PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

SUZIE SMIBERT

CISO & GLOBAL DIRECTOR ENTERPRISE ARCHITECTURE, FINNING INTERNATIONAL

HEADQUARTERS: Vancouver, British Columbia

EMPLOYEES: 14,500

ANNUAL REVENUE: $6.9 Billion (Canadian Dollars)

BUILDING A CULTURE OF CYBER SECURITY

Suzie Smibert, the Global Director of Enterprise Architecture and CISO at Finning International, the world's largest Caterpillar dealer, knows her strengths. She explains, "When I get hired, it is because they want to build something from scratch, create a culture of cybersecurity, bring on a team, processes and vision, and execute on it." Finning brought her on board to set the cyber security groundwork for the company.

When Smibert joined the organization, she understood the cyber security program required dedicated work and a strong, positive influence. She comments, "The existing cyber security program was still very much a dinosaur. It was a program predicated on saying 'no', not wanting to enable business and find a different way of getting things done. My team was motivated to switch that mindset and we wanted to find a creative way of making things secure."

Almost three years into the role, Smibert reports the company has advanced significantly, but as most security programs, still requires continued support. She says, "Finning is a large organization that historically has not thought of itself as innovative in technology, yet we are transforming and growing our digital business."

To that effort, Smibert notes the company has made tremendous progress with regards to cyber security awareness. She notes, "That is the easiest and cheapest way to reduce risk to an organization and engage the end user communities and executives in wanting to support cyber security."

Smibert continually works to instill security as a basic safety issue for the company. She explains, "People do not think twice when they see a cable on the ground. They say, 'Hey, that's a safety hazard' and then they make sure no one trips on it. We're transforming our culture so cyber security becomes the same as our reaction to health and safety issues like that. "

The work of Smibert and her team are paying off in this regard. She says, "We went from an industry average click-rate on our phishing campaigns to less than 10% globally. That is a tremendous achievement for our organization over the last few years. Once we achieve a very solid foundation, and our security culture is more mature, we are able to leverage automation capability for e-commerce and for IoT devices for our customers."

MAKING CYBERSECURITY PERSONAL

To transform Finning's cyber security culture, Smibert made security personal for the company's almost 15,000 employees across the globe. She explains, "We have a multi-faceted approach to training. Not everybody learns the same way. One of our team members is a behavioral psychologist. He made us realize the mind works differently depending on our countries and languages. Some people need to read, others need to hear, others need to see."

To address these different learning styles, Smibert's team provides various security training tools, including videos, posters, face-to-face training and third party-led sessions. She states, "We focus on making learning fun, and reaching an individual with the tools they need to succeed."

Her personalized approach extends beyond diverse training tools. "We are making cyber security awareness about the individual, not about the organization. Our employees need to understand there is something in it for them, as opposed to making cyber security all about compliance and protecting the company. We make our training personal by providing tips to improve security at home, while shopping, and for child safety online." This approach helps Finning employees internalize the value of cyber security.

EXECUTIVE SUPPORT BY ALIGNING SECURITY TO BUSINESS GOALS

Executive alignment, including valuable support from Finning's CEO and CIO, strongly helped empower Smibert's security program transform the culture of the company. Furthermore, her relationship with the Board weighs strong, she says, "It is respectful; there is trust, and the right questions are being asked. I have been privileged to not be confined to only five minutes, once a year, in front of the Board. We have a dialogue and ongoing conversation on the state of cybersecurity, risk profiles and the trends we see. The CEO and CIO have empowered me to execute on my strategy. That has helped me drive lots of change."

Smibert gained the confidence of Finning's Board by focusing on key, valuable business-aligned metrics. She comments, "What I do must support what the company's objectives are. I like to understand where we are in terms of maturity. What are we missing? What are the biggest risks? Then, I need to understand the senior leadership's and the board's overall risk tolerance."

Her presentations to the board constantly relate to business goals and risks. As a result, the Board understands and acknowledges the state of the program along with Smibert's goals and what she needs in order to execute on the program. She notes, "We are not presenting metrics about how many attacks we have thwarted. Instead, we are translating our content from security in terms of maturity, in terms of impact to bottom-line and in terms of reasonable and prudent operating model."

Building a High Performing Team

Smibert believes great talent attracts more great talent. She explains, "Empower your people when they join your organization. My job is to remove obstacles and give them guidance. Let them fail and fail fast, and do not dwell on it. Instead, celebrate and make progress."

When it comes to the perceived lack of available talent in the cybersecurity industry, Smibert believes security leaders are being self-limiting. "I think we are bounding ourselves too much to specific degrees and technology, or specific paths to get where you are. You could hire paralegals, auditors and HR people. We are restricting ourselves too much in what we are looking for in terms of talent. We keep looking for technical backgrounds. But those technical people, they hate writing policies and they do not like to present when it is security awareness month. Other backgrounds might be more inclined to round up all the diversity of thought you need in a team."

"I see the stigmas around the security industry changing. I have a diverse team comprised of different ethnicities, backgrounds and genders. While my team is one third female, integrating women into the security industry is key and must start with encouraging more women to be interested in STEM fields. We need to promote, be visible and not tolerate anything that goes against diversity."