PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JENNA MCAULEY
CISO, MERCER

HEADQUARTERS: New York

EMPLOYEES: 20,000+

ANNUAL REVENUE: $4 Billion

Jenna McAuley is eight months into her role as CISO at Mercer, a global consulting leader in talent, health, retirement, and investments. She says, "At Mercer our mission is to advance the health, wealth, and careers of 110 million people. We do that through talent development and learning programs. The mission of Mercer is tightly entwined with my approach to security. I believe in the idea that security is a corporate culture. It needs to be in the fabric of everyone's interactions with clients, customers, and data. So this human-focused approach to security is really just a natural extension of the Mercer mission." She continues, "My biggest objective is expanding ownership of security. I want to empower people in accounting, HR, and executive assistants – everyone in the company – to realize that they can be a part of the security solution."

COMMUNICATION, REVENUE ALIGNMENT, & EFFICIENCY GAINS

McAuley employs a number of security awareness training programs. One successful program was a blog campaign tied to Cyber Security Awareness Month. For 31 days she posted a new, easy-to-understand blog post each day about a different security topic, such as two-factor authentication to better secure your Amazon account. Her users truly embraced the learning because it was communicated in an easy-to-understand and engaging manner. By the end of the month she was able to impart more advanced security topics, like threat modeling. As employees felt empowered to protect themselves outside of Mercer, they felt, in turn, more empowered to protect Mercer as well.

McAuley takes security out of the back room and makes it something everyday users can understand and talk about. Bringing security out of the back room means technical team members have to be competent communicators. "Communication in general is so important. We need to translate the technical aspects of what we are doing to a non-technical audience. This is likely the most important factor for career growth for security professionals. You have to be able to translate battlefield to boardroom. The ability to communicate how security impacts sales and revenue in a business manner is critical."

Prior to Mercer, McAuley worked in consulting, where she had to prioritize financial impact for her clients. She says, "As a consultant I was forced to think about driving profitability. As a CISO you need to be competent in all

> For a CISO, the CIO can be a very powerful ally so long as the organization they are running is not solely a technology shop. Information Security and Cybersecurity are broader than IT. Security is based in risk and it has to be something that is aligned to business strategy. As long as you have a broad enough perspective into these business functions, then the security program can be effective under the CIO. When the CIO function starts with information, not technology, the CISO and CIO functions can be highly collaborative and successful.

technical domains. I need to be competent as an incident responder, as a SOC engineer, I need to understand threat intelligence. But layered on top of that is the sense of driving profitable growth."

Another way McAuley is instilling a security aware culture is by saying "Yes". She says, "These days clients are buying with security as a consideration. They need to know that their information is protected, and used appropriately. This is a great opportunity for our team to show our impact on growth. Instead of viewing security as a cost-center, we aim to present security as a key business enabler that can drive profitability and client experience. We need to take down some of the challenges and frictions between security and process in an organization and focus on how to be more operationally efficient with our security. We need to make it easier for employees to be productive. We do that by saying yes instead of no and figuring out how to securely enable those functions."

DRIVING THE CONVERSATION WITH THE LEADERSHIP TEAM

"Transparency is a big part of how I communicate to my leadership team. I present a realistic portrait of where we are and where we need to be. If you want the CEO and CFO to understand the technical risks and the value of a solution you want to implement, then it behooves you to articulate the ROI. That means answering questions like 'How are we mitigating risk?', 'What is the commercial viability of a solution?', 'How does this solution drive the growth agenda we have as an organization?'. Understanding our growth agenda is of critical importance. If I don't understand where we need to grow then I don't understand how to securely enable it."

As with many companies, growth will come from innovation, a large priority for Mercer. McAuley needs to be in lock step with the CEO's vision in order to align security appropriately to enable innovation. To do so, McAuley says she follows the military concept of "two-up/two-down". This means the team needs to have an understanding of the priorities, challenges and decisions being made two levels up, while teaching and coaching those same priorities and challenges two levels down the organizational hierarchy. This approach allows her team to understand motivations and drivers across the organization and effectively communicate and position security to be successful.

McAuley has open dialogue with her CEO and the rest of the executive team. While being open to any questions or concerns they have, McAuley makes an effort to drive their conversations by proactively providing educational information. "Rather than waiting for a question from my CEO, I try to keep the leadership team well-informed. I send a weekly communication explaining what has happened in the industry and the potential impact it can have on Mercer." By driving the conversation, McAuley is able to better direct the CEO and various executive committees' questions and areas of attention.

STARTING EARLY WITH CYBER SECURITY AWARENESS

It is no surprise that a CISO who values the human element of security would want to start early with security training. As a member of the Executive Women's Forum, McAuley regularly participates in the Cybersecurity Schools Challenge. In the challenge, security professionals teach kids as young as five to think about online safety and security.