

MSPs PIVOTING TOWARDS MDR AMID RISING CYBER THREATS

The managed service provider (MSP) sector is swiftly expanding. As global cyberattacks show no signs of slowing down, an increasing number of businesses are turning to MSPs, entrusting them with the responsibility of strengthening their security.

As business prospects rise, so does the competition. To stay ahead, MSPs are recognising the importance of providing the crucial security services that businesses urgently need. Notably, they are continuing to pivot toward the managed detection and response (MDR) technology market this year.

MDR ADOPTION

This shift was highlighted at a 'Leaders in Discussion' roundtable in London in September last year, jointly hosted by cybersecurity firm Sophos and IT Europa – with a significant 80% of the MSP delegates present at the event leveraging MDR. Among these, 60% are breaking new ground by crafting their own solutions.

Recent studies also reinforce the momentum behind MDR adoption. According to Gartner, by 2025, half of all global organisations will be employing MDR services for continuous monitoring, threat detection, and responsive actions.

Kyle Torres, Senior Channel Account Executive at Sophos said: "Considering the data around MDR, there's potential for significant growth in the MSP market."

However, a pressing challenge for MSPs is data governance. "MDR providers seem reluctant to establish data centre in the UK," one of the attendees at the roundtable said. "It's challenging when discussing with UK partners who are saying they intend to transfer data to locations like Frankfurt or Central America. Given the UK's departure from the EU, there are changes to GDPR."

Another guest agreed, adding "It becomes a pressing concern when engaging with these vendors, emphasising the importance of a UK-based data centre to cater to the governance and data protection needs of UK clients. There's no option in the UK, and that needs to be addressed."

OBSTACLES TO GROWTH

During the recent luncheon, participants also shared their views on obstacles hindering business growth via a poll. Their feedback provided valuable insights into the challenges they face in the cybersecurity sector.

One participant highlighted the potential influence of mergers and acquisitions (M&A) on their business's trajectory. "Typically, there comes a time when mergers and acquisitions play a pivotal role in outcomes. I anticipate that growth and margins will remain, but M&A will shape them."

Another attendee highlighted digital marketing as one of its challenges. "Though we excel at what we do, we've missed out on some years and struggled to reach our clientele. I'm deeply committed to ensuring our success. Given a choice, I'd trade a top-notch cybersecurity expert for someone who truly knows how to elevate our presence on Google."

Competition was also a common refrain for some of the attendees. "We acknowledge that there are entities that can rapidly establish similar infrastructures to ours, especially when collaborating with partners to compete with us. We're losing out to cheaper providers who heavily utilise global offshoring, a strategy we don't typically employ. It's challenging for us."

Echoing these sentiments, another participant remarked, "For MSPs, it's obvious that pricing is crucial. Typically, these smaller firms are simply adjusting the profit margins set by others to meet the needs of customers."

REGULATIONS AND CYBERSECURITY SKILLS GAP

While enjoying dessert, a subsequent poll inquired about their predictions for the future direction of the industry. “I think stricter regulation is one of them,” one of the attendees said. “With initiatives like the government-backed Cyber Essentials, while not mandatory, it will become widely recognised as essential. When we consider the GDPR, the UK chose to adopt it as the UK GDPR, a regulation essential for businesses interacting with Europe.

“It remains to be seen how the UK government will approach regulations, and while it’s uncertain if the outcome will be positive or negative, it’s definitely something I’m keeping a close eye on.”

Another attendee noted: “The cyber threats landscape is intricate and constantly changing, making every business, whether big or small, vulnerable to risks. Tightening regulations and making more regulations for the protection of cybersecurity is crucial as insurance companies right now are backing away from anything remotely. Notably, insurance companies, like Lloyd’s, have become hesitant to cover cyber incidents.”

More businesses will continue to incorporate top cybersecurity talent into their teams, as noted by another guest. “We’re likely to witness more firms filling their cybersecurity positions,” he said. “With the recent surge in graduates, the highest we’ve ever seen, there will be an

influx of individuals with genuine skills entering the market. These people will actively choose a career in cybersecurity, as opposed to being pushed into it.”

Torres concurred, noting that the industry’s shortage of skilled cybersecurity professionals will diminish this year. “This upcoming Spring term, I’m scheduled to speak at the University of Bedfordshire to their senior cybersecurity students about the vital role of soft skills in the cybersecurity sector. I believe it is often more feasible to train someone with these interpersonal skills in the technical aspects than the other way around.

“I anticipate seeing more cybersecurity professionals who not only possess the requisite technical know-how but can also effectively communicate with clients, creating meaningful cyber dialogues.”

COMPLIMENTARY VS COMPETITIVE

Wrapping up the roundtable, Torres touched upon Sophos’ strategy: “We are a channel centric supplier, and our roadmap is heavily influenced by community feedback, particularly in MDR. One of the things we’re focused on at Sophos is this idea of complimentary versus competitive. So when we engage with a partner who offers their own MDR services, our goal isn’t to be viewed as competition but instead we try to find ways to augment the services they already offer to deliver a better overall experience for the customer.”

