PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

RICHARD LICATO
CISO, THE AIRLINES REPORTING CORPORATION

HEADQUARTERS: Arlington, VA

MEMBERSHIP: 229 airlines, 7,000 travel agencies, 12,000 points of sale

ANNUAL REVENUE: $88.5 Billion airline ticket transactions settled in 2017

Rich Licato describes the path that brought him into information security as "almost by accident, then by design." Licato began his career as a developer, moving into coder roles, then management and delivery of larger projects over time. He eventually transitioned into enterprise architecture, where he moved from the delivery of systems to the design of how systems were delivered. By performing more strategic responsibilities, he gained an understanding of how a multitude of program components work together, instead of working in silos. He says, "I gained more exposure into an enterprise-view and had my first opportunity to manage security and enterprise architecture. From a corporate perspective, I saw different challenges. I also had the opportunity to work in an operational risk role before becoming CISO at The Airlines Reporting Corporation (ARC)."

As CISO of ARC, Licato ensures the organization meets their mission, which includes driving air travel intelligence and commerce, providing business solutions and travel agency accreditation services, and processing financial management tools and data. Now over six years into his role, Licato has a clear picture into the organization's operations and business functions, all of which are owned by eight major airlines.

The opportunity at ARC presented Licato with the ability to re-establish a security program, and re-energize and re-focus the organization from a security perspective. Licato explains, "I was doing consulting work for ARC and able to see how the organization operated and what challenges they faced as an outsider. I was then invited to become an insider as their CISO."

Licato felt the personal and professional growth opportunities significantly appealing as he became ARC's full-time CISO. He comments, "From a security program perspective they were in a place of transition. There wasn't a dedicated leader in the security space for them and there

> "Three things I've always been taught are to take stock of where you are, where you want to be and have the ability to articulate how you're going to get there."

was a large hole to fill. In the past, I've been a problem solver and I had the ability to set a strategy and vision. I was excited to make my own program and put my stamp on it. I was also lucky to have a leader and boss who supported me."

Not only did the growth potential appeal to Licato, but ARC's culture and environment were ripe for providing him a platform to build his program. He says, "During the interview process I made sure to understand the organization's attitude towards security. It was clear I had an opportunity to make an impact. CISOs must understand they might be able to affect the culture, but they might not be able to change it significantly from a process perspective. CISOs need to know what their constraints are and the attitude of management towards risk and security. Understanding the top down view of whether security will be supported is important."

BUILDING A STRONG PROGRAM

On building a program from the ground up, Licato states, "Three things I've always been taught are to take stock of where you are, where you want to be and have the ability to articulate how you're going to get there." Taking stock of where you are involves a great amount of self-evaluation, something Licato relied on his team to help understand. After engaging with the current team and gleaning valuable program information, Licato says creating a baseline using a framework must be done along with developing relationships with business leaders.

Licato states that establishing strong lines of communication with executives is important. "It doesn't matter what your opinion is, what's most important is their opinion on how security should function," he says. "What I mean by this is sitting down with each business leader of legal, product development, services, among others, and understanding their perspectives and expectations for security. I need to know what challenges they are facing, what problems they have, and how I can address them."

After partaking in crucial conversations and aligning with executives, Licato comprehensively understood the important business functions, how the business makes money, and was armed with information to build his program with a robust strategic focus. Licato explains, "It was clear to me I had to protect our most important assets. We make money through our settlement business that accredits travel agents, and back-end settlements from a financial transaction perspective. I need to make sure transactions are secure from beginning to end with no ways of compromise. We also have facilities for agents to charge for their services, and a data business. My mission from a business view is to secure information and ensure it will not be compromised. I am focused on less friction in a transactional environment, not putting up roadblocks that stop the business from settling transactions more efficiently, and handing the agents facility."

STRATEGIC TEAM GROWTH

Due to ARC's security professionals taking on more responsibilities and functions, Licato's team continues to experience significant growth. When Licato started at ARC his team had only a few people, which he has now grown to more than twenty members.

On building a successful team, Licato says, "For me it's about passion and intelligence. I'm looking for smart people who I can train in security functions. I'm looking for people who have an analytical nature and are always asking questions. Also, some level of skepticism sometimes works well in security." Licato leads his team with openness and honesty, to encourage them to have effective communication. He does not micro-manage, but instead creates a safe environment with everyone on the same page.

BOARDROOM FOCUS

"To me, boards are always asking if we are okay. And that can mean a lot of different things to different people. What does okay really mean? You normally don't figure it out in just one board meeting. Typically, from a program perspective, it means 'are we protected if something occurs?' Sometimes it can be a hard conversation for a board. CISOs must make sure they communicate the inevitability that something bad could occur and have adverse effects in terms of reputation or operations. Trying to have that conversation is hard, but it is necessary. There are ways to illustrate that we are okay and doing the right things and spending the right amount of money. Boards want to know what kind of protection the organization is getting for what they're spending on security. The bottom line is they want to know how you are enabling the business."