PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

DAVID LOEWY

CISO, SUNY DOWNSTATE MEDICAL CENTER

HEADQUARTERS: Brooklyn, NY

EMPLOYEES: 8000+

NET POSITION: $2.9 BILLION

In the early 2000s, David Loewy began working on HIPAA projects, his start in getting involved with information security. He says, "Back then, the government put out in the congressional record, this is what you have to do to comply with the laws of HIPAA. And it used to be very much that you had to click off policies and you had to show how the policies were implemented and that you were compliant. Since the early or late nineties, HIPAA has evolved into a risk-based compliance program, if you will. And the natural evolution of HIPAA and the security piece of the risk-based part of assessments is how I evolved into security."

In 2015, after working as a HIPAA risk assessment consultant for State University of New York, Downstate Medical Center, they decided to hire him as their full-time CISO. SUNY Downstate Medical Center includes multiple graduate colleges in healthcare, a hospital and a large-scale research facility. Loewy was tasked with stabilizing and developing the information security program, starting with conducting outside assessments, remediating holes, then addressing policies and procedures.

One key challenge early on was ensuring all initiatives were applied to all units under the university's umbrella. Loewy explains, "We have the university and the teaching component, we have the medical and the hospital component, and we have the research component with the administration sitting over the top. And we must make all of our policies work for each one of those segments. Procedures are different. To enforce a policy may be a very different procedure for the hospital than it is for the medical school, but the policy must be able to meld across the entire institution. And that's what we started working on."

STRENGTHENING COMMUNICATION AND RELATIONSHIPS

Loewy believes his long-standing success at SUNY Downstate Medical Center is attributed in part to his relationships with C-level executives and his team. When discussing the importance of strong communication and relationships with his team, Loewy states, "When I hire people, one of the things I tell them their job is, is to make me look like a hero. And my job is to give them the tools and the support they need to do that. If you can pull that together, everything suddenly becomes copacetic. And I'm not going to tell you it's easy, because it keeps me awake at night. But you must rely on them. You have to build that relationship. And that makes my job a hundred percent easier when I'm not worried at night, whether a specific individual is going to do what needs to be done."

Armed with a strong sales background, Loewy believes sales skills significantly impact who he is as a leader and communicator. He says being a sales person means being quiet and listening, because that's when you learn vital information from someone. He also strongly encourages making time to care about your team and business counterparts.

THE IMPORTANCE OF SECURITY AWARENESS

"There's a lot of really good technology that is available in the marketplace, but 70 percent has nothing to do with gizmos, it has to do with people being aware of what the bad guys look like and how they're trying to break into our environments. 90 percent of cybersecurity tools are promulgated through email," says Loewy. As an industry, Loewy explains how most organizations are finding email as the number one tool people use in their organization. And through email, adversaries are getting into networks by clicking links or providing information like passwords.

He continues, "In the United States, I believe 30 percent of the people who get emails, will click on an email not knowing where it's coming from. Some 20 percent will click on links they don't have a clue where they're coming from. 8 to 10 percent of the people in this country will give out personal information, passwords, or login credentials, without having a clue where it is going. We have been able to drive Downstate down to less than 1 percent of our people will give that out. And that's a risk we're willing to assume, and less than 3 percent of the folks will click on links."

Loewy's resilience with security awareness campaigns means his network remains safe from most ransomware and viruses. For his role as CISO, it is his job and his team's job to make sure the organization is safe from adversaries getting in, because people's lives depend on their network not being penetrated.

ADDRESSING GOALS AND CHALLENGES

As a state-run organization, Loewy's goals are to remain transparent and keep the organization out of the press, maintain financial viability, and ensure they leverage the latest technology to achieve these goals.

One of Loewy's top challenges is secure communication between 'bring your own device' due to many of their medical residents moving between up to six or seven different hospitals. Loewy explains, "The face of healthcare in New York is changing probably faster than some of us want to think. We need to hammer that down. We need to figure that out."

Loewy believes healthcare is five years behind banking when it comes to securing innovation. He notes the ability to deposit checks through cellphones as an advancement in respect to how security can leverage new technology. He would like to see healthcare mirror these types of technological capabilities, and says, "Five years ago, they would have told me I was crazy if I suggested that's where we were going in banking. And in healthcare, we need to be able to ramp up the way the banking industry has and utilize all the marvelous tools we have and that are coming out of research and keep them secure."

He continues, "And that is a problem with the Internet of Things and with all the new medical devices. When somebody's had an epileptic seizure, they previously would shave spots on the head and put on probes so they could get readings on what the brain was doing. It took a long time to do that and sometimes the seizure would end before that was done. They've now developed a watch cap you just pull over your head and they can instantaneously start reading what the brain's doing. This all goes out over an internet and it's captured on a computer."

However, Loewy believes there is still a large risk with some advancements in technology, from a security perspective. He explains, "The benefits are greater than the risk usually, but there's a large risk in that side of healthcare and there's a large risk with the Internet of things. One year ago, we were moving out of one of our main offices, and some folks put copy machines out in the hallways and didn't realize that every copy ever made was captured on a hard drive. It was sitting right out there in the hallway and it's those kinds of things that we just are not cognizant of. And that's going to be the next big black hole that we're going to have to struggle with and get our arms around."