PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

PABLO MOLINA

CISO, Drexel University

HEADQUARTERS: Philadelphia, Pennsylvania

EMPLOYEES: 9,800+

ENDOWMENT: $779 Million

MOVING FROM CIO TO CISO

During his time as a seasoned CIO, Pablo Molina attained his security and privacy certifications, created security policies for many organizations he worked for, and eventually realized he wanted to instead work as a CISO. Currently the inaugural CISO for Drexel University, Molina initially sought out to ingrain the idea of how information security shows strong business value to the institution's community. Doing so required Molina to speak in both business and technical language. He explains, "I'm talking about business and technical language and I'm very fluent in both. I'm an expert in higher education administration and have a doctoral degree in this topic. I've worked for many institutions, so I understand the business of research and teaching and everything I do. Whenever I bring up the issues of risk management or incidents or policies or initiatives, I do so by translating that into the business value and the risk management for the organization. Because we speak the same language, I think that I'm a very effective communicator."

LEVERAGING BUSINESS KNOWLEDGE FOR BOARD INTERACTIONS

Molina works closely with all senior executives, from the President to the Chief Information Officer, along with meeting with the Audit Committee of the Board and other Board Members. He says he is often requested to meet with these individuals because of the strong interest in managing risk for the institution.

He relies on communicating in the language the board understands by being well prepared to anticipate questions they may ask. He does not overwhelm them with technical terms or with reams of information. He shies away from 'scare tactics' and instead leverages his business knowledge to correlate security to things most important to the running of the institution.

Molina comments, "I think that we have very talented board members. They're very smart people. I like to provide written information. I like to provide some concrete metrics. For example, financial information is critical both for risk management, for savings, and for contributions to the bottom line of the business. I also like graphical presentations because when presented with information, humans oftentimes prefer this type of presentation. I do not overwhelm my audience with scores and scores of numbers."

MAKING SMART TECHNOLOGY INVESTMENTS

Making smart, purposeful investments in technologies are key for Molina's program. He explains, "Our advanced next generation firewalls are helping us protect the community, combined

"WHENEVER I BRING UP THE ISSUES OF RISK MANAGEMENT OR INCIDENTS OR POLICIES OR INITIATIVES, I DO SO BY TRANSLATING THAT INTO THE BUSINESS VALUE AND THE RISK MANAGEMENT FOR THE ORGANIZATION. BECAUSE WE SPEAK THE SAME LANGUAGE, I THINK THAT I'M A VERY EFFECTIVE COMMUNICATOR."

with our ability to respond to incidents, by using security information and automation technology. Also, security training and awareness tools for our thousands of faculty, staff and students are important to impact the culture of the institution."

To reduce complexity and ensure the technology investments continually meet needs from a security perspective, Molina has instituted a vendor assessment program. This program ensures they select vendors that are secure, have both security and privacy by design, and follow responsible computing principles. He says, "Everything becomes much simpler because it is not that you bought a product or a service and now you have to figure out how to make it secure; it is by definition that the company was thinking of making the product or service secure. Sometimes it requires making what may initially look like more expensive purchasing decisions, but in the end you realize that the total cost of ownership and the total risk profile are much more beneficial to your organizations."

Furthermore, Molina believes many CISOs have invested in security products and services yet are not taking advantage of the full business value they offer. He says you must maximize their use and master your own knowledge in order to get the most out of those products for your organization. He comments, "You have to be strategic about it. In my case, I have limited resources, and because they're limited, I may pay attention to new and interesting technologies, but in the end, I concentrate my efforts into doing business with a handful of vendors. And for those, I know the executives, I know their roadmaps, I know the application cases, I know the adoption patterns within the organization. That's the way I do it."

Molina encourages CISOs to work through their vendor and reseller channels to convey to them that they are strategic partners and attend their executive briefings whenever available. He also suggests for any vendors who host annual conference, to make it a priority to attend them.

FOCUSING ON FRAMEWORKS AND ASSESSMENTS

Drexel University is a complex institution with many divisions and units that are regulated differently, creating a unique challenge for Molina. He explains, "We do align to some different frameworks. For example, we have to be HIPAA compliant and for that we use specific frameworks. We have to be compliant with the Department of Defense Regulations for Contractors, so we need to follow those specific frameworks. We also consider the maturity index by organizations like Gartner. And then finally, because we are a higher education institution, we use many of the models and metrics for our specific vertical."

Molina conducts annual assessments, either internally or externally depending on what they are specifically evaluating. In some instances, he may conduct certain assessments every four years with an external partner, yet he prefers to conduct other assessments internally. He comments, "Internal is cheaper because you are re-purposing the resources that you already have in house. Internally is much easier because you reduce the friction of having to receive requests from the consultants, translate those and then securing those, the process is much more streamlined. The problem when you are internal is that on the one hand you may not have an objective point of view, as you are involved with day to day operations. And also, it could be the case that at the end of your assessment, you lacked the credibility that an outside party would have."

TRAINING AND RETAINING TALENT

Molina strongly believes in offering training and certification opportunities to his team and solidifies budget to accomplish this each year. He says, "I've always faced an interesting question from budget committees and board of directors, when I ask for a training budget, they have the argument that well, you train new people and then they leave. And my counter argument has always been: training people and having them leave is better than not training people and having them stay because they are not qualified to continue doing their jobs."

Molina sends his team to vendors conferences, large-scale conferences such as Black Hat, and specific training for sophisticated technologies like computer forensics. He also encourages minorities and women to enter into the cybersecurity field. He makes it a point to recruit both women and minorities. He is an active supporter of the Philadelphia Women in Cybersecurity group and helped create a Women in IT group on Drexel's campus. He is also one of the early members and board members for the Hispanic information Technology Executive Council, helping their mandate of finding a more diverse pipeline of talent.