PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JUSTIN SOMAINI
CSO, SAP

HEADQUARTERS: Walldorf, Germany

EMPLOYEES: 84,000

ANNUAL REVENUE: $26 Billion

"I think it is human nature to want to talk first, in order to communicate your point. But to build relationships within the company, you must ask questions and find alignment with others. It is important to start with a consultative approach to these initial conversations, as you work to understand their business goals and challenges."

- JUSTIN SOMAINI

TACKLING BIG CHALLENGES, FROM THE GLOBAL THREAT LANDSCAPE TO SECURITY SKILLS SHORTAGE

While Justin Somaini believes there are only two main reasons he took the newly established role of Chief Security Officer at SAP in 2015, it might better be described as more than 300,000 reasons. He explains, "The first thing that motivated me to take this role at SAP was the challenge of tackling the threat landscape on a global scale. The second reason was SAP's more than 300,000 customers. SAP's product security is critically important to our customers, because our solutions deal with their most critical business information."

As Chief Security Officer at SAP, Somaini leads a team of 250 security professionals, providing physical security, enterprise security and product security. For Somaini, the high stakes nature of SAP's security program is very appealing. He comments, "Probably more than many other companies, SAP sits right in the middle of the information security challenge on a global scale. My team has the ability to shift the needle on security and solve big problems for our customers."

Somaini says SAP made a significant commitment to security starting in 2015, when the Board created the CSO role. This high-level commitment holds important to Somaini's ability achieve success within the role. He explains, "SAP is not just paying lip service to security. This is obvious in the way the organization is structured." Somaini first reported into a Board member, and now into the CTO. He says, "Security remains a Board-level priority and many conversations about information security take place at that level."

"YOU HAVE TWO EARS AND ONE MOUTH FOR A REASON"

A true veteran as an industry leader, Somaini has held many distinguished security positions before,

most notably the CISO at Yahoo and Chief Trust Officer at Box. He explains, "The first three months as a new CSO can feel like vacation. It's all about kissing babies, shaking hands, and understanding the environment." He explains one of his first priorities is to understand the objectives and challenges of business owners. "In the first three months, you want to gauge security maturity within the company, ensure security is aligned with business priorities, identify major problems and most importantly, build strong relationships with peers inside the company."

He continues, "But the first year can be a real challenge too, you need to make strategic decisions while dealing with tactical problems, and sometimes without all the information you would like to have. That is why it is so important to form strategic relationships with line of business executives."

Somaini notes that at SAP, the line of business leaders are very open and receptive to having conversations about security, and making changes to address security problems. He has advice to pass on from one of his mentors, John Thompson, the former CEO of Symantec.

"John said to me, 'You have two ears and one mouth for a reason. Use them to listen twice as long as you talk.' I think it is human nature to want to talk first, in order to communicate your point. But to build relationships within the company, you must ask questions and find alignment with others. It is important to start with a consultative approach to these initial conversations, as you work to understand their business goals and challenges."

Somaini also suggests new CISOs should prioritize learning the business, first and foremost. He suggests, "New CISOs need to educate themselves on the business. For example, understand how marketing works, and how it can impact the sales cycle. Sometimes security teams are out in left field, with no visibility and no desire to understand how businesses operate. But to build alignment and to figure out how to build security into the business you need to be able to speak the language of business. Few line of business leaders will participate in security efforts if you cannot speak their language."

UNDERSTAND CUSTOMER REQUIREMENTS AND PRIORITIES

According to Somaini, after the first year, security efforts should evolve beyond internal operations to understand customer priorities. "We have to understand how our customers are using SAP products and what their specific vulnerabilities and requirements are for the product. We have customers across multiple vertical industries, and their expectations are not always the same. We must realize what a financial services organization needs and expects is different from what a healthcare or oil and gas company needs. I am constantly assessing if my team has a good read on customer expectations and if our security measures are meeting and exceeding those expectations."

STAFF A PYRAMID TO CONQUER THE SKILLS SHORTAGE

"I've been doing information security for more than 20 years, and I can tell you that the skills gap is nothing new. In 20 years, security teams have evolved from offering simple technical solutions, to addressing compliance requirements, to understanding international law, and now we play a role in the customer purchasing cycle. As an industry, we have a massively increasing expectation of skills every year for our security professionals," explains Somaini.

He continues, "Information security is a tough business. Every company is looking to hire from the same mature talent pool, which cannot expand quickly enough to meet our needs. When you really think about it, this is a silly way for us to be addressing the growth of our industry."

"When we only hire mature and experienced professionals, we stifle growth. That is why I staff our organization as a pyramid. Most companies staff information security like a diamond. There is a CISO, then a large staff of experienced security professionals, then only a handful of early talent. With pyramid staffing we have experienced security professionals distilling difficult challenges down to simpler problems that early talent can address confidently, while also learning from new experiences."

At SAP, Somaini introduced a two-year training program to bring more employees into the security program. His managers identify young professionals, recent college grads, or IT support staff who are curious, technically adept and have a strong moral compass, and put them through a two-year on the job training program. This gives young professionals the opportunity to mature more quickly into more senior roles.

Somaini points out that on-going training is required, as once a security professional reaches the management level they need another set of training in managing people and programs. He says simply, "Our organization needs more mature and skilled employees, and it is our obligation to train people to fill those roles."

He is also quick to note the need for on-going education does not stop outside the CISO's office. He explains, "The role of the CISO is continuing to mature as we would expect, and as result we need to have leaders that are continuously educating themselves."