MSPs CHAMPIONING 'SECURITY-FIRST MINDSET' FOR ADVANCED MOBILE CYBER PROTECTION

In the rapidly evolving digital landscape, the mobile security market is booming, on track to hit $36 billion by 2029, according to a recent study by Market Research Reports. This growth is fuelled by the shift towards cloud-based systems and an increasing focus on regulatory compliance like GDPR. The demand for advanced mobile integration is also increasing, as users expect access to critical systems through personal devices, often beyond IT department control.

The COVID-19 pandemic catalysed this trend, making mobile devices indispensable for remote work and driving significant investments in technologies like always-on VPNs and edge computing. However, the explosion of mobile applications, over 5.5 million to date, has opened the door to sophisticated malware challenges, often slipping past traditional security measures.

LACK OF SECURITY UNDERSTANDING

A recent roundtable in London, conducted under the confidentiality of Chatham House Rules and in collaboration with security specialist Lookout and IT Europa, underscored a significant challenge confronting Managed Service Providers (MSPs): a prevalent lack of awareness and understanding of mobile-related cybersecurity issues among their clients.

"We often encounter people [clients] who lack a clear understanding of what cybersecurity and its associated threats really entail," a delegate from a London-based MSP said. "They recognise the need for action but are unsure of the specifics. In our discussions with them, it's crucial to first assess their level of understanding and then tailor our approach accordingly.

The delegate emphasised that threat actors are more interested in exploiting data for monetary gains rather than targeting the devices themselves. "They leverage vulnerabilities not just in the hardware, but also in the software and operational processes. We steer the conversation away from a narrow focus on cybersecurity or specific devices and applications. Instead, we emphasise the importance of understanding assets, vulnerabilities, and threats as the foundational elements of effective cybersecurity."

Another participant from a London-based MSP pointed out a common psychological unpreparedness for

cyberattacks among organisations, often rooted in the belief that "it won't happen to us." The delegate remarked, "The issue at hand is more than just about money; it's a matter of reputation damage. Changing the mindset of people is a challenging task, and clearly, it's something we all grapple with."

Echoing this, a delegate from a Hertfordshire-based MSP highlighted that people often prioritize ease of use over security when using technology. "If you can't change this mindset, so that they adopt a security-first mindset for their own personal devices, they're not going to adopt it in business."

MOBILE MANAGED SECURITY

During the luncheon, attendees indicated through a show of hands whether they provide mobile managed security services. About half confirmed they do, while the rest haven't fully implemented such services yet.

One delegate explained their hesitation in offering comprehensive mobile security services. "When offering a service on mobile, it's important to provide complete management capabilities," he noted. "If we're unable to do so, we avoid promoting such services unless we can fully support them. Interestingly, many of our customers haven't expressed a need for mobile management services."

Another attendee shared that their business avoids offering mobile security management services to maintain minimal interaction with clients. "We prefer to remain 'low in touch' with the client," he said. "We really want the customer to be secure without us having to manage the device. Therefore, instead of seeking an MDM (Mobile Device Management) solution, we're in search of a mobile threat defence solution.

"We always say to customers who have mobiles that 'XYZ', for example, is available to them at no cost. We encourage them to utilise this, as it restores their scanning capabilities and includes a QR code scanner. Additionally, it offers a link scanner for enhanced security. Since this feature doesn't generate revenue for us, it alleviates us from certain responsibilities. That's why we are busy investigating what's the best route to market and determining the ideal product."

Another delegate mentioned that while their firm is in search of a product, they emphasise the importance

of offering it as an integral part of a service. “We’re seeking a fully multi-tenant solution to ensure client security and to generate revenue. Instead of selling a product, we offer a service, and it’s important for them to comprehend the nature of this service.

“We haven’t yet discovered a solution that functions what we desire. Therefore, we assist with computer and email security, along with auto scanning. We also provide breach washing and monitoring, and aid in backup and recovery processes, all within their office environment. The next step for us involves expanding our services to include mobile and browser security.”

EDUCATION AND CYBER HYGIENE

Towards the roundtable’s conclusion, delegates discussed strategies to mitigate mobile-related cyber risks, with a consensus on the importance of education and cyber hygiene.

A delegate emphasised the importance of understanding all facets of technology. “There are over 5.5 million applications in the market,” he says. “If we don’t grasp these technologies ourselves, how can we guide our spouses, children, and families, let alone our customers? We have a duty of care to implement the correct solutions and technologies to make sure that they don’t get exposed to things like phishing. If you’re not doing this, how can you expect to hold your employees accountable for it?”

Another attendee added: “All of us are cybersecurity people. I’ve never used a bill for security because it’s ingrained in the service we deliver. When you’re setting something up do you leave the backdoor open? Do you lock your front door when you leave the house? As IT people that’s our job to empower people with that understanding. it is it is incumbent on all of us to almost preach to those around us the hygiene.”

WHAT IS LOOKOUT’S CHANNEL POSITION?

Concluding the discussion, Matt Nichelson (pictured), who serves as the Regional Channel Sales Manager for Northern Europe at Lookout, detailed the company’s strategy: “Lookout is a 100% channel focused organisation delivering the industry’s most advanced Mobile EDR Solution.

“We launched our Mobile EDR Managed services programme last year empowering MSSP’s to protect their customers from mobile specific threats including phishing attacks, apps threats, device exploits, and risky networks. Lookout also enables the proactive enforcement of compliance policies based on the NIST Cybersecurity Framework to address GDPR, CCPA, and other regulations.

“Mobile is increasingly becoming the primary attack vector for cybercriminals because it provides a silent, highly distributed entry point into organisations. Whether it is a phishing attack, spyware, operating system vulnerability, or zero-day threat, Lookout empowers MSSPs to detect and respond to these threats, improve their customer’s mobile security posture, and ensure they meet their compliance requirements.

“We would love the opportunity to speak with any MSSP that this may be of interest to. Whether that be running a mobile threat landscape session where we will dig into our threat intelligence and offer our unique view on the landscape today or get the solution in the hands of the MSSP’s so they may evaluate its capabilities and review how seamlessly in can be integrated into the MDR / XDR services they are already delivering today.” |