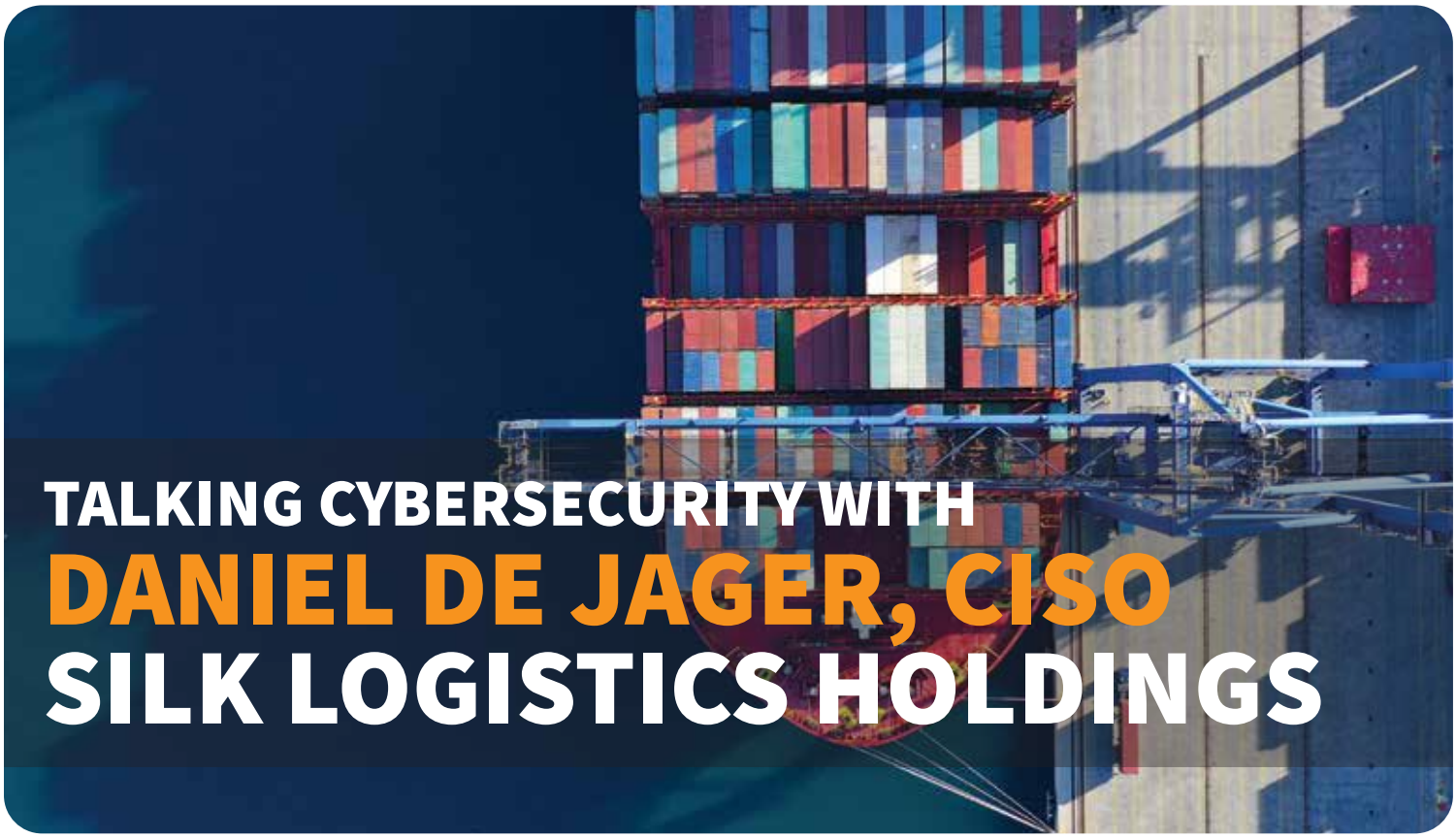

TALKING CYBERSECURITY WITH DANIEL DE JAGER, CISO SILK LOGISTICS HOLDINGS

Today we're talking with Daniel de Jager, CISO for Silk Logistics Holdings (ASX:SLH), an ASX listed entity with a workforce of 1,878 people and FY24 turnover of $554 million. SLH is proudly 100% Australian-owned, providing integrated, port-to-door, landside logistics services to some of the world's biggest names. The group provides Port Logistics and Contract Logistics services, including warehousing and distribution services.

Welcome Daniel, how has your day been so far?

Thanks for having me. Our days are filled with a variety of technical activities, reflecting our fast growth as an organisation.

For example, one of the key projects we're currently focused on is enabling seamless access for all staff to our SaaS application for health and safety via Single-Sign-On. I'm deeply involved in the architecture and engineering aspects, collaborating closely with our vendor, business leaders and technical teams to ensure a smooth transition and successful implementation.

This project represents a major strategic milestone for us, showing how we are collectively maturing and enhancing not only our security controls but our business as a whole.

And you have a disparate workforce to protect comprised of approximately two thousand people?

Our workforce may not be as large as some global organisations I've worked for before, but it comes with its own unique challenges and opportunities. I joined Silk in July 2023 after working with a major international Systems Integrator that operated across 60 countries with around 65, 000 staff. In those environments, there are different resources and dynamics at play.

What I've found at Silk, and more broadly in Australian organisations, is that the culture is distinct-it's all about people. Getting hands-on and working alongside the team to demonstrate value has been key. When we show tangible improvements and a better way of doing things, it fosters openness to change and growth. This approach has been a significant part of our journey and success over the past year at Silk.

Where do you start when you come into the role as CISO for a major supply chain and logistics company like SLH?

One of the first things we focused on was assessing our security architecture across the group, to understand what we had and where it was. It became clear that we needed to rationalize our approach because we were working with disparate technologies across the group, which makes management quite challenging. So, we took on the task of standardising our systems.

While the primary focus was on creating a more streamlined and manageable environment, this approach also led to significant cost savings as a natural consequence of rationalisation and consolidation. By aligning our group's efforts, we are simplifying processes and achieve more cohesive operations-it's been a win-win for all stakeholders.

Many new CISO's might start with gap assessments against, ISO27001 or NIST, but while those frameworks are valuable, we chose to get everyone on the same page with our technology. Once that foundation is set, everything else tends to follow naturally.

"When we show tangible improvements and a better way of doing things, it fosters openness to change and growth."

And that process included your email security with MailGuard?

Absolutely. In cybersecurity, simplifying processes is key, especially when you don't have a massive team in-house. The support we received from partners like MailGuard has been invaluable to date. The support team is highly responsive and knowledgeable, which has made a big difference for us. They have a deep understanding of what they are doing, and their experience shows.

During the transition to MailGuard, their support was exceptional. For instance, when we carried out the cutover, we experienced minimal false positives-far fewer than what we anticipated. This kind of smooth transition is a testament to the team's expertise and commitment.

"The support we received from partners like MailGuard has been invaluable to date.

The support team is highly responsive and knowledgeable, which has made a big difference for us.

They have a deep understanding of what they are doing, and their experience shows. "

What stands out is that they go beyond just meeting the SLA requirements, they are proactive in ensuring everything runs smoothly. This level of dedication is exactly what we need in a partner, given the critical nature of email security in our operations.

Had you worked with MailGuard before?

No, I hadn't worked with MailGuard prior to joining Silk. However, the decision to move to MailGuard was driven by a thorough and rational assessment. We replaced a well-known global mail filtering solution with MailGuard based on a detailed evaluation of its capabilities, support structure, and alignment with our specific needs. It was important for us to choose a solution that provided simplicity, effectiveness, and confidence, and MailGuard met those criteria well.

What was your process for evaluating SLH's needs?

Our evaluation process began with a comprehensive architecture assessment to understand the current landscape of our technology across different companies within the group. From there, we conducted a technology fit assessment, identifying common denominators that could serve as standardised solutions. For example, Secon Freight and Logistics, a part of the SLH group, was already using MailGuard, which provided an opportunity for us to evaluate its effectiveness firsthand. This hands-on approach, combined with a financial analysis and a key decision document, allowed us to make a well-informed choice that aligned with our strategic goals.

You mentioned that you have experience that you can speak to. How does MailGuard compare to your experience with other providers?

I've worked with various vendors, and, through that experience, I've learned the importance of transparency and straightforward communication. In the past, there were instances where we faced challenges with service providers due to a lack of clear responses and consistency, particularly when handling incidents. For me, it's crucial to work with partners who value open dialogue and trust, as those elements are key to building strong, lasting relationships.

What stood out for me about MailGuard was their confidence in their solution and their willingness to put their reputation on the line. As I told our CIO, MailGuard's approach demonstrated a high level of assurance and commitment to quality, which aligns well with our values. It's a refreshing difference compared to some of the more complex and opaque experiences I've had previously.

When you reflect on your first twelve months in the job, what have been some of the highlights?

I think the journey so far has been about simplification and developing a technology strategy that aligns with our overall security strategy. The progress we have made has been a natural consequence of these efforts to uplift how Information Technology operates.

I'm seeing Silk Logistics becoming one of those unique logistics and supply chain organisations that set the standard for operational effectiveness and security. It is not about being cutting-edge, but rather about implementing the right level of security to protect and serve our customers.

The strategy we've set is comprehensive and innovative in certain aspects, with a strong enterprise architecture that we are moving towards.

What I bring to the table is pragmatism from my background with a global Systems Integrator, where I was involved with addressing complex security challenges. Applying those experiences at Silk has enabled us to embark on a transformative journey that is clearly making an impact. I see our internal IT teams upskilling and adapting to new ways of working, which is really encouraging.

"I'm seeing Silk Logistics becoming one of those unique logistics and supply chain organisations that set the standard for operational effectiveness and security.

It is not about being cutting-edge, but rather about implementing the right level of security to protect and serve our customers."

Overall, the role here is about transformation-about being hands on and demonstrating what is possible. It is not just about talking; it is about showing the way forward, collaborating with teams, and making meaningful progress together.

There have been some high-profile incidents impacting companies in your sector in recent years and targeting supply chains. So, what does that mean for SLH? What are you particularly concerned about?

For a company like Silk, the smooth flow of electronic data is essential to our supply chain operations. Any disruption to this data flow could halt our logistics processes, affecting everything from trucks moving

goods being unpacked at shopping centres. Ensuring these systems are operational is a priority for us, and it is something that keeps us vigilant daily.

From a threat perspective, we've observed that the most common attack vector over the year has been email-based threats. Attackers often use this tactic to gain initial access by harvesting credentials and establishing persistence within the environment. Fortunately, our layered security approach, combining solutions like MailGuard and Defender 365, has proven effective in mitigating these threats, and we haven't seen any significant incidents of credential compromise.

"The smooth flow of electronic data is essential to our supply chain operations. Any disruption to this data flow could halt our logistics processes, affecting everything from trucks moving goods being unpacked at shopping centres. Ensuring these systems are operational is a priority for us, and it is something that keeps us vigilant daily.

From a threat perspective, we've observed that the most common attack vector over the year has been email-based threats. Attackers often use this tactic to gain initial access by harvesting credentials and establishing persistence within the environment."

We continue to build on this foundation with additional security controls, particularly around Spear phishing and Adversary-in-the-Middle (AiTM) attacks. We leverage best in class DNS security and network defences to ensure comprehensive coverage. My focus remains on maintaining uptime and securing the systems that underpin our port logistics, warehousing and distribution services.

We are also moving away from on-premises high-value assets towards more SaaS-based solutions, as this shift allows us to focus more on access management and securing our entity under a zero-trust architecture. The future for us is clearly in SaaS, and our efforts are aligned to secure these environments.

Can you share some more about your journey getting on board with MailGuard?

Before joining Silk, I wasn't familiar with MailGuard per se, as I had been closely working with another major provider in this category. In that role, I applied a rigorous, data-driven approach to understanding the risks posed by email-borne threats, using mathematical analysis to gauge susceptibility areas.

So, the key question we ask is: how susceptible are we to email threats? Essentially, how many of our team members might click on a phishing link. To answer that, I've introduced risk metrics at Silk that we used globally in my previous role, which proved effective in highlighting potential vulnerabilities.

When I learned that Secon Freight Logistics, a part of Silk Logistics Holdings group, was already using MailGuard, I decided to explore it further. After an initial discussion with the MailGuard team, I took the time to review the solution, keeping in mind our objective of consolidating all technology under the same stack. It was clear that MailGuard could simplify our processes and align with our strategic directions.

Upon gaining access, I reviewed the policies and saw firsthand how straightforward the tool was. The simplicity and effectiveness of the platform convinced me that it could be the right fit. After a comprehensive technical fit assessment and internal discussions, the decision to adopt MailGuard became a logical and strategic choice for us.

So, what's the greatest value that MailGuard gives you?

I have certainty and a confidence level of assurance. That's the value that you guys bring - I'm not going to be compromised.

So, the value is a very high level of confidence and assurance that I've got the best level of protection for this type of company and I'm managing risk as a result.

So that's the value. We went through a thorough process with various options as part of our key decision process. We have done what many other outfits would have done to make a technology decision. So, based on our needs assessment, my decision in selecting MailGuard was as simple as that.

What are three key pieces of advice you would give to business leaders that are wanting to keep their business cyber safe?

First, understand where your critical value lies – know where the money comes from in your organisation. This means identifying and securing your most important assets. For us, this includes our warehouse management systems, distribution systems, transportation management systems and electronic data interchange systems. Understanding your value chain helps you prioritise efforts where it matters most.

Second, be aware of your external attack surface. Know what systems are exposed to the internet and ensure that they are regularly patched and well-defended. This approach must be proactive so that weaknesses are not exploited by attackers.

Third, manage identities rigorously. The landscape shifted with more companies, including ours, adopting hybrid environments. It's essential to manage identities properly, ensuring secure access and minimizing the risk of unauthorised entry.

These three areas of Asset Protection, Attack Surface Management, and Identity Management, are fundamental. I advise getting to grips with these areas before anything else. It is not just about talking to your CEO or board for a bigger budget; it is also about demonstrating through your actions that you are protecting the business, the board and the bottom line. The results and their alignment with business objectives will naturally lead to support and trust.

How do you think cybersecurity and cyber risk will evolve in future?

I believe the fundamentals of cybersecurity won't change-crime will still be crime. Threat actors will always seek opportunities to exploit vulnerabilities. What will evolve, however, is the level of sophistication and the methods they use. We're already seeing more automation, machine learning and artificial intelligence being deployed on both sides, which will likely continue to escalate.

As defenders, we must adapt to this reality by constantly thinking ahead. That means understanding the triangle of crime: where there is a motive, means and opportunity, crime will happen-whether online or offline. Our goal should be to limit those opportunities through proactive and innovative defence strategies.

Cybercriminals are evolving their approach and organisation, and we need to do the same. Sometimes they mimic legitimate businesses, completely with a high level of sophistication and organisation. We've even seen instances where threat actors operate with the same efficiency as a well-run corporation. This means that we-as defenders, need to be equality creative and proactive.

To effectively counter these threats, we need a mix of technical

defences and strategic planning. For example, there have been times when we've had to understand our adversaries deeply, even to the point of accessing their infrastructure to gather intelligence. While always ethical and within legal boundaries, this level of insight helps us understand their tactics and prepare accordingly.

Ultimately the future of cybersecurity will be about staying agile, informed, and ready to pivot as threats evolve. It's not just about the technology; it's about strategy, teamwork, and resilience. In this high-stakes environment, every decision counts, and preparation is key.

That experience must sharpen up your readiness coming into a role like this one with SLH?

When approaching cybersecurity at Silk, I ask myself, "If I were to assess this organisation from an attackers' perspective, where would the weak spots be? What methods would be most effective?" This mindset helps me think like a potential adversary, which is crucial for identifying vulnerabilities and fortifying them. It's a strategic exercise that drives us to strengthen our defences accordingly.

There is no room for complacency. We have seen other companies in our sector experience significant impacts, often because of phishing attacks or not patching internet facing assets. It is a harsh reality of the cybersecurity landscape, and we need to stay ahead by being vigilant and proactive.

Tools like MailGuard give us visibility into the types of threat we're facing. These insights are vital as they help us understand the tactics used by attackers and to adjust our defences accordingly.

Our goal is always to execute our plan fully and thoroughly. It's a journey, but we're focused on tackling the critical challenges head-on and making substantial progress swiftly and efficiently.

Daniel, thanks for being so generous with your time and for sharing your vast experience and insights. The team at Silk are in great hands.

Thanks, mate, have a great day. Goodbye.

"Threat actors will always seek opportunities to exploit vulnerabilities. What will evolve, however, is the level of sophistication and the methods they use. We're already seeing more automation, machine learning and artificial intelligence being deployed on both sides, which will likely continue to escalate.

As defenders, we must adapt to this reality by constantly thinking ahead."

Reach out to our team of experts to learn more about bolstering your business's **email security**

1300 304 430

expert@mailguard.com.au

mailguard