PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT INFORMATION SECURITY PROGRAMS

ANTHONY SIRAVO
CISO, LIFESPAN

HEADQUARTERS: Providence, RI

EMPLOYEES: 23,000+

ASSET SIZE: $1.9 Billion

Anthony Siravo is the Chief Information Security Officer at Lifespan, Rhode Island's first health system founded in 1994 by Rhode Island Hospital and The Miriam Hospital. Working at a healthcare organization enables Siravo to feel a sense of community contribution. He said, "My contribution is being on the front lines protecting our patients' data, and ensuring the security of their private information."

Prior to Lifespan, Siravo held a CISO role at a large technology organization with 140 global locations. Siravo said, "I chaired the Information Security Governance Committee and was a principal member of the Product Security Council. I oversaw the successful $3.5B acquisition and subsequent secure integration of Motorola Solutions' enterprise business."

While chairing his previous organization's Information Security Governance Committee, Siravo had exposure to the executive board and key stakeholders in the company. "I worked with key business unit partners to implement practices that meet defined policies and standards for information security. I also served as the process owner for all activities related to the confidentiality, integrity, and availability of customers, business partners, employees and business information, in compliance with their information security policies."

AN MBA TAKES SECURITY TO THE BOARDROOM

Siravo's extensive experience with business leaders in past roles inspired him to seek his MBA. Although he possessed an expert technical mind, he needed to improve his ability to translate security to the business community. He recognized that executives who held the purse strings, such as CEOs and CFOs, only cared about technical requirements to a certain extent. To achieve the funding he required to run a successful security program, Siravo knew it was essential he understood how to speak the language of business.

Siravo said, "There are only so many security threats you can throw at an executive and effectively convince them of the importance without tying it back to financial risks. It didn't really matter that I thought a risk was not acceptable if I could not understand what the business thinks is unacceptable. My MBA provided the knowledge necessary to dive deeply into finance, budgeting and business presentations."

Siravo believes the most important thing he learned in business school was the value of being prepared to address questions from business leaders immediately, and with an answer they

can understand. "We learned how to present to the Board. I call it 'Boardroom Mode'. You need to speak slowly, avoid fillers, and repeat your message in laymen's terms. You also have to dress the part. Lots of executives pre-determine who you are based on how you are dressed. Technical people do not always realize that how you dress matters. When I first started presenting, I wore business casual. When I switched to suits, all of a sudden they wanted to hear more from me. This is called mirroring. If you make them comfortable by dressing the part you will have better results."

Siravo attended the MBA program at Bryant University, where they also emphasized the importance of working in a team. "The program used the Meyers Briggs test to methodically create teams of diverse personalities. We had to learn to work together. Every team member hated it at first, but by the end we were all best friends. It showed that you can work with anyone if you put in the effort."

MATURE SECURITY STRATEGIES IN THE HEALTHCARE INDUSTRY

At Lifespan, Siravo came into the position after a number of shorter term predecessors, creating a challenge to piece together a somewhat disjointed information security program. He said, "While I wasn't starting the security program, I have had to act as if I was. We were nearly starting from scratch."

Another challenge Siravo faced was understanding the appropriate methods to increase budget and resources. To overcome this challenge, he put his MBA-acquired skills to use through strategic communication. He commented, "I spoke in business language while I presented and educated the Board and business leaders. I put together real business cases, not PowerPoints that do little more than point out threats and risks. I have an open-door, education-focused policy."

Through discussing risk as it relates to business goals and metrics, Siravo further aligned information security with the organization as a whole. He emphasized, "Security is not the only risk to an organization, so you really have to build your case to get the budget you need."

According to Siravo, "Lifespan's mission is to "Deliver Health with Care" and we accomplish this by prioritizing the 4P's. The 4P's are Patients, Providers, People, and Purpose, with sub goals to increase quality and safety in order to provide patients a better experience. Our security effort aligns with these corporate goals by ensuring compliance with regulatory requirements such as HIPAA, CMS, and TJC and securing the technology and patient data that help deliver health with care. My organization seeks to protect Lifespan's network, information assets, intellectual property, and PHI from internal and external cyber and information security threats."

Siravo lists education, training and awareness as one of several strategic security goals for Lifespan. Ensuring the entire workforce understands cyber threats, improves the organization's ability to protect the patients and people, and deliver on their purpose. To achieve this level of awareness, Siravo's team focuses on educating users about ransomware and phishing scams. "I launched a phishing campaign at Lifespan that notifies a user when they have been successfully phished. More than half of our executives failed our first phishing test. They were mad! Now they are our biggest reporters of phishing. They took the exercise very seriously and we have dramatically improved as a result."

His efforts are paying off as the organization continues to move to a more formalized security process. He said, "Exception approvals used to be verbal, we now have a written system. New risks are managed in our enterprise risk register (in conjunction with Corporate Audit), providing proper evaluation, and are addressed by Lifespan executives. There was no risk register when I came in."

In addition to users and executives, Siravo holds business partners more accountable for information security. He established his own security analysis program for third parties and partners, and keeps tight control over security policy adherence. He said, "The SRA (Security Risk Assessment) is a process that all new vendors must go through if they access, store, or transmit personal health information, personally identifiable information or payment card information and business confidential data. We based our SRA on the NIST framework. The questions in the assessment align with generally accepted practices for a comprehensive security program. Once we have the answers, my team presents the results of the SRA to the legal, purchasing and the business sponsor for consideration."

Another important strategic role for Siravo is his position as security consultant during intra-hospital or business partner organizational activities. He commented, "When new business partners inquire about our security capabilities, my office will, upon request, provide descriptions of our capabilities and our operational security execution." By being a vocal and willing contributor to all conversations about security process, Siravo makes it easier for the business to collaborate and engage with partners, and important business objective for the company, and an obvious example of Siravo putting his MBA to good use.