PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JAY LEEK
CISO, BLACKSTONE

HEADQUARTERS: New York City, NY

EMPLOYEES: 2,190

ANNUAL REVENUE: $7.4 Bliion

"I believe that we have a CEO-led information risk and security program," says Jay Leek, CISO at Blackstone, a New York based asset management firm. According to Leek, a CEO-led information risk and security program means Blackstone executives contribute to a strong top-level commitment of protecting company assets and information. Leek became Blackstone's first CISO four years ago due in part to support from senior management in the firm, who were the major drivers in creating the position. During this time, senior management clearly identified security as a priority for the company, something that remains a top priority today.

Leek reports into Blackstone's CTO, who reports to the CFO, yet still possesses ample visibility with other senior leaders throughout the firm. When *Feats of Strength* spoke to Leek he had just come from a regular, standing meeting with Blackstone senior leaders. In that meeting Leek presented the three year security plan for the company. Leek says Blackstone senior management's commitment to security comes from understanding the value of the firm's information. Leek says, "My senior management feels confident in where we are, but remains on guard about the unknown. The key takeaway is that we can never slow down. In fact, it is how can we speed up? We are constantly challenged to push the program as fast as we can without breaking the organization. We have a responsibility to do our best to protect the firm for our shareholders and limited partners."

Since Leek has regular interaction with senior management, he has developed a proven approach to effective communications. "Facts," continues Leek, "We weave in qualitative analysis about our company, and support that information with external data points. Our program is focused on situational awareness, intelligence-led information security and risk management. With regards to threats and incidents, we need to know who, why and how they are attacking us. We need to know their motivations – that requires intelligence gathering and situational analysis. So we educate our senior leadership on this information and approach, and back it up with facts. This approach helps us frame the problem on a continuous basis and helps the executives wrap their heads around it."

Leek states that part of building and maintaining an executive-supported security program requires thinking like business people, specifically your company's business people. "If our senior leaders think of me as just 'the security guy' then I have failed in my mission. I believe that our leadership team views our security team as business leaders who simply happen to know a little more about security than others in the room. This approach allows us to function as

Mentors and a Network of Peers Help Leek Make Tough Decisions

Leek is fortunate that he has access to a large network of security professionals, which he has helped to hire at Blackstone's portfolio companies. Accordingly, Leek serves on the Board of some early stage security companies, so he has multiple opportunities to engage with security leaders. One of Leek's mentors is Jim Routh, the CISO of Aetna who was also featured in *Feats of Strength* last year. Leek says, "I have so much respect for Jim. I have consulted with him, in an advisory way, before I have made big steps in my career. When we see each other, we compare notes and collaborate. I have a lot of senior level security executives like Jim in my network and am both grateful and fortunate for this. We make a concerted effort to get together on a regular basis and compare notes. We are a collaborative community so no one has to reinvent the wheel. We learn from each other's successes, and yes, failures, too."

trusted business advisors in conversations about cyber risk. We must be thoughtful in how we frame that risk in regards to all the other risks across the firm."

Retaining a sturdy business-focused approach permits Leek to consider security through the lens of a financial business leader. He asks, "What is the impact of this security function on the business use. How does the business user feel? Does it impact their work? What is the benefit the business gets from this security control? Is it worth it in the end?"

With security as a central priority for the company, Leek acknowledges the opportunity for security to be considered a competitive advantage for Blackstone, even though the company does not talk about security externally very often. "The alternative asset management community is close knit. There may be eight or nine firms that have CISOs. We are very open in communicating across all these firms and believe this is an important advantage. We also educate our limited partners on what we are doing from a security perspective and why we are doing it. They ask about business continuity and disaster recovery, and we go beyond that to explain information security risk management. It sends a positive message to our limited partners. These limited partners are making 15-20 year financial commitments with us. They want to know our strategy and our culture to make sure their investments and information is safe." Leek believes their security program can be a differentiator in many of those conversations.

A "NO EGO" POLICY MEANS GOOD SECURITY IDEAS CAN COME FROM ANYONE

"I believe that over the last 20 years, as an industry, many of us have done a disservice to our security programs with complex frameworks and too many controls. Security needs to be described simply so that everyone outside of the security and technology teams can also understand it," said Leek.

He continues, "Others [in the organization] can come up with security ideas that can make your business better when they understand security's objectives and necessity. The Blackstone security program is not my team, it is the firm. We support a culture that understands security. Our program is not perfect; we need to get better, but we have been building this culture of education and responsibility for four years. Now we have people from across the company weighing in on how Blackstone can be a safer place."

That collaborative, open environment starts within Leek's team, which includes dedicated internal security personnel, an outsourced SOC and numerous other personnel who help support security functions in other areas of the technology group and in regional offices. "We have a 'no ego' policy," said Leek, "I don't believe in a hierarchy. I do have a deputy CISO to help scale our program, but we maintain a flat organization and a team of equals. There is implicit trust between us. Every now and then someone needs to make a decision and that is what I am here for, but we work openly and collaboratively as a team. Communication is pervasive across our team. Everyone knows what is happening across the program with a few exceptions, for things like sensitive investigations. Everyone is held accountable and empowered to make decisions."

GROWTH AND EDUCATION ARE PRIORITIES FOR THE YEAR

Leek says his team works continuously at educating the most senior level management on the importance of security, but his team must focus the firm as a whole. It is everyone's responsibility to help protect the firm, and it is our job to empower them with the knowledge on how to do it. "We try to train everyone without being a nuisance. We want to make sure everyone understands security's purpose and are following processes not because they were told to do so, but because they understand the value it brings to Blackstone."

Leek's other goal is internally focused on his team. He wants to make his team operate at twice their efficiency scale of physical capacity, while working fewer hours. "I am not talking about Six Sigma, rather just automating manual functions and becoming one thousand times more efficient as a result." They are constantly striving to get closer to this goal.