PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

ED FERRARA
CISO, CSL BEHRING

HEADQUARTERS: King of Prussia, PA

EMPLOYEES: 17,000

ANNUAL REVENUE: $6 Billion

"It is important to remember that information security is one of 500 issues that the Board is dealing with at any one time. We need to have a succinct and clear message to the Board – this is what we are dealing with; this is how we measure it; and this is our path."

- ED FERRARA

It is not uncommon for CISOs to take non-traditional paths to the role, as the industry has only recently emerged. Ed Ferrara's path is just as unique as many of his peers. Ferrara came to the position of CISO at CSL Behring after getting his start as a software engineer, designing new software development processes and methodologies for complex software projects. He became interested in information security because of the poor quality he was seeing in software. It is as most security professionals believe the source of all hacks. Hackers take advantage of software vulnerabilities. Prior to becoming CISO, Ferrara worked in consulting leadership for several global tier 1 consulting companies. Some may recognize Ferrara as the former Vice President and Research Analyst for cybersecurity at Forrester Research.

Ferrara looks back fondly at his time as a Forrester analyst but says he made the jump to become a CISO because he wanted to be more involved in the implementation of strategic security initiatives. He says, "At Forrester, we wrote and researched security topics, but I wasn't doing the dirty work. I wanted to get my hands dirty again, and when the CSL Behring CISO position came up, I jumped at it."

The specific opportunity at CSL Behring has motivated and energized Ferrara. "We are a six billion dollar company providing lifesaving therapies that treat immune deficiency and hemophilia. We are growing fast and that creates its own security challenges. We are growing in parts of the world, like Asia, that require significant security investment."

Ferrara is the company's first CISO and comments, "I am really building the program from the ground up. Before I arrived, CSL had implemented specific security controls,

but there was an inconsistency to the model, so we started with the blocking and tackling first."

Ferrara reports into the CIO, and believes that the Business Technology (BT) organization is the appropriate spot for his security team. He says, "The question of where the security organization should exist within the business is largest a question of maturity. For us, BT is the logical place for my team. Historically, there has been an adversarial relationship between information security and application and infrastructure teams. But we do not have that here. Part of the reason why is because I do not allow my team to say, 'no'. We says 'yes, and let's do it securely'. With this approach, we break down walls and build relationships that make us successful."

"I always use this metaphor," says Ferrara, "The president says to the Secret Service 'I am going to Iraq' and the Secret Service does not say no. It is their mission to allow him to go there safely."

CONFIDENCE IS KEY WITH THE BOARD

"It is important to remember that information security is one of 500 issues that the Board is dealing with at any one time. We need to have a succinct and clear message to the Board – this is what we are dealing with; this is how we measure it; and this is our path."

"This is not the first time I have presented to a Board. I think that Boards are really good at taking a read of the presenter. If the presenter is confident in their data, and projects confidence that he knows what he is doing, then the Board will not have too many questions. Of course the Board also relies on the CEO and COO to assure them that they should place their confidence in this person."

MANAGING ALL THE NOISE

There has been a massive and nearly unprecedented influx of spending from venture capitalists in security startups and as a result, noise in the market. Every vendor touts the next big solution. These startups combine with increased political chatter about cyber security and front-page hacks to create an awful lot of noise and potential distractions. Many CISOs have found it difficult to keep focused on their strategy and execution.

Ferrara says, "This is something I talked a lot about at Forrester with other analysts. We would get a lot of calls from threat intelligence vendors. Threat intelligence is great as long as it is actionable, but if you have all that data and can't do much with it, then what is the point? But the VCs see this as a growth industry. There are lots of smart people studying threat-scape and coming up with ways to protect and defend. At the end of the day the customer needs to do a lot of due diligence. Speaking as a former analyst, I can say that due diligence means doing more than just reading the analyst report and buying the recommended technology. Consider how the technology fits within your business model."

Ferrara continues, "The analyst in me dies hard, so I make it a point to do regular research. I read Daily Dave and Krebs. I also do a lot of my own research on specific topics that are important to us, such as cert management and web filtering."

The Best Way to Learn is to Teach

"I teach one course per year at Temple University. It is a Masters level course titled Data Analytics for Computer Audit and Cybersecurity. In the class, we use big data techniques to find adverse behaviors, such as expense fraud or finance fraud. We also look at cybersecurity. The interesting thing about the class is it combines students from two tracks – audit and cybersecurity – they learn from each other. Fraud detection is all about understanding patterns of behavior, which is where a lot of cybersecurity is headed. Teaching is more than a hobby for me, it's the best way for me to stay current and continue learning."