eSENTIRE

Trust and proactive investment crucial for MSPs amid cybersecurity regulation hurdles

At an eSentire roundtable MSPs emphasised that trust, proactive investments, and education to help service providers navigate the complex security and regulatory landscape.

eSENTIRE

In today's rapidly evolving digital landscape, the regulatory environment for cloud transformation has become increasingly complex. New frameworks such as the Digital Operational Resilience Act (DORA) and the Network and Information Security Directive (NIS2) impose stringent demands on Managed Service Providers (MSPs). These regulations aim to ensure data security, privacy, and compliance with industry standards, creating a challenging terrain for MSPs.

BUILDING TRUST IN A COMPLEX REGULATORY ENVIRONMENT

At a recent roundtable hosted by IT Europa, in association with sponsor and security vendor eSentire, MSPs gathered to discuss the critical build-versus-buy decisions facing the industry amidst these regulatory changes.

A recurrent theme throughout the discussion was the importance of trust between MSPs and their clients. One attendee from an MSP based in Peterborough emphasised this by stating, "Trust is massive because if we mess up, our trust with customers goes out the door."

Building on the theme of trust, another participant added, "Trust is crucial because we ask our customers to trust us to effectively manage risk. When deciding to buy or build, such as a Security Operations Center (SOC), it's important to consider not only the initial costs but also the ongoing expenses and efforts required to stay up to date with the evolving threat landscape. The threat landscape constantly changes, and it requires continuous effort to keep pace with these changes."

This sentiment transitioned into discussions about the repercussions of inadequate investment in security tools. One attendee recounted, "We had a customer who got breached because they never invested in the security measures we recommended. When it happened, we refused to fix the issue until they paid for the necessary tools," highlighting the critical importance of proactive investment in cybersecurity measures.

IMPACT OF CLOUD MIGRATION ON CYBERSECURITY

During the luncheon, the discussion turned to cloud migration and its impact on clients' security postures. One delegate emphasised the critical importance of proper preparation for ensuring a positive outcome.

He said: "It depends on how ready you are for it and how much you planned it. We always do a sort of audit prior to cloud migration. It could be a shambles or surprisingly well-organised from a cybersecurity perspective."

Another delegate echoed this sentiment, adding, "Cloud migration can be an excuse for people to actually improve their cybersecurity. We're changing fundamentally broken processes for something better," emphasising that cloud migration, when executed correctly, can serve as a catalyst for enhancing overall cybersecurity measures.

However, there were also concerns about the suitability of cloud solutions for all businesses. One delegate remarked, "It's about whether cloud is right for your business. Not every cloud solution is suitable. For instance, managing large amounts of data might be more cost-effective on an in-house server."

Phil Skelton, Sales Director - Europe at eSentire weighed in, emphasising the role of cloud services in advancing cybersecurity: "We see cloud as an enabler, not an evil. Over the last 12 to 18 months, we've added Managed Detection and Response (MDR) for cloud to our portfolio. We've partnered with platform providers like Lacework and Tenable to address misconfigurations and user behaviour in cloud environments."

Transitioning to the challenges of cloud deployment, Skelton noted, "Environments are spun up quickly for development work, sometimes within hours. But this agility can lead to oversights and increased risks if not properly managed.

"We have a comprehensive portfolio of security services, which enables our partners to effectively support small to medium-sized organisations to help them proactively manage risk."

THE ROLE OF CYBER INSURANCE, REMEDIATION AND EDUCATION

Towards the end of the roundtable discussion, dessert was served alongside a rich conversation on the critical role of remediation services for MSPs. Delegates underscored the indispensable nature of these services in today's cybersecurity landscape, where breaches are not just probable but expected.

One delegate stressed the importance of being prepared for breaches, stating, "If you're ready for breach remediation, preparation is everything. If you're not prepared, you may never recover."

This sentiment was echoed across the table, highlighting the necessity for MSPs to offer robust remediation services to help clients bounce back swiftly from cyber incidents.

Cyber insurance also took centre stage in the conversation. Delegates pointed out that while cyber insurance is crucial, it often falls short of expectations. One delegate noted, "Insurance companies are often behind in terms of cybersecurity and self-insurance."

This gap in understanding has resulted in low cyber insurance rates, according to another attendee. "Cyber insurance rates are low due to a lack of understanding of potential risks," he argued, pointing out that both insurers and insured parties often underestimate the complexity and cost of cyber incidents.

However, the limitations of cyber insurance extend beyond just financial misunderstandings. A delegate highlighted, "Cyber insurance often lacks SEC regulation and adequate breach response," indicating that the policies may not provide the comprehensive support businesses expect during a crisis.

This can leave companies vulnerable even if they have insurance, another attendee added, highlighting "that is the fundamental problem with cyber insurance".

The conversation also veered into the challenges of educating partners and clients about cybersecurity. One delegate emphasised, "it is imperative for skilled partners to educate customers about cybersecurity."

WHAT IS ESENTIRE'S CHANNEL STRATEGY?

To conclude the roundtable, Skelton delved into the eSentire's strategy: "eSentire is actively looking to work with partners that want to offer best-in-class Managed Detection and Response services to their customers. The eSentire e3 partner ecosystem was created to simplify security sales and transform how we deliver value through and with our partners to the end user customer. The needs of business leaders are changing and how they're choosing to transact continues to evolve.

"At eSentire, we take personal ownership in protecting our customer organisations. We are looking for e3 ecosystem partners who share our commitment to going above and beyond to ensure their security. We are mission-driven and live by the customer-centric statement: **An Attack on You Is An Attack On Us.**

"It's our mission to help business leaders make sense of the complex vendor landscape, simplify the security buying cycle and demonstrate strong time to value from onboarding to cyber risk reduction, as we partner to put businesses ahead of disruption."

Phil Skelton, Sales Director, eSentire

eSENTIRE

https://www.esentire.com/partners

https://www.linkedin.com/company/esentire-inc-/

Phil.skelton@esentire.com