PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

BRIAN HAUGLI

VP & CISO, THE HANOVER INSURANCE GROUP

HEADQUARTERS: Worcester, MA

EMPLOYEES: 4,800

ANNUAL REVENUE: $5 Billion

ELEVATING THE CISO ROLE AT THE HANOVER INSURANCE GROUP

"I report to the Chief Administration Officer (CAO), as do the CIOs for all of The Hanover's lines of business. This was really important to me when I took the position," said Brian Haugli, who is ten months into his role as CISO and Vice President at The Hanover. "This reporting structure is incredibly valuable. I participate with the CIOs in discussions around efficiency and operations; my opinion is valued equally. When I speak to CISOs in other companies who report to CIOs they tell me they have the problem of having to defer to their CIOs regarding those kinds of discussions and decisions. I don't have that issue."

Haugli's boss, the CAO, was hired just four months before Haugli, and highly values the role of the CISO. This support gives Haugli tremendous confidence in his ability to evolve the security program at the company.

With executive-level responsibility and visibility, Haugli has regular access to the company's leadership. "Information security is critically important at The Hanover. Maintaining security around the data our agent partners and their customers entrust to us is essential. With that in mind, I meet monthly with the CEO to go over operational security areas, security posture, and on-going initiatives," said Haugli. "His interest in security and support around making our security initiatives more effective makes my job much more rewarding."

ASSET OWNERSHIP AND RESPONSIBILITY

"I get really solid questions about The Hanover's security posture from the members of our leadership team. They want to know what we are doing, what is going on in the news, and what the global picture is. They want to talk about business risk and take that into account. It's an open dialogue that is influenced by our strategic business goals," said Haugli.

"We talk a lot about asset ownership, and understanding what is most critical to the business

units. We look at the systems and processes that are revenue generating for each line of business," said Haugli. "They want to make sure our technical investments and capabilities align with business needs."

When Haugli speaks to the business units about security he focuses on two areas – asset ownership and general security awareness. "I am a big proponent of establishing asset ownership," Haugli reiterated. If I am looking at a network component, I want to know who owns it. That person needs to take responsibility for what is on the system and ensure systems and processes are secure. If no one takes ownership of a system it is very difficult to make positive changes to it, and it probably should not be in the technology portfolio."

Haugli uses education and awareness training to heighten awareness and change behaviors by employing practical applications of security best practices. "I use a lot of analogies to educate about vulnerabilities and the need for patches and security changes. I say, 'Just like you do not want your kids' friends to be playing computer games on the computer that you do personal finances on, you also want to limit access to your systems at work.' We want to be certain that access privilege is given only to those who need it."

BUILDING A TEAM AND A ROADMAP FOR THE FIRST 18 MONTHS

Just ten months into the job, Haugli has just begun the transition from what he describes as "unboxing the company" to creating a strategic 18-month plan to strengthen the foundational aspects of network security and vulnerability management. While Haugli's background is in the Federal Government, the learning curve has been minimal and he is quickly developing an understanding of the network, people, and organization.

"I am growing my security team internally and I have hired a new Director for Governance, Risk, and Compliance who, like me, came from a government background." He also created and hired a dedicated Manager of Training and Awareness Outreach. "His entire role is focused on the human element of the company. Everything is about the employees, in order to train them and make them more aware."

During the hiring process, Haugli approaches candidate searches by focusing on skill sets and overall ability to adapt. More importantly, he believes there is not a "one-size fits all" in information security. For example, the manager Haugli hired to perform security training was a math teacher with a Masters in Psychology, resulting in an impactful team member with the ability to better understand user actions and teach new behaviors. He is able to take feedback from operations about what they are seeing in terms of security issues and go talk to the employees responsible for the asset and hash the issue out effectively. He is able to understand their process and work with them to make the process more secure."

"Strict hiring specifications can often preclude really solid candidates who would perform well in specific roles. I will look at the person who might not fit into a corporate workspace and see if they are the best person to hunt for malicious activity on our network. You have to understand and evaluate specific skill sets against the job function."

Revenue Impact of Cyber Insurance

"Insurance is one of the few sectors where security has a clear opportunity to impact revenue," said Haugli. "I cannot think of how a manufacturing firm or a retail company can empower a CISO to drive revenue. But in insurance there is a clear need to enhance our cyber security insurance program and that takes insight from Information Security and a solid understanding of risk management practices. At Hanover, I have been working with a specialty line of business on improving risk management and bolstering our capabilities around cyber insurance." Haugli says Hanover has several different cyber security products but what the industry really needs is a uniform national standard to measure risk against in offering these insurance policies. "NIST is one of the best standards to come out over the years, and is a great first step in the right direction."