PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

GARRETT SMILEY

CISO, Serco

HEADQUARTERS: Herndon, VA (Serco, Inc.) / Hook, England (Serco Group – Parent Organization)

EMPLOYEES: 50,000+ globally

ANNUAL REVENUE: £2.84 Billion GBP ($3.44 Billion USD) globally

Garrett Smiley is currently the CISO at Serco, a Financial Times Stock Exchange (FTSE) top 250 federal contractor company that provides business process outsourcing, citizen services, defense, healthcare, justice, immigration, and transportation services internationally in both the public and private sector.

Smiley approaches his work as a CISO by focusing on being a risk management advisor. He explains, "I think that a lot of people have historically misunderstood that security is not meant to be a control. The controls must be put in place by the organization and by IT proper. We simply help them to manage the risk by identifying it, helping them prioritize the remediation of it, and then confirming the remediation of that, functioning as an advisor. When we're acknowledged that that's why we're around, things tend to be a lot more mature in the organization and they tend to be a lot more secure, quite frankly, because the role of the entity is understood better."

BUILDING RAPPORT FOR STRONG COMMUNICATION

Smiley believes developing and maintaining rapport with both his team and other executives helps him accomplish goals in a meaningful way. He works hard to ensure he is constantly engaging with his team in a positive fashion that creates strong communication and solidifies team work. He explains, "Rapport really can't be built with individuals if you don't know something about them. And it can't just be because of the project that you want them to work on. Rapport is what sums it up. If I've gone to the trouble of building a relationship with you, then when challenges come, you're probably going to be a little more willing to work with me. This way we can achieve common goals instead of me only showing up when there's something that needs to be done."

Smiley says everyone on his team goes above and beyond and he ensures that he provides them with opportunities for upward mobility. Recognizing quality and effort among his team has resulted in promoting people in non-management roles into management roles, among many other ways his team continues to evolve.

MEANINGFUL BOARD INTERACTIONS

Smiley attends quarterly board meetings to regularly discuss cyber posture. He says, "During these meetings, cyber posture is being discussed in front of the senior executive management team, including the CEO as well as three other board members. They are hearing about it regularly. And my reports to them are pretty advanced. It covers things that we've accomplished, areas for improvement, KRIs, vulnerabilities status and dashboards, phishing campaign results, and whatever else is pertinent for that quarter. But they've definitely been seeing a lot more in the way of really detailed ground truth. Obviously, we frame it in such a way

"RAPPORT REALLY CAN'T BE BUILT WITH INDIVIDUALS IF YOU DON'T KNOW SOMETHING ABOUT THEM...IF I'VE GONE TO THE TROUBLE OF BUILDING A RELATIONSHIP WITH YOU, THEN WHEN CHALLENGES COME, YOU'RE PROBABLY GOING TO BE A LITTLE MORE WILLING TO WORK WITH ME. THIS WAY WE CAN ACHIEVE COMMON GOALS INSTEAD OF ME ONLY SHOWING UP WHEN THERE'S SOMETHING THAT NEEDS TO BE DONE."

that we can have a discussion about it."

To present in a meaningful way that translates technical into business language, Smiley follows certain rules of thumb. These include using visuals and explaining the security program in plain language. He says the more text dense presentations become, the more likely you are to lose your audience. To provide concise, business-aligned language he may not describe a tool to the board as a vendor would use to describe it, but instead put a business-impact spin on it (e.g., "insider threat" vs. behavior analytics).

To prepare for questions from board members, Smiley encourages CISOs to be armed with the ability to respond on the fly, and to deliver answers in a frank, straight-forward manner. He comments, "The people who are on our board are on other boards as well, as is common. And I could tell that they were not used to seeing this level of sophistication and level of truthfulness, to be blunt, in board presentations. I'm thrilled that I was the one that helped them to better understand these blunt truths and they've adjusted appropriately."

THE CHALLENGES OF BENCHMARKING

Smiley was recently asked how Serco stacked up against other federal contractors in regard to what they are spending on security and how others are staffing their security teams. Due to the sensitive nature of their industry, there is limited knowledge sharing taking place, and Smiley says no one is racing to divulge details about their programs.

He explains, "There are so many variables when it comes to benchmarking. Other organizations' budgets for security might exceed all the money my company makes in one year. It's not really comparable to talk dollars. And then when you get into percentages, does that make sense when you're taking a look at two entirely different industries? Federal contracting is kind of similar to the margins they deal with in retail, but it wouldn't be appropriately comparable to finance. I am not aware of there being any sort of public repository of information that would truly answer that question. I know it's something that everybody asks, but I'm unaware of where it would exist."

For internal benchmarking, Smiley focuses on Key Risk Indicators (KRIs) for all the regions Serco covers across the globe. He then compares where they are seeing risks across the number of different KRIs in that report. This provides a benchmark for risk, and he eventually plans to work with an external, federally supported group to measure risk.

MEASURING AND MONITORING TECHNOLOGY INVESTMENTS

Smiley continuously measures and monitors technology investments within the organization. This effort includes tracking contract renewal dates, evaluating cost, and determining functionality within the environment. He comments, "We take a look at old technologies that cost a fortune and see if we can do it for the same cost or cheaper with something new. Cost is always a driver and things going end of life is always a driver. Maybe this costs the same as that, but this provides me a lot more capabilities, so on and so forth. On average, throughout the calendar year, we are probably having serious discussions about replacing at least 10 to 15 technologies a year. And we're talking enterprise-wide stuff."

CONTINUING TO GROW AND LEARN

Heavily engaged in professional development, Smiley attends countless CISO events, conferences, and symposiums, and is a part-time adjunct who chairs multiple dissertation committees. He says, "I force myself to be aware of what's going on out in the academic world as far as research is concerned whether it's robotic process automation or cyber physical systems security. I've engaged in robust professional development and might even take on more than I should. But, it's smart to force yourself to continue to learn. I also try and force myself to take at least one professional certification exam a year, if not two. And the reason I do that is because, as most CISOs, I'm very busy and if I wait for an opportunity when I'm not going to be busy, it'll never come."