PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

LUKE MCCONOUGHEY

CISO, Workfusion

HEADQUARTERS: New York, NY

EMPLOYEES: 350+

ANNUAL REVENUE: Undisclosed

"We have been successful leaving the technical jargon behind and discussing cyber threats as corporate outcomes. With a sound business plan, budget, and staffing, our priorities are attainable."

- LUKE MCCONOUGHEY

Luke McConoughey has worked in every aspect of information security, ranging from satellite cryptography to cybersecurity operations to audit to policy and governance. He says, "I love every aspect of it, it's very interesting to me; there are opportunities everywhere."

Currently the CISO of Workfusion, an Artificial Intelligence powered robotic processes automation platform that automates operations and upgrades customer experiences, McConoughey's role allows him to work at the nexus of cybersecurity, DevOps, automation, and artificial intelligence. This unique position enables him to take on new priorities and challenges. He explains, "We're doing robotic process automation powered by an AI engine. It seems that most AI solutions today are marketing gimmicks, especially in the cybersecurity and IT space. Most of the promising and interesting AI is still on the front office, business development, revenue generation side. But being able to be an early adopter of applying AI to cybersecurity is incredibly exciting."

As the organization's first CISO, McConoughey finds himself equipped with adequate budget, strong support, and innovative opportunities. Before joining the Workfusion team, he carefully evaluated the CISO position, how the management team approaches leadership, the top organizational goals, and how he would fit into the overall corporate mission. While many organizations face challenges around budget, time, and people, McConoughey responds, "We have been successful leaving the technical jargon behind and discussing cyber threats as corporate outcomes. With a sound business plan, budget, and staffing, our priorities are attainable."

Transitioning into a C-level role required McConoughey to take on larger organizational challenges. He comments, "Moving into the C-level, for me, meant focusing on the practical

applications of transforming cyber risk into business sense through quantitative risk assessments, automated risk assessments of activities, then setting acceptable risks thresholds and tolerances and where that deviates, and getting additional insights or awareness of what's happening in the environment."

One of McConoughey's current top challenges is getting visibility and understanding of the business operations. He describes this as implementing measurements and starting to quantify aspects of the business itself. This enables him to focus on reducing the threat surface but also gaining valuable insights into activities that are going on and making sure the right controls are in place.

FOCUSING ON METRICS

McConoughey understands the importance of preparing for board presentations by being mindful of key topics board members are interested in discussing. His security program produces operational metrics, he says these are not insightful for board members, and can distract from what truly matters. To have an impactful engagement with board members and executives, McConoughey communicates in dollars, goes into detail discussing probable outcomes, and concisely shares how they've mitigated risk. By doing so, he sets himself and his team up for success and encourages business alignment.

When McConoughey initially started putting together board presentations, he tried to leverage outside sources for inspiration and guidance yet found a lack of readily available information. He says, "I looked to a number of my peers, I searched for 'CISO board presentations' and nobody is willing to share. I was not seeing samples of what works in terms of what is important and what isn't. No one is sharing that learning, that experience, or that scar tissue. That's kind of sad for me. I was able to leverage our internal board presentations for something that had the same ergonomics. I ended up sticking with my intuition and experience."

McConoughey shares different metrics with the board than those he shares internally among his team in terms of varying detail, approach, and granularity. He explains, "The team metrics are much more detailed, things get abstracted into thematic risks focusing on the actual impacts and communicating what's happened versus what was a near miss. It's a lot easier to talk about it in that respect. Here's what happened, here's how much it cost, here's what a mitigation solution would be and why we're going to accept that risk or we're going to fully mitigate that risk. At the executive level it's pretty much dollars. We'll frame the conversation around the type of challenge, how this happens, and what we've done to fix or address it. I also share what we're considering or what we're planning and the residual costs. And if someone disagrees, we talk about what it would take to get further and evaluate the costs."

LEADING A STRONG TEAM

"My current team is five and we're growing and expanding. I worked in China for several months and one of the most important things for me was this concept of "Guanxi", where in China, you have to build a personal relationship before you can get down to business. That was something that helped me be very successful in China and also here building personal relationships and trust, and helping demonstrate that we are successful together and not be a department of "no" or someone that's going to hinder their ability to reach success. Guanxi is my secret," says McConoughey.

When hiring new talent, McConoughey explains, "I look for a balance of soft and technical skills. I don't want someone that's overly technical that is unable to communicate effectively and rationally, I can't have an incredibly smart person talking a foreign language to the leadership. At the same time, during my interview process, I've had HR complaints about how difficult they are, but it's incredibly simple. I want to plumb the depths of your knowledge and get you to say, 'I don't know'. If you make something up, we're not moving forward with you, but if you say, 'I don't know' a hundred times, that's still a big plus in my book as we can teach you, we can help build those skillsets. Overall, I want someone that says they don't know something, who we can train."

McConoughey provides his team the opportunity to attend training courses and conferences, or attain a certification, however he believes certifications don't typically solve many of the problems the industry faces today. He comments, "If there was a certification or a training class, and if only you did this, you would be secure, we wouldn't have the headlines we have today. What I value most is the ability to think through a problem and look at it from many different angles and figure out the best methods to solve it."

"In the next few years, AI will have an incredible impact on how we staff, how our tools interoperate, and how we fight badness. I see us sharing entire cybersecurity AI operational models from company to company and across industries, while maintaining confidentiality via differential privacy. This isn't science fiction; this is the science today."

- Luke McConoughey