PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DOUG GRAHAM
CSO, NUANCE COMMUNICATIONS, INC.

HEADQUARTERS: Burlington, MA

EMPLOYEES: 14,000

REVENUE: $1.93 Billion

DOUG GRAHAM IS A CHANGE AGENT AT NUANCE

Doug Graham, the Chief Security Officer at Nuance Communications, views the CSO position as a "change agent, driving transformation across the organization." Before he joins any organization, he evaluates the company's commitment to the security program, and the company's ability to withstand the kind of change required to build a next-level security program.

Graham notes, "While the interview process is the organization's chance to learn more about me and determine if I am a good fit, the interview process is equally my opportunity to gauge if the security program is well-supported within the company."

He continues, "At the C-Level, information security is more about chemistry, fit and philosophical alignment than it is about technical capabilities. Of course, a CISO or CSO needs to have a technical resume, but if he or she cannot work with the other executives, or within the existing company culture, it will be difficult to be successful in driving change. In the interview process, neither the company nor the candidate will have all the answers, but both sides should be able to come to a shared understanding of what a good program will look like."

At Nuance, Graham says his charter is, "to strengthen the security posture and build out a strong team, and make the security program match the company's culture."

VETERAN CISO ADVICE FOR THE FIRST 90 DAYS

With many years of leadership experience in information security, Graham offers advice to CISOs who may be new to the role. "There is a bucket of things to consider in the first 90 days in a new organization," explains the veteran CSO. Graham recalls these priorities:

1. Assess the maturity of the security function

Graham encourages CISOs to first understand the knowledge levels of team members across technology, governance, risk and compliance and policy. A new CISO must determine if team leadership accurately reflects the structure required to effectively enhance the security program. When possible, review previous security efforts and understand where the previous CISO succeeded and failed.

2. Understand the operating model of the company
Graham points out the importance to understand organizational structure. For example, he states, "Identify if there is a single IT entity across the organization, if shadow IT is a concern, and if the company operates offsite data centers and global operations."

3. Build a network of support
"Build support for the security program from the top down, as this will provide the necessary mandate for security changes," explains Graham. It is also important to note the relative security expertise across the entire organization. Security savvy organizations will more easily adapt to changes, while less savvy teams may need more persuasion.

Graham says at the end of sixty or ninety days most organizations will expect the new CISO to be able to provide a high-level read-out on the security program, including basic outlook, significant risks and priorities.

A FIVE-POINT PLAN FOR SECURITY

Once a high-level understanding of the security program is in place, Graham suggests implementing a strategy. Graham notes, "A twenty-page document or dissertation is not required, but something that can be modeled and repeated, and aligns with future activities, is a good starting point." As an example, Graham shares his "five-point plan". He says the plan provides clarity about your mission and encourages a consistent approach and set of core goals.

Nuance's five-point security plan includes:

1. Company-Wide Security Hygiene
"Security needs to be treated like hygiene. Everyone needs to do it, just like brushing your teeth. Although every organization has a security team, security is everyone's responsibility."

2. Incident Detection and Response
"There needs to be a system of safeguards in place for when hygiene fails."

3. Compliance Management
"At Nuance, we have a billion-dollar healthcare practice, and we often operate with financial services organizations. We need to understand compliance across those industries, and many others. We must understand privacy requirements and regulations, and acknowledge that sometimes those requirements will conflict with our risk strategy."

4. Risk-Based Strategy
"My goal is not to create maximum security. We need to balance risk with security. We always have to consider that too much security opens up its own risks, and presents challenges to business operations."

5. Customer Transparency
"We will not meet our revenue goals if we cannot present a transparent security program to our customers."

Graham notes, "These five points have been the five key pillars of our security program since day one. Everything we do aligns back to these points. We report to the Board based on these pillars."

While this program, which tends to be more qualitative than quantitative, works well for Graham, he cautions new CISOs to resist a one-size-fits-all model for presenting to the Board. "You want to tailor your presentation to the Board based on context and situation-specific requirements. You need to do your upfront research. Understand who is on the board, what their security knowledge is and how they absorb technical information," explains Graham. He continues, "The most important part of any Board meeting is the work you do before-hand and the action items that come out of it."

CYBERSECURITY SKILLS GAP

"I think there might not be as big of a gap in the market as we think. I think a lot of CISOs are looking for unicorns. They want to find one employee who can do every aspect of the security job. Someone who is technical, a visionary, an architect and a skilled operations guy. That is just not realistic. This might be because we ask for five employees and we get budget for two, so we try to jam-pack our job descriptions. We must design our job descriptions based on realistic understandings of the talent pool."

Graham continues, "Security people have an unbalanced sense of duty. More than salary and work-life balance, they want to do the right thing and impact change. I see security people get really frustrated when feel they are not listened to within the organization. If you are able to pay the right people a fair salary and show them the organization is behind the security vision, and if you can give them the opportunity to impact positive change, then you are much more likely to hire and retain talent."