SHAWN KEELEY

MANAGER OF INFORMATION ASSURANCE
BLUE CROSS BLUE SHIELD OF RI

HEADQUARTERS: Providence, RI

EMPLOYEES: 1,100

After graduating law school, Shawn Keeley was applying to legal and technology sector positions because he found both to be fascinating areas of work. He also had his Masters in Cybersecurity and was looking to marry his two focus areas. By chance, he had an opportunity to join Blue Cross Blue Shield of Rhode Island in an interim role as assistant privacy officer.

He explains, "I learned a lot in the interim role and when that position was ending, I stayed by moving into a different department, starting at an associate level on the information security team. I started with leading project management and then took over the architecture of our cloud security as we were migrating to the cloud. Then it really snowballed from there, I had the opportunity to take on governance, risk, and compliance as a program while doing project management and cloud security. And it really opened me up to learning everything about the organization, how the business worked, how healthcare worked, and how everything works behind the scenes."

Shawn then transitioned into his first managerial role, taking on manager of information assurance under the information security program. Shawn says he intertwines his legal background on a daily basis, and he feels the overlap between the two has positioned him well as he moves up in his career as a second year manager.

RESILIENCY, THIRD PARTY RISK, AND ARTIFICIAL INTELLIGENCE

Shawn's responsibilities include threat intelligence, enhanced vendor oversight, governance risk and compliance, security project management, training and awareness, privileged access management review, and the artificial intelligence product risk management process.

He explains, "There's a lot of different areas underneath me. We are part of the Blue Cross Association as a licensed entity and our big focus for the year is around resiliency. How do we make this a key priority, not only in our organization, but communicate the risk that is related to a vendor, security process, or configuration to our leadership with regards to resiliency? We make sure to create a baseline appetite and tolerance level for certain situations. It is really important for us to continue to remain resilient and keep the CIA triad, the confidentiality, integrity and availability, of our information while allowing business to take place. That's a very tough area, and it's a probably my number one priority this year."

Along with resiliency, Shawn and his team are focused on their third-party risk management program. They are working diligently to perform deeper dives into the criticality of assessments and creating a risk tier system that is easily digestible by leadership so they can fully grasp the actual risk levels. They are moving from a letter grading system to one that is numerically-risk based to demonstrate exactly where gaps may exist and ensure better remediation efforts.

AI governance is another area of focus as they are a little over a year into their work around AI development and third-party tooling. They brought in an AI product manager that has allowed Shawn time to enhance their security controls and risk awareness around projects and vendors before entering their environment. Shawn also speaks regularly on the topic of AI governance, sharing his knowledge with the community and learning from others and their experiences.

"It is really important for us to continue to remain resilient and keep the CIA triad, the confidentiality, integrity and availability, of our information while allowing business to take place."

> *"I'm always going to prioritize the needs of my team. I'm going to support their development educationally and help them get to where they want to be career wise. I also make sure that they have a balance of well-being in their life and understand that work is work and when they go home they need to be able to unplug. I encourage them to unwind and enjoy the time they have outside of work to enjoy the fruits of , their labor. That's one portion of it, that's the servant style."*

MANAGING TIME AND BANDWIDTH

Similar to many managers working in security programs, one of Shawn's biggest challenges is time management and bandwidth for his team. He states, "I've always told my team that I'd rather have 7 great days of work than 14 days of okay work because I know we can accomplish so much more when they aren't burnt out or they do not feel that they are against the wall. It's a balance to make sure our day-to-day responsibilities can take place along with any security incident we might be working."

SERVANT AND DEMOCRATIC LEADERSHIP

Shawn says he considers his leadership style a combination of servant and democratic. He has relied on great mentors to be a sponge and learn from them, and having those mentors allowed him to put those skills into practice as he moved into a manger role.

He explains, "I'm always going to prioritize the needs of my team. I'm going to support their development educationally and help them get to where they want to be career wise. I also make sure that they have a balance of well-being in their life and understand that work is work and when they go home they need to be able to unplug. I encourage them to unwind and enjoy the time they have outside of work to enjoy the fruits of their labor. That's one portion of it, that's the servant style. "

He continues, "The democratic style allows me to empower them as well. I allow them to participate in the decisions that have either tangible outcomes or output so that they can see the reward at the end, and make sure that they have a seat at the table. I like to refer to that as "listen, evaluate, discuss". I can't make a decision until I've at least heard you out as an individual and understood what your thinking is. What we have found is that that has allowed the associates underneath me to come to me with their problem, and I'll walk them through as far as I can to the end of the rope before I say, hey, jump, and that allows them to make that decision themselves."

INVESTMENTS

"No decisions are made in silos. We include IT in any decision along with different areas of the business to make sure we understand the true impact of any new tools. And at the same time, are we getting the best bang for our buck? One of the major questions we ask as we're going through it is how are we going to balance that? We have a clear picture here of how we want to do it with the mission that we've been given by our organizational leadership. It's just getting the buy in and trying to remain proactive and not reactive in tools. We see that all the time in security. We're one step ahead and then a threat actor becomes one more step ahead. So how do we get to the finish line before they do is always something we're looking at. And also assessing the benefit and cost of certain risks versus the others," says Shawn.