PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT INFORMATION SECURITY PROGRAMS

CORY SCOTT
CISO, LINKEDIN

HEADQUARTERS: Mountain View, CA
EMPLOYEES: 9,900
ANNUAL REVENUE: $2.99 Billion (2015)

When Cory Scott joined LinkedIn more than three years ago, he took on an emerging, yet highly visible role at one of the largest social networks in the world. "LinkedIn is in a unique position in the ecosystem. We are a large social network focused on the professional aspect of peoples' lives. The platform has influence on peoples' careers and personal growth, and I was very attracted to the job. When I came on board there was not a significant security presence, so this was also an opportunity for me to build the information security program from the ground up," said Scott.

In order to strengthen and elevate the security program, Scott understood he needed clear support from most senior executives. "When I was considering the role, one of the things I was concerned about was the support of senior management," Scott continued, "I was lucky to speak with Jeff Weiner, CEO of LinkedIn, during the interview process. We talked about the priority he knew LinkedIn needed to give to security. I found he had an incredibly detailed and technical grasp of the challenges of security. He had taken the time to educate himself on its value. He was very supportive of putting security first to build up the trustworthiness of the platform."

The trustworthiness of the platform is a central theme for Scott. Building up consumer, internal and partner trust in the security program at LinkedIn is the guiding objective for Scott's group.

"Trust in our platform is integral to how we execute on our vision to connect professionals and make them more productive and successful. If members believe that LinkedIn is a trustworthy place to do business then they will engage with the platform more, and the more they engage, the more valuable the platform is to them, and to us as a business."

"In my three and a half years here we have learned a lot about the value of trustworthiness. What matters is not just the impact of security actions, but the message you send about security as an inclusive, participatory initiative. It signals to the rest of the world that the organization takes security and privacy into account at every step of development and innovation. Security is moving more into the forefront of peoples' minds. It is something they consider more now than ever before."

Scott runs his security program to support the company's mission of connecting professionals to make them more productive and successful. Three specific objectives drive the information security organization's ability to make a positive impact.

1. Attract and Retain Talent Who Execute on Vision – When building an effective team, Scott knew he must

first consider the audience and culture. LinkedIn has a strong engineering and data-driven culture, so his security team consists of employees who succeed in that environment. “Even the program managers on my team have written software. When the security talent aligns with the rest of the organization, we have more successful interactions. It also makes our organization more attractive partners to the other business units.”

Scott continued, “It is no secret there is a shortage of security talent. Because we are LinkedIn, we have access to a lot of data on supply and demand for professionals. For every four people employed in information security today there are three open positions. It is hard to find talent with specific security expertise. To combat this, we try to bring people over the wall from other parts of the technology organization into our security team.”

He said, “We have a strong technical bar for almost all security employees. We also look for people with key soft skills, who understand how to problem solve and work with multiple stakeholders. Most important of all, we want our team members to be curious. They need to want to figure out how things work, and how things can be improved.”

2. Achieve Operational Excellence – Scott’s team must understand how to handle demand, standardize on approach and processes, and effectively communicate success as it relates to key metrics. When measuring success and reporting on metrics, Scott divides the functions of the security team into two sets – internal demand and external demand. “Internal demand includes securing the infrastructure, discovering new attacks, maintaining plan alignment and reducing security risks. Progress on these efforts can be tracked via traditional means, such as milestones and achievements. But the other 50% of our time is spent on external demands, which are tougher to measure. This includes servicing the organization, ensuring new projects and programs kick off with strong security, doing compliance work and reviewing contracts and plans because policy requires it. External demand boils down to supporting someone else’s big project. But we still have to measure our work. So we measure things like the number of security reviews we do, the number of bugs found before the application goes live, and we have metrics to measure incident response.”

It is important to note that Scott shares these metrics with all stakeholders, not just his team. He said, “We report on our performance to my direct manager and CEO, but also horizontally to the head of IT, legal counsel, the internal audit committee and engineering leadership. We want a lot of people to be aware of our organization’s performance.”

3. Foster an Inclusive Program – “We emphasize that security is not a team in the corner or in an ivory tower,” said Scott. “We try to be available and involved. That means we are visible, both online and offline. We hang out where engineering and operations congregate and spend time in the same internal chat rooms. Our role is as internal consultants to help teams find solutions to security problems and reduce risks. We want them to see us as advisors more than regulators.”

Scott’s team expanded upon the standard security ambassador programs that some organizations run, when they created the Security Champions program to foster inclusion and commitment outside of the security team. This program requires 25% of an employee’s time and is a six month commitment. “The program is broken into two halves. The first half requires participation in the Stanford Continuing Education program to obtain a certificate in advanced computer security. Once that is complete the Champions become advocates for security within the company. They also perform a “tour of duty”. We put them to work on security, this is where our program goes beyond traditional ambassador programs,” said Scott.

Scott noted that interest in the program is high (they have a waiting list) because security is fun and interesting, but also because it is a good career move. He said, “LinkedIn is committed to the development of our employees. Our founder and executive chairman Reid Hoffman wrote a book called The Alliance that focuses on the relationship between employee and company and the mutual agreement to support advancement, including the employee’s next play. The Security Champions program fits right into that approach.

Scott believes LinkedIn’s approach exemplifies what the future will look like for information security, as the discipline takes on a bigger role. He commented, “Security is becoming a key differentiator for products as they go to market. Large organizations talk about it now as part of their core message. There is always a need to tell a good story about security to the market.”