are on the IT/security team, taking regular time out for ongoing education is challenging. Furthermore, with fewer co-workers, individuals have less opportunity to benefit from peer-to-peer learning.

Lack of capacity

Adversaries don't work a 9-5, making cybersecurity a round-the-clock requirement. In fact, 91% of ransomware attacks start outside standard business hours as attackers look to penetrate organizations without being detected[1].

Feedback from frontline operators suggests that delivering 24/7 cybersecurity coverage requires a minimum of four or five full-time staff to allow for holidays, sickness, and weekend coverage. For most SMBs, this is simply unachievable through in-house resources alone.

Illustrating this point, the survey reveals that **one-third (33%) of the time, SMBs have no one actively monitoring, investigating, and responding to alerts**. Without an active responder, smaller organizations are widely exposed to attack.

33%
of the time SMBs have no one monitoring and investigating security alerts

Over the last year (including nights, weekends, and holiday periods), what percentage of the time did your organization have an active responder monitoring and investigating security alerts? n=1,402 organizations with 100-500 employees.

1 Stopping Active Adversaries: Lessons From The Cyber Frontline, Sophos

The impact of the cybersecurity skills gap on small businesses

The skills shortage impacts SMBs in many ways. They are the segment most likely to have data encrypted in a ransomware attack, with 74% of incidents resulting in data encryption. This likely reflects their lower ability to detect and stop adversaries before the ransomware can be detonated.

Percentage of ransomware attacks that resulted in data encryption

SMBS (n=1,402)	LARGER ORGANIZATIONS (n=3,598)	
100 – 500 EMPLOYEES	501 – 1000 EMPLOYEES	1001 – 5000 EMPLOYEES
74%	72%	66%

Source: The State of Ransomware 2024, Sophos. Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Yes. Base numbers in the chart.

Furthermore, with fewer people to share the cybersecurity load, the potential for talent burnout is high. In separate Sophos-commissioned research across Asia Pacific and Japan, **85% of organizations stated they experience fatigue and burnout among their cybersecurity and IT professionals**, with almost 1-in-4 (23%) experiencing it "frequently", and 62% "occasionally". Troublingly, 90% of companies state burnout and fatigue have increased in the last 12 months, 30% of these saying the increases have risen "significantly".

85%
of organizations reporting fatigue and burnout among their cybersecurity or IT professionals

How to address the small business skills gap

Hiring more people is simply not a viable option for most SMBs. Bringing in additional cybersecurity staff is a considerable budget ask and one that will have a disproportionally higher impact on headcount budgets in smaller organizations than in larger ones. At the same time, organizations are in competition for a limited pool of talent. People with in-demand skills can be selective, often preferring to work in larger organizations that offer greater peer-to-peer development opportunities. The solution to addressing the expertise and capacity challenges is to work with third-party security specialists and use cybersecurity solutions designed for SMBs.

Work with third-party security specialists

Engaging third-party cybersecurity specialists is often the easiest and most cost-effective way to add expertise and capacity. The two most common approaches are using managed detection and response (MDR) services and managed service providers (MSPs).

MDR services typically provide 24/7 expert-led threat hunting, detection, and response across your environment. Analysts monitor your organization, identifying and responding to suspicious activity and neutralizing attacks before they impact your business.

Look for a provider that adapts to your needs and preferred way of working, whether you want to fully-outsource threat detection and response or collaborate with your provider's analysts. And, with budgets invariably tight, it's important to work with a service that can leverage your existing security technologies – avoiding the cost and disruption of rip-and-replace.

To help fund MDR services, you can look to unlock savings from your cyber insurance provider. MDR users are widely considered "tier one customers" by insurance providers because they are at a lower risk of making a claim. As a result, insurers typically offer material discounts to organizations using MDR services – money that can be redirected to fund the service itself.

Sophos case study: non-profit organization with 350 staff

A non-profit organization in North Carolina, U.S. with 350 employees was able to reduce their cyber insurance premium by $8,000 because they were using the Sophos MDR service. With their annual Sophos MDR subscription coming in at $8,467, the insurance savings meant they could enjoy 24/7 expert-led threat detection and response for an incremental spend of just $467.

For many years, **MSPs** have been providing IT and cybersecurity support to the smallest businesses, acting as their in-house team. As cyber threats increase in complexity, medium-sized organizations are increasingly choosing to work with MSPs to supplement their in-house resources.

MDR and MSPs are not mutually exclusive; separate Sophos research reveals that most MSPs (81%) offer MDR services,[2] enabling you to benefit from both layers of support through a single provider. Some MSPs choose to deliver MDR services solely in-house while others prefer to leverage third-party specialist MDR providers.

Choose solutions actively designed for SMBs

Most cybersecurity solutions are designed and built for larger organizations with extensive teams to deploy and manage them. While using enterprise-level solutions may sound appealing, smaller organizations often struggle to see security and return on investment (RoI) benefits from these solutions as they are unable to use them effectively.

Instead, look for security tools that are technically advanced under the hood but designed to be easy to use by stretched real-world IT teams. Switching purchase focus should not increase spending – and may even offer the opportunity to reduce both technology and management expenses. When evaluating security solutions, consider both platform and product features.

Platform

- A cybersecurity platform is a centralized tool that enables you to deploy, monitor, and manage multiple cybersecurity solutions in one place, for example, your endpoint protection/antivirus security, email security, and firewall.
- Consolidating your cybersecurity solutions in a single platform considerably reduces day-to-day admin overheads – no need to jump from console to console to see what's going on. Reducing the number of providers you work with helps reduce vendor management overhead.
- An effective platform will also allow your security solutions to work together, sharing telemetry, insights, user-based policies, and more to elevate your cyber defenses.

Product features

- Vendors present long lists of features and capabilities on their websites. Before evaluating solutions, take time to understand exactly what you do and do not need to avoid paying for technologies that you will not benefit from.
- To get the most from your cybersecurity investments, you need to be able to deploy and use them effectively. Choose solutions that automatically deploy recommended settings from day one, eliminating the need for time-consuming and risky manual configuration. Also, look for intuitive controls designed for real-world environments that are easy to use.
- Security tool misconfiguration is a major risk for SMBs. Maintaining good posture is essential for your ongoing security, which means choosing solutions that provide easy-to-understand visibility into sub-optimal deployments and quick-fix support.
- As a smaller business, your team is unlikely to be able to focus solely on cybersecurity. This makes it particularly important to choose solutions that automatically respond to attacks, taking action until you can step in.

2 MSP Perspectives 2024 - Sophos

How Sophos can help

Sophos has deep experience in securing small and medium-sized organizations from advanced cyber threats and we have purpose built many of our products and services to specifically address their needs.

Third-party security specialists

MDR

Sophos is the world's most trusted MDR service, securing more small businesses than any other provider. We have extensive insights into attacks on small businesses and leverage telemetry from across our customer base to elevate protection for all users.

The Sophos MDR service is top-rated by customers and analysts alike. Recent recognition includes:

- Gartner® Peer Insights™ Customers' Choice for the last two years, with a 4.8/5 rating across 647 reviews as of September 17, 2024
- G2 Leader for MDR, including the #1 rated MDR solution among mid-market customers
- IDC MarketScape named Sophos a Leader for Worldwide Managed Detection and Response (MDR) in their 2024 Vendor Assessment

"Where organizations are seeking an MDR provider with deep security expertise and a human-led service that engages with them from the outset until an incident has been resolved, Sophos represents a compelling option."
- Richard Thurston, Research Manager, European Security Services, IDC

MSP

Sophos has a large and fast-growing ecosystem of MSP partners who provide Sophos products and services – including Sophos MDR – to SMBs around the globe.

Solutions actively designed for SMBs

Platform

Sophos Central is the largest, most scalable cloud native AI-powered platform in the industry. It's used to manage all Sophos next-gen cybersecurity solutions, including Sophos Endpoint, Sophos Firewall, Sophos XDR, Sophos MDR, Sophos Email, and Sophos ZTNA. Integrations with a broad range of non-Sophos technologies, including Microsoft and Google, ensure that customers can see full value from their existing security investments.

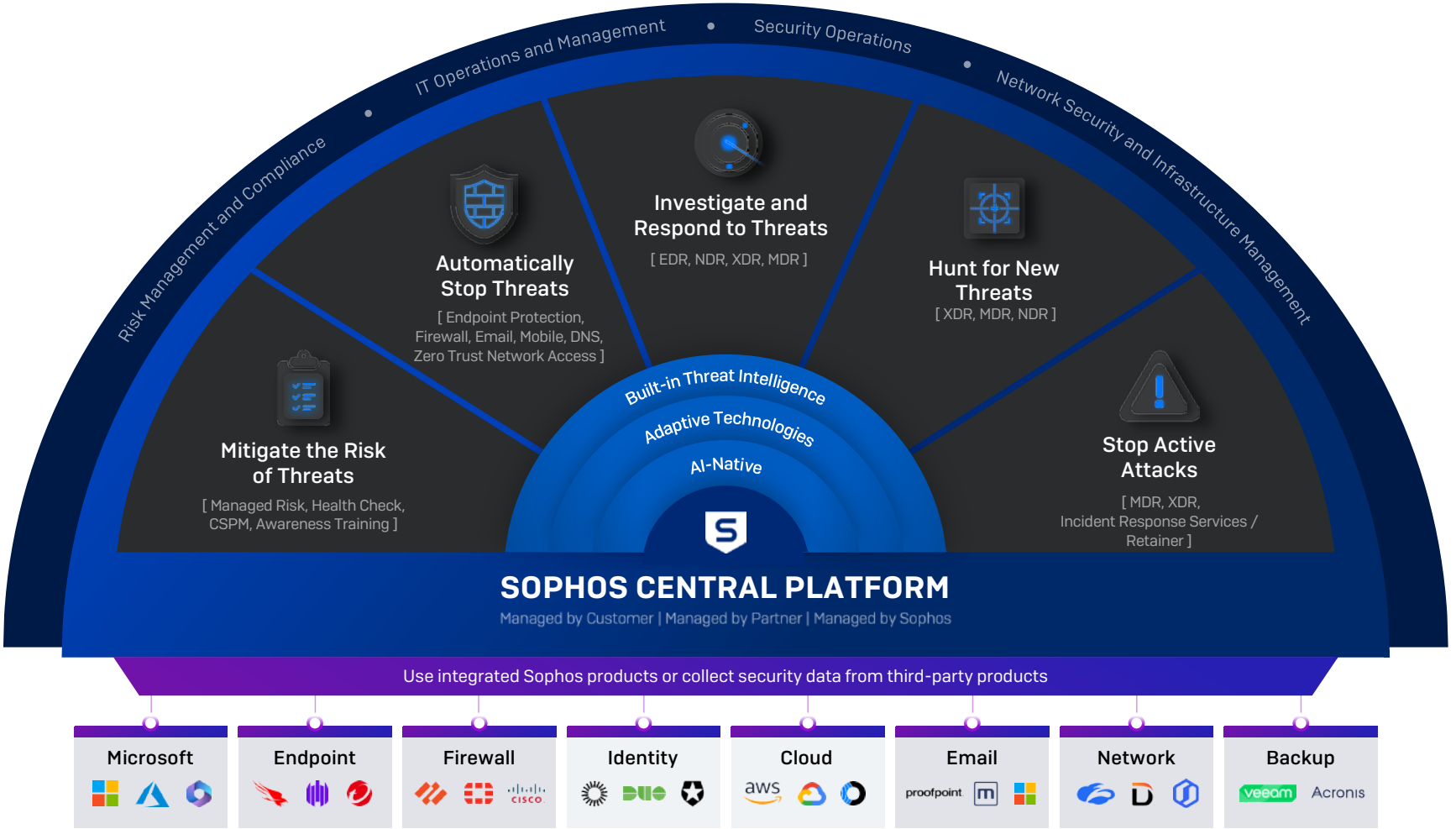
Product features

Sophos solutions are highly sophisticated and powered by decades of experience in stopping cyberthreats. They are also designed for ease of use, ensuring organizations of all sizes and resourcing levels benefit from market-leading defense capabilities.

Examples include:

- **Sophos Endpoint** automatically deploys with recommended settings, including our market-leading ransomware protection and anti-exploitation capabilities – no manual fine-tuning needed.
- **Sophos Firewall's** centralized management and reporting enables you to manage multiple firewalls in one place, which is particularly useful for organizations with dispersed sites.
- **Sophos Endpoint** includes adaptive defenses that detect the presence of adversaries in your environment and automatically respond, elevating your defenses and buying you time to respond.
- **Sophos Endpoint's** built-in Account Health Check provides clear, real-time visibility of security posture together with a Fix Automatically button that enables you to return to recommended settings in a single click.
- **Sophos Firewall's** integration with the broader Sophos platform enables it to automatically block active threats and coordinate a response across endpoints and ZTNA, as well as switches and wireless access points to prevent lateral movement.

The Sophos cybersecurity platform



Conclusion

The survey reveals that the cybersecurity skills shortage weighs heavily on small and mid-sized organizations. The resulting lack of skills and capacity has a material impact on businesses' abilities to defend themselves from attacks. With no end to the resourcing gap in sight, smaller organizations would be wise to take steps to mitigate its impacts by working with third-party specialists and choosing solutions specifically designed for their businesses.

To learn more about Sophos solutions for small and mid-sized organizations, speak to your Sophos representative or partner or visit www.sophos.com.

Gartner and Peer Insights™ are trademarks of Gartner, Inc. and/or its affiliates. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

© Copyright 2024. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2024-10-01 (WP-NP)

SOPHOS