PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DR. DAVID REIS

INTERIM CIO & CISO, LAHEY HEALTH

HEADQUARTERS: Burlington, MA

EMPLOYEES: 15,000

ANNUAL REVENUE: $2 Billion

APPLYING AN INNOVATION FRAMEWORK TO INFORMATION SECURITY

"Trends in the security industry change so frequently we need strategies that help us deal with the near term while also preparing for the future," says Dr. David Reis, CISO at Lahey Health. "We have to get a step ahead. There are specific frameworks to use to get through that process. The Kellogg [Northwestern School of Business] Innovation Framework resonates really well with me. It helps you develop an innovation engine for reacting to today and preparing for the future."

Many CISOs regularly leverage frameworks and controls such as NIST and the Top 20 Critical Security Controls, however there is a lack of CISOs who implement specific business approaches. Dr. Reis fundamentally aligns with the Kellogg Innovation Framework to cohesively run Lahey's security program. Dr. Reis explains how maintaining an eye to innovation helps enable a strong competitive advantage and makes a lasting impact on organizational revenue.

"The Innovation Framework is qualitative and mathematical in that it can help you track your progress towards creating a security program that brings value to the organization. Through this approach we look at what is going on today, and what happened in history. We review how breaches occurred industry-wide. What has changed over time and what has caused that shift? This allows us to identify future indicators and prepare for them in advance. In security, it is counterproductive to look out more than a year but we can be ahead of this week's malware."

The security program at Lahey facilitates business programs by moving past "blocking and tackling". Dr. Reis accomplished this enablement by demonstrating how information security can drive innovation and evolve to become a high-functioning service. An example of this is the robust role of security in connected health, described as "telemedicine" with patients and other providers, where doctors and patients can interact outside of health care facilities.

Lahey demonstrates a cutting edge technology, delivering healthcare outside of the four walls of treatment rooms and in an easily accessible and secure way, as a direct result

of the information security program. Dr. Reis says, "We are giving patients access to providers who they would not otherwise be able to access. For example, someone may be in the hospital with a chronic illness, and that person would typically have to come back to the hospital for on-going visits. This might be the appropriate treatment plan for some patients, but others would benefit from telemedicine. Our security team is driving the effort to extend the patient portal and video conferencing technology to connect patients to providers for follow-up after discharge without having to come back for an in-office visit. This is novel for healthcare."

Dr. Reis understands the significant role information security plays in an organization and acknowledges a potential for impact on revenue. While he stops short of saying the program is a revenue generator, he does believe security enables revenue. He comments, "I can show you how we have enabled millions of dollars a year in new revenue because we have securely opened up our services and access to populations that we could not reach before."

Dr. Reis also recognizes that revenue impact is strengthened by support from Lahey's business leaders, including the CEO, CFO and Board. Dr. Reis says, "The organization has given IT security a lot of resources and we are able to show our value. It can be hard to show ROI in security, so I focus on value. Kellogg teaches that value is equal to service plus quality divided by cost. At Lahey, our team is relentlessly focused on proving value."

THREE COMPONENTS TO EXTEND SECURITY'S IMPACT

To establish the security practice as a business enabler within Lahey, Dr. Reis focuses on communicating without security jargon, acting as a trusted advisor, and resisting temptations to advocate through Fear, Uncertainty and Doubt (FUD).

• Communication – Dr. Reis believes effective communication is integral to developing a satisfactory relationship with the Board and senior organization leaders. He learned the language of business when he got his MBA, and now easily translates security requirements and needs into financial and business conversations. "You have to speak the same language as the executives," he says.

Communication skills were fundamental in the early 2000s when Dr. Reis got his start in information security. He learned this lesson at a large, regional audit accounting firm where he performed internal and external audits. He says, "That is where I learned how to eliminate security jargon from my presentations because you could not get past the audit partners with security jargon in your report. That became a Rosetta Stone for me. I already knew about security, now I had a new language to communicate it to executives."

• Never Say No – "Executives have their trusted advisors, the people on the team they go to in order to get things done, and you have to do the work to join that circle. "My motto is never say no. Instead we say 'yes, and here is how'." By saying yes when executives or others in the organization want to implement a new tool, or introduce a new process, Dr. Reis engenders collaboration and positions security as a business enabler. To do so he must understand the team's business goals and objectives. Then the necessary controls may be put in place to make the process work in a secure manner.

• Never Promote Fear, Uncertainty and Doubt – Dr. Reis advocates for security by talking about pragmatic approaches and security's impact on positive business outcomes. He focuses on risk management and incidents in the company, and the industry, that can impact revenue. Sometimes, the Board will ask questions related to incidents in the industry, but Dr. Reis works hard to steer the conversation away from FUD. "What you present is as important as the fact that you are in the Boardroom presenting in the first place. You have to establish credibility as a business thinker. This is developed overtime. We can now anticipate the questions our Board will have and proactively address them. This allows us to lead the conversation and helps establish confidence in our program."

The First 100 Days

Dr. Reis has advice for new CISOs and says, "Gartner has a great CISO Framework for the first 100 days. The most important thing is to engage the leadership population and to understand at a general level what is working and what is not within the business. Ask, "What can I influence?" You can gain credibility by delivering on things that address specific pain points, even if they are tangential to security." Dr. Reis suggests that by establishing yourself as a business partner who can get things done you gain flexibility and leeway to implement vital programs.