White Paper

Leveraging Managed Detection and Response to Achieve Effective Security Outcomes and Business Value

Sponsored by: Sophos

Cathy Huang Craig Robinson

October 2023

IN THIS WHITE PAPER

As organizations bolster their digital-first business strategies, their reliance on technology to achieve strategic competitive advantage ramps up significantly. IDC's research shows that tech buyers are increasingly prioritizing cybersecurity and cyber-recovery capabilities because they are critical and strategic in ensuring an organization's digital success.

Global and local regulations continue to drive significant changes in accountability and the relationship between cybersecurity leaders and their board of directors. Small and medium-sized businesses (SMBs) are no different from large companies in needing to demonstrate strong security posture and compliance throughout their supply chain. New regulations including the recently announced final rules on disclosure of material cybersecurity incidents and annual cybersecurity risk management strategy and governance reporting by U.S. Securities and Exchange Commission will have a profound effect on cybersecurity risk management, strategy, governance, and incident disclosure.

AT A GLANCE

- 46% of CEOs rated "cybersecurity threats" as the greatest risk in 2023.
- The average number of cyberattacks experienced over the past 12 months is 3.8.
- Nearly 40% of all organizations indicate the need for substantial improvement in their ability to detect, investigate, and respond to threats.
- Insufficient testing of cybersecurity plan and lack of budget for cybersecurity were equally ranked as the top challenge for managing cybersecurity for SMBs.

SITUATION OVERVIEW

Cybersecurity Is the Top Business Priority

Many organizations need to reevaluate their approach to cybersecurity. The COVID-19 pandemic had a dramatic effect on where and how work is accomplished, and cybersecurity teams need to adapt to the new reality. Budget allocation needs to align to heightened awareness of the risk profile. The board's ability to recognize and push for ways to reduce the cyber-risk of the organizations that they engage with will increasingly become the norm.

October 2023, IDC #US51259723

About half of the organizations that IDC studied have experienced malicious infiltration, 20% of organizations have experienced ransomware attacks over the past 12 months, and the average number of cyberattacks experienced over the past 12 months is 3.8. Despite spending $213 billion globally on security technology and services (based on IDC's latest Security Spending Guide for 2023), many CEOs are not feeling equipped to make decisions when cyberattacks occur. According to IDC's January 2023 *CEO Survey* (n = 165 NA CEOs), 46% of CEOs from North American organizations rated "cybersecurity threats" as the number 1 risk in 2023, which is greater than macroeconomic headwinds (see Figure 1).

On a positive note, cybersecurity focus and attention from the board has increased over the years. In 1Q23, IDC conducted a North American MDR survey to better understand organizations of various sizes and industries' decision-making processes as well as expectations and preferences when it comes to managed detection and response (MDR) services. In the survey, almost 6 out of 10 organizations rate their board of directors' engagement in cybersecurity initiatives as high or very high. It is clear cybersecurity is becoming much more of a business priority and not just an IT priority.

FIGURE 1

CEOs' Greatest Risks in 2023: Cybersecurity Threats — the Top Concern

"Cyber is one of these long-term things that might not produce immediate results or, if you don't do something, it produces immediate negative results. But on those things, the CEO should be more involved. The more something has a longer-term impact, the more important it is for the CEO to be on top of it. Like climate change, for example." — CEO of a $4 billion U.S. company

n = 165 North American CEOs

Source: IDC's *CEO Survey,* 2023

Nonetheless, as cybersecurity becomes an important business priority, lack of measurable results or empirical evidence leads to frustration. In *IDC FutureScape: Worldwide Future of Trust 2023 Predictions* (IDC #US49755022, October 2022), IDC predicts that by 2025, 45% of CEOs, fatigued by security spending without predictable ROI, will demand measurement of security metrics and results to assess and validate investments made in their organizations' security programs.

Simply put, organizations cannot afford to grow their security spend at the same rate of digital scaling for their overall business. The phrase "do more with less" is a common term that CIOs and CISOs are hearing from budgetary decision makers. Investments in cybersecurity cannot be made in a vacuum. With clear security metrics and data, CEOs will be in a much better position to be accountable for cybersecurity and articulate the value of security investments. Moreover, organizations can reduce the likelihood and impact of cybersecurity incidents by applying the right security controls to the right weaknesses and allocating the right resources to build more proactive and resilient enterprises.

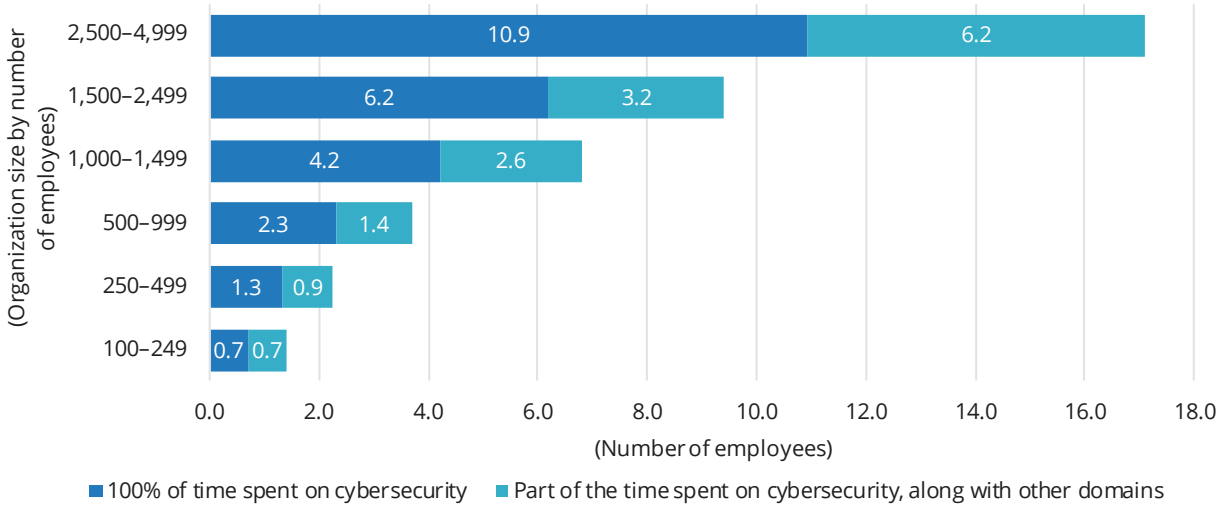
The Challenges in Building an Effective Internal Security Operation

As organizations continue the pace of digital transformation, cybersecurity concerns are at the forefront. Protecting corporate and customer data through cybersecurity practices and having cyber-resilience during and after cyberattacks provide strategic advantages to an organization's digital success.

However, organizations are finding that recruiting, training, and retaining security expertise can be one of the most challenging aspects of their cybersecurity programs. Security professionals are juggling multiple tasks – over a third of those working on cybersecurity spend only a part of their time on cybersecurity efforts (see Figure 2).

FIGURE 2

Lack of Dedicated Cybersecurity FTEs at SMBs



n = 501

Source: IDC's *North American MDR Survey,* 2023

In particular, smaller organizations with 100-249 employees *do not have at least one full-time equivalent (FTE) employee* dedicated solely to cybersecurity, while organizations with 250-499 employees are barely able to surpass having someone fully dedicated to cybersecurity (rounding to the nearest whole person). Unfortunately, this reality makes it difficult for them to focus on cybersecurity and can lead to security vulnerabilities and costly consequences.

The lack of employed cybersecurity practitioners in the SMB space is not unusual. There are two primary reasons for this shortage. The first reason is there is a lack of practitioners available. Handling security in a small team of one or two people is particularly burdensome. The technology moves fast and the ability to provide good coverage during a normal 40-hour work week is difficult. Add in the reality that cyberattacks can be perpetrated at any time, and the chance for burnout of the people running cyberoperations becomes high.

The second reason for the lack of employed cybertalent in the SMB space is highlighted in Figure 3. Close to 30% of SMBs cite the lack of budget for cybersecurity. The people part of the cybersecurity budget can take up a disproportionate amount of the budget, and the salaries that these cyberwarriors require are sizable.

Making changes to legacy security infrastructure was the top challenge noted in the North American MDR study. Doing the research, figuring out the fine print of contracts, and then setting up the new on-premises or cloud-based tools are not easy when you consider that these smaller cyberteams have their "day job" to consider. Change is hard, yet staying static and not keeping up with the changing infrastructure that digital-first companies utilize are not sustainable.

Figure 3 lists the multifaceted challenges faced by many organizations today, including technological, operational, financial, knowledge, awareness, and leadership. In IDC's *North American MDR Survey,* SMBs are defined as organizations with 100–499 employees.

FIGURE 3

Main Challenges in Managing Cybersecurity

Q. What are the main challenges for your organization in managing cybersecurity?

n = 501 for total, n = 150 for SMBs

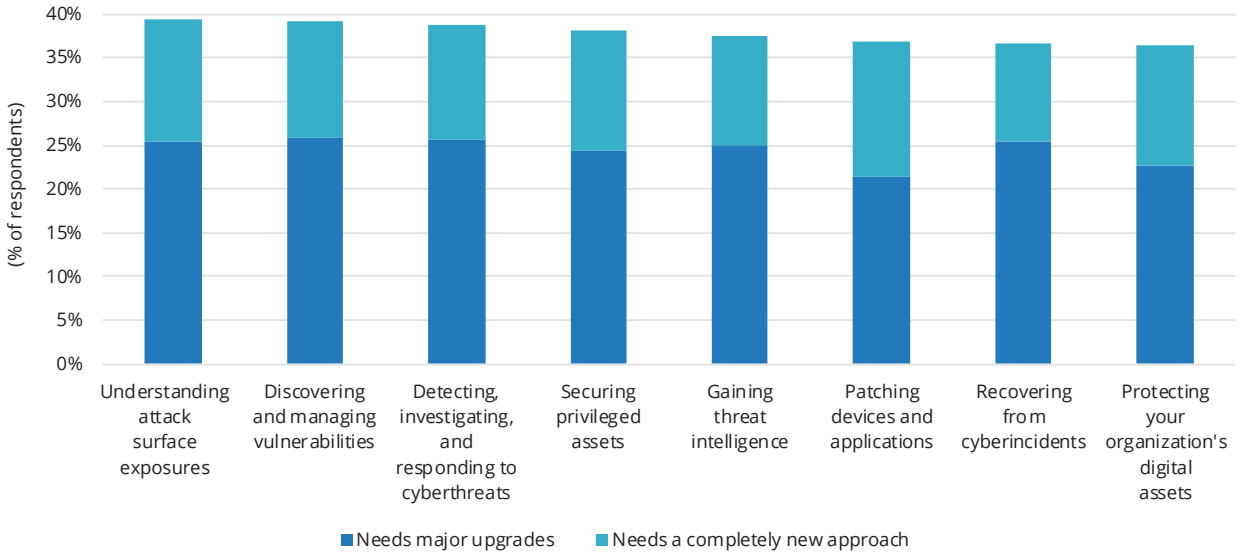
Source: IDC's *North American MDR Survey,* 2023

In addition to the top challenges, nearly 40% of IDC-surveyed organizations in the same study indicate the need for substantial improvement in their ability to detect, investigate, and respond to threats that have become more complex, sophisticated, and elusive. Similarly, about 40% of organizations also highlight "understanding attack surface exposures" and "discovering and managing vulnerabilities" as the areas that need major improvement or a completely new approach (see Figure 4).

FIGURE 4

Highlighted Areas for Cybersecurity Capabilities Improvement

Q. How would you assess the following cybersecurity capabilities in your organization?



n = 501

Source: IDC's *North American MDR Survey,* 2023

With organizations transforming or scaling into digital-first businesses, they do not necessarily have a good understanding of their complete exposure on the internet or the breadth of their digital presence. This tainted view is especially troubling with their growing reliance on digital channels and digital infrastructure.

Changes in the tech environment are inevitable as organizations invest more in SaaS, cloud, and other digital technologies. However, the challenges of leveraging security point products and making them relevant for the fast-changing environment become expensive and oftentimes cause more problems than they address.

It's clear that ongoing support and maintenance of cybersecurity solutions becomes inconsistent or is not done at all. Patches and vulnerabilities are continuous and occur in large volumes. Each potential attack surface requires visibility and continuous monitoring to detect attacks. It's no longer sufficient for an organization to take on the laborious and cumbersome tasks of monitoring, alerting, and incident management solely with its own cybersecurity staff.

IS THERE AN EFFECTIVE OUTCOME-BASED SECURITY SOLUTION?

It is almost untenable for many organizations, particularly small and midsize companies, to build a security operation program internally. If the organization could do it internally, why should it? Having and maintaining a security operation program is a big investment and commitment both operationally and financially.

IDC believes that the fast-evolving MDR service has the potential to address all the aforementioned pain points. The following customer benefits of leveraging an MDR solution are most valuable to SMBs:

- **Technology value:**
  - **Immediate access to security expertise:** The MDR provider acts like an extension of the organization's cybersecurity team, actively working 24 x 7 x 365 to try to prevent cyberincidents. This extended group comes with a larger and more seasoned team that can be utilized as needed.
  - **Manageability and higher efficacy of security operations:** The core competency of an MDR provider is detecting and responding to attacks.
  - **Optimization of the value of existing technology investments:** Many MDR providers do not require a rip-and-replace approach to the existing security stack.
- **Business value:**
  - **Better protection of corporate and client data and intellectual property:** Part of the ROI in cyberinvestment involves the safeguarding and protection of information – the digital currency of digital-first organizations.
  - **Assistance for overall resilience and business continuity:** Keeping the lights on is important. That means having cyber-resilience that allows firms to be able to withstand attacks that come their way and, on a very bad day, to be able to pull in the incident response capabilities of the MDR provider to restore the firm to a functional operating level.
  - **Insurability and cyberinsurance cost savings:** Getting cyberinsurance is difficult. Even when obtained, there is the question of whether it can be renewed without a significant increase in pricing. Having an MDR service is a way to demonstrate increased cybersecurity maturity and capabilities that help organizations get through underwriting.

Evolution of Managed Detection and Response

The managed security services (MSS) market has seen three distinct evolutionary points. The first offerings were designed to protect the perimeter of the organization by providing the management and support of security devices and software such as antivirus, firewalls, and log management. The second generation saw evolutions such as comanaged or outsourced security information and event management (SIEM) and the use of artificial intelligence (AI)/machine learning (ML) technologies to help speed up the detection of indicators of compromise (IoCs) as organizations were launching their digital transformation efforts.

In the third generation, MDR services offerings have come about to provide a unified service to protect organizations from the advanced velocity and quality of cyberattacks that are now the norm. Service providers can deploy MDR services utilizing a mixture of clients' existing capabilities and cybersecurity partners' supplied tools or services as well as private intellectual property. MDR services are typically

supplied by a provider's well-trained cybersecurity staff in a 24 x 7 x 365 remote security operations center (SOC).

How MDR Delivers Effective Security Outcomes

The rise of MDR services is reflective of customers' continued pursuit of an effective cybersecurity program. Some outcomes to expect are:

- **Transparency leads to more trust:** Many MDR providers, especially MDR pure-players or MDR solution providers, enter the market with strong emphasis on "transparency," breaking up the "black box" approach of traditional managed security SPs. When an MDR provider allows its customers to see exactly what MDR security analysts would see, including alert triage, event investigation, root cause analysis, and playbook development, it adds differentiation and trust for its customers.
- **Flexibility leads to value maximization:** Not all, but some MDR providers allow customers to leverage their existing security stack, including endpoint detection and response (EDR), SIEM, or any security operation control points/platform in which the customer has already invested. This approach significantly helps customers maximize the value of their existing security investment. Higher levels of flexibility test the MDR providers' engineering and integration capabilities.
- **Higher security efficacy leads to insurability:** Cyberinsurance policies are becoming increasingly rigid, costly, and demanding in terms of the things that the cyberinsurance providers require organizations to do. Having an MDR service serves as effective proof of the cybermaturity of the organization.

CONSIDERING SOPHOS MDR SOLUTIONS

Sophos, a United Kingdom-headquartered cybersecurity firm, has a wide breadth of security hardware, software, and services. It was acquired by private equity firm Thoma Bravo in March 2020 for $3.9 billion.

Sophos MDR is a fully managed service delivered by experts that specialize in detecting and responding to cyberattacks. It was first launched in October 2019 as Sophos Managed Threat Response (MTR), which fuses machine learning with expert analysis for improved threat hunting and detection, deeper investigation of alerts, and targeted actions to eliminate threats. These innovative capabilities are based on Sophos' acquisition of Rook Security (acquired in June 2019) and DarkBytes technology (acquired in January 2019).

Since its launch, MDR has been Sophos' fastest-growing new offering. Subsequent to its entry into the MDR market, Sophos acquired Refactr, a process automation and DevSecOps platform in August 2021, and SOC.OS, a spinout from BAE Systems' cybersecurity division, providing a cloud-based security alert investigation and triage automation solution in April 2022. These two acquisitions have further enhanced Sophos MDR, XDR, and the overall Sophos' Adaptive Cybersecurity Ecosystem. In October 2022, Sophos MTR became Sophos MDR, adding the ability to incorporate telemetry from across the security stack – including Firewall, NDR, Email, Cloud, and Identity solutions – to accelerate threat detection and response. The evolution of MTR into today's Sophos MDR illustrates how Sophos is adapting its solution to meeting the evolving needs of customers; this is integral to Sophos' growth strategy.

The market witnessed a fast-growing adoption of Sophos' MDR solutions. A few factors contributed to this growth:

- **Effective escalation process.** The format of case escalation within Sophos MDR is consistent and, moreover, involves the Sophos' team completing a thorough investigation prior to the escalation, so the client can focus on reviewing recommendations and implementing them where it can.
- **Business value.** Clients can work directly with Sophos' team to design and develop clear reporting when managing the environment. Such reporting and visibility enable effective communication to the C-suite.
- **Flexibility.** Customers have the flexibility to change the response actions at any time depending on the level of comfort. The client can choose the level of involvement when an active threat is happening, from low (e.g., notification) to high (i.e., fully authorize Sophos' team to resolve the active threat).

CHALLENGES/OPPORTUNITIES

In conversations with Sophos MDR clients, many of them have existing or past work relationships with the company. The familiarity of using the Sophos Central Platform is an advantage when these clients consider its MDR services. The Sophos Central Platform is a cloud-based, purpose-built security platform that has a whole team of Sophos Central engineers focused solely on the platform. It can be used to manage and monitor endpoints, servers, tablets, firewalls, switches, access points, email security, and cloud security.

However, the integration and correlation engine that goes beyond Sophos' own technology stack (i.e., Sophos' Adaptive Cybersecurity Ecosystem) is in its early days. This is important when Sophos is on the path to become a more service-oriented cybersecurity firm.

CONCLUSION

Cybersecurity is complex and difficult and moves fast. Most organizations simply cannot manage it effectively on their own. Cybersecurity teams need to partner with the right security partners to identify the right metrics to track the security value creation as security is rapidly becoming a strategic business risk to the enterprises.

After all, organizations need to have a cybersecurity program that enables a strong cybersecurity posture and cyber-resilience and helps meet cybersecurity and compliance objectives in a cost-effective manner.

MESSAGE FROM THE SPONSOR

Sophos defends more than 600,000 organizations worldwide against active adversaries, ransomware, and other breaches. Our broad portfolio of advanced, proven cybersecurity services and products enable organizations to lower cyber risk, increase efficiency, and lower the overall total cost of ownership (TCO) of cybersecurity.

Powered by over 500 experts, Sophos MDR is a 24/7 human-led threat prevention, detection, and response service that defends organizations against even the most advanced attacks. For organizations that wish to investigate threats in-house, Sophos XDR is a powerful, analyst-designed tool that enables operators to hunt for, investigate, and respond to suspicious activity and indicators of attack.

Sophos Intercept X Endpoint delivers protection against advanced attacks, employing an extensive suite of technologies to stop the broadest range of threats before they impact the systems. Sophos Firewall protects networks from the latest threats while accelerating important SaaS, SD-WAN, and cloud application traffic.

To learn more and start a free trial visit www.sophos.com.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2023 IDC. Reproduction without written permission is completely forbidden.