IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In Conversation

In Conversation with Sean Muirhead

Carol Baker

As Logpoint announces the appointment of seasoned cybersecurity professional Sean Muirhead as its new Chief Product Officer, we ask Sean what attracted him to the role at Logpoint, and why in an era where cyber threats loom the boardroom is fast becoming a battle ground that sees both the cybersecurity industry and CISOs struggle to get messaging across to boardroom room executives.

*Cybersecurity veteran **Sean Muirhead** brings 20+ years across corporate and vendor roles to the table.*

He holds numerous industry certs and an MBA from Cranfield (2021). This diverse experience has equipped him with a deep understanding of cybersecurity challenges and solutions, from both customer and vendor perspectives.

Sean leverages this expertise to develop solutions that directly address real-world customer pain points, ensuring they are secure and effective, currently as Chief Product Officer at Logpoint.

Tell our readers a little bit about yourself and what attracted you to Logpoint

As Logpoint's Chief Product Officer, I have overall responsibility to ensure that all Logpoint's products help our customers and partners overcome the cybersecurity challenges they face now and into the future. I have been in cybersecurity for 25 years, and through my various experiences from being an information security officer, later in technical pre-sales, product management, and most recently in mergers and acquisitions, I have noticed a significant trend: the merging of risk and threat.

A lot of analysts will refer to this as being consolidation of technology, but consolidation is often driven by customers, their budgets and more importantly, what we are seeing is the need to improve efficiency and effectiveness in the effort, or in the hope, of improving their companies security posture. This is being driven by a big shift in cyber insurance and the changing dynamics driven by the underwriters and their appetite to risk.

After working with Logpoint on a consultancy basis for a few months, I learned a lot about what the company had in terms of its people and technology and realized the


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

skill that Logpoint has in looking at the cybersecurity problem from a different angle. As I see it, there's a real opportunity here where joint risks and threats are evaluated to create an 'analyst workbench' that could be a real differentiator in the cybersecurity market. Logpoint has a lot of excellent resources in terms of its intellectual property and skilled teams with the potential to solve real future problems for our customers, and that is what sets Logpoint apart and makes it a cybersecurity powerhouse in Europe.

Trying to get the correct cybersecurity message over to boardroom executives can be challenging for CISOs. Why do you think this is?

The conditions in cybersecurity are changing with expanding data and cybersecurity regulations and the ever-changing methods of threat actors. The main problem CISOs have is speaking the board's language. The board speaks the language of risk to the business, whereas CISOs see it more from a technological perspective. As CISOs language matures they need to focus on how business risk needs to be tied back to technology, if the risk is to be controlled.

Cybersecurity challenges have been around for decades, and they are not going away anytime soon. Customer acquisition costs in cybersecurity are high. As an industry there are over 3,500 vendors. No CISO can be expected to evaluate them all and from a vendor perspective, the cost to acquire a customer and gain market share is steep. Many public companies remain unportable for years post IPO with most money spent on customer acquisition instead of R&D. As a result, we can expect to see some consolidation in the vendor space.

The industry is driven by the customer's desire to improve their risk posture, both at a board and CISO level, but also from an insurance underwriters' point of view – this is particularly key given the increasing demands of cyber insurance providers. The insurance industry is now looking for more clarity, examining how businesses compare to their peers, and their ability to keep pace with compliance mandates.

Emerging threats will always continue to challenge the sector, and businesses will need to take much more of a pragmatic risk-based approach. If an organization can tighten its boundaries – whether these be cloud or hybrid infrastructures -– they can implement controls and protect itself from so-called "spray and pray" attacks whereby attackers gain complete control over the system or move laterally from there to launch additional compromises.

From an emerging threat perspective, attackers and defenders have been using machine learning, deep learning and artificial intelligence (AI) to create attacks and form defensive mechanisms. Attackers have become more sophisticated in creating attacks. Social engineering and the introduction of ChatGPT has made it more difficult to spot potential spam or phishing emails because of poor language or grammar. This means that attackers have been able to step up their game.

There is very little you can do to 100% defend yourself against a true targeted attack. After all, humans are ultimately the weakest link in the chain when it comes to security. You can put as much technology as possible in there, but there will


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

always be a human element to breaches. So CISOs are faced with the challenge of not only controlling their technology assets, but also educating their people as the last link in defense.

Apart from the consolidation issue, what other challenges are vendors likely to face?

The vendor landscape is driven by customers. As an industry, vendors are only here to solve customer challenges. Besides cyber threats, customer challenges include talent shortages, alert fatigue, and false positive alerts, and so the vendors who address those challenges will be the ones who will ultimately win and succeed. This is where Logpoint is a key player in bridging the reactive world of log management and the proactive approach of risk management. We can help customers or partners streamline their operations, potentially lower their TCO, and improve visibility. For a vendor, if you can supply the customer with a 'single pane of glass' you provide a single source of truth. And if you can be the single source of truth, you can be an authoritative report to the board and to insurance underwriters.

Do you feel that AI is accelerating the take up of cybersecurity solutions?

AI is certainly increasing the take up of attack methods, and this is leading the cybersecurity industry to investigate how AI can be adopted to streamline operations and win the AI attack battle. Many software vendors have already implemented chatbots from a support perspective to help streamline or expedite support tickets, and resolution. More importantly, vendors are also using AI to internally investigate those large language models (LLMs) in the data that we collect from our customers daily and log data to create inferences and potential detections which it would not have been possible to write a rule-based detection for, simply because it's a statistical anomaly.

The UK Government has been urging businesses to take out cyber insurance. How do you see cyber insurance developing?

Like every sector, the insurance industry wants to be profitable. In the recent past, many insurance companies found that cyber insurance was a loss leader. Now, driven by the influx of ransomware, underwriters are adding exclusions or additional security requirements to their policies and increasing prices.

For those unable to meet the security requirements, obtaining cyber insurance for their business will be more challenging. As a result, we will see more CISOs struggle to find ways of proving their organization's level of maturity and controls to the underwriters in a way that allows them to obtain cover or reduce their premiums. Underwriters have a deep understanding of a company's external posture, so when they are contacted for an underwriting quote, they can run it through their models based on their quantifiable risk. For all organizations, cyber insurance is going to be a popular topic for quite a few years to come.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Are there any other closing thoughts you would like to get over to our readers?

Logpoint is the only converged SIEM vendor in Europe, and the creator of a reliable, innovative cybersecurity operations platform that offers SIEM, UEBA, SOAR and SAP security technologies converged into a complete platform to empower organizations worldwide to thrive in a world of evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, Logpoint is in a unique position and on track to become a cybersecurity European powerhouse.