PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

LEON BROCKWAY
ISO, TOMPKINS FINANCIAL

HEADQUARTERS: Ithaca, NY

EMPLOYEES: 1,000+

ANNUAL REVENUE: $6.7 Billion

Leon Brockway had his first exposure in information security while working in military intelligence for the United States Army over 18 years ago. From there, he transitioned into the Department of Defense contracting sector, working on large projects for various federal agencies to support technology and security programs. Over the last three years he has led the Information Security Program as the ISO for Tompkins Financial, a New York state-based financial services holding company. He comments, "My work experience so far has been a case study of the transition of information technology, to IT security into information security to where we are today, what we're seeing quite a bit of in the industry is information security more appropriately aligning with business function(s) and risk management specifically, it is really an exciting time to be part of the maturity of the Information Security profession."

CONCENTRATING ON KEY STRATEGIC GOALS

Brockway approaches 2019 with clear strategic goals in mind including aligning with business and IT strategy, forming strong coalitions with business partners, recruiting, training and retaining top security professionals, establishing operational excellence and creating and maintaining key risk indicators.

Alignment. Alignment is a constant strategic objective for Brockway, as he continues to expand maximum participation around strategic discussions. He also emphasizes the importance of collaborating with his business and IT counterparts.

Strong Coalitions. He encourages and empowers his team to form strong coalitions with business partners by engaging at the appropriate management levels. He explains, "We must make sure there's good communication channels with each one of our business partners. We'll be looking to maximize that kind of coalition around information security across different departments."

Risk Indicators. On focusing his time around key risk indicators, Brockway explains, "I think we're in the intermediate step and we'll continue strategy around making sure we have solid key risk indicators, and that we have matured our program to be

"THIS IS A FINANCIAL INSTITUTION, SO IT'S IMPORTANT TO ALIGN THE INFORMATION SECURITY PRESENTATION AND REPORTING TO SOMETHING THAT MIGHT LOOK LIKE ANOTHER DEPARTMENT REPORTING."

able to measure the effectiveness of our control framework. We're in the financial industry and moving those types of indicators to a numbers game is critical, we're going to have to continue to align our metrics with the numbers that our board and our senior leadership team are accustomed to getting from other business departments."

OVERCOMING CHALLENGES

Brockway believes many of his challenges are common among information security and other business sectors. These include buy-in and adequately balancing time and resources.

He comments, "Buy-in across the organization can be a big challenge, which is also very common, and why coalition is so important across the organization. You must make sure you have really strong relationships to be able to execute these particular activities. The other challenging piece is around one of our tactical objectives, operational excellence; we're spending lots of time to make sure we're doing the fundamentals exceptionally well. And that takes a fair amount of resources and time from the information security team, and the organization, to be able to do the traditional cyber and IT hygiene fundamentals. Another significant challenge is overcoming regulatory control oversight vs. risk alignment, this will continue to be a challenge as our regulators evaluate our program against a control and threat landscape as opposed to basing it on our risks."

FOCUSING ON SECURITY PROGRAM AREAS

Brockway notes the program area that takes up the most amount of his team's time is information security administration. These fundamental tasks include day-to-day, week-to-week, or month-to-month activities around ensuring controls are operating in place and operating as expected. He says these are the 'bread and butter' of his program, yet take an exceptional amount of time.

From a culture perspective, getting traction and projects going in the right direction also takes a great deal of time, as he explains, "We particularly are a culture of collaboration, which is a good thing and you typically end up with polished and strong results. But the process of collaboration, maximum buy-in, and consensus takes a lot of time to get the right pieces in place. It's about all the right people moving in the right direction, sharing the same objective, and sometimes finalizing projects takes a lot of effort and time."

One of the more streamlined tasks with minimal time impact on Brockway's program is threat intelligence. He says, "Threat intelligence comes relatively easy and quickly into us, given we subscribe to multiple, different threat feeds, and different information sharing forums. We usually just get a lot of information from an emerging threat and a threat perspective, and we tend to be highly vigilant around emerging threats that we may need to take some type of action against."

COMMUNICATING AND REPORTING ON RISK

To judge how well Brockway's security program performs, he relies on identifying risk thresholds. He does this by starting with strong controls and identifying the appropriate thresholds of risk acceptance in order to report if the program is effective and operating properly. He subscribes to the CIS Critical 20 for control structure because they are prioritized, prescriptive, and a 'paint by number' approach, as well as mandatory controls from NY Department of Finances and the FDIC. If something bubbles up above the threshold, he then reports to senior leadership or the board.

He takes an educational approach with senior leadership, coupled with meaningful data. He encourages CISOs to find ways to take extremely complex security controls and processes, and turn them into a simple and digestible format. He pinpoints this as a key skill for CISO success and constantly challenges himself to improve and fine tune his approach.

During board discussions, Brockway will be simplifying his approach by correlating information security risk, controls, and program effectiveness into financial numbers his organization is accustomed to seeing. He explains, "This is a financial institution, so it's important to align the information security presentation and reporting to something that might look like another department reporting. So, massaging the information security report to something that can be presented in that same way, but conveys all the important things of the information security program, is certainly a big challenge for CISOs. You want to align with what your board might be accustomed to, to the best of your ability. That's a challenge. I can present this in a very technical way and we all know that's probably not the best way for people to digest it from a board and a senior leadership level."