PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JAKE MARGOLIS

CISO, METROPOLITAN WATER DISTRICT OF SOUTHERN CALIFORNIA

HEADQUARTERS: Los Angeles, CA

EMPLOYEES: 1,400+

ANNUAL REVENUE: Undisclosed

SIZE OF SECURITY TEAM: Undisclosed

"I think there's different levels of education because people need to understand what risk there is to them based on their role, what responsibilities they have in leadership for roles and responsibilities within a holistic security program."

- JAKE MARGOLIS

Early in his career, Jake Margolis served as an Officer in the United States Army Forward, deployed to Afghanistan as the Combined Joint Signal Officer, a role some would equate to that of a CIO. When he returned to the United States, he was asked to become the Information Assurance Manager for the California National Guard and California Military Department, a role comparable to that of the CISO. He was chosen for this assignment because he had the correct Department of Defense (DoD) certifications and security was the responsibility of all people working in IT within the U.S. Army. Shortly after stepping into this role, his first major responsibility was to prepare for, and pass, the U.S. Cyber Command, Command Cyber Readiness Inspection. He says, "That was really how I got into information security as a discipline, if you will, because they put me in there. And that was just an assignment for me as an Army Officer. I didn't set out on a career path to become a CISO one day, or even a pen tester or anything like that. I just bounced around the IT profession, largely within the DoD. And because of the level of rigor put on things in the DoD, I had this level of exposure to security."

He continues, "When I came up doing this in the military, the security guys didn't harden servers for you. We were responsible to meet standards that were published by the security team. So, I've been doing security probably my whole career. I had my CISSP before I was officially in security. I was a network operation center manager and the DoD required me to have my CISSP to perform that job, so security was just part of it. For me, the journey has always been different, because when I talk to other people that haven't had that upbringing in security, their experiences are very different with it," explains Margolis.

After working in a number of roles for the Army, California National Guard, and serving as the CISO for the County of Orange, Margolis is now CISO for the Metropolitan Water District of Southern California.

STRONG SECURITY AWARENESS

Margolis believes security awareness is vital to a strong security culture within an organization. He says this starts with embarking on holistic and multi-layered security education, and a strong security awareness program should encourage people to consistently think about being secure, both inside and outside of the workplace.

For example, he says it is important to educate your workforce about small adjustments to their everyday routines such as taking off their badge when they go to Starbucks. To fundamentally instill a security-aware mindset for employees, he suggests publishing threat intelligence summaries around the holidays to tell parents what IoT enabled toys are less secure or educating about parental controls that may be complimentary from your internet provider.

Margolis approaches security awareness with business executives in a more specific manner, one that resonates directly with their responsibilities, goals, and challenges. He comments, "I think there's different levels of education because people need to understand what risk there is to them based on their role, what responsibilities they have in leadership for roles and responsibilities within a holistic security program."

BEST PRACTICES TO CREDIBLE RISKS

Margolis emphasizes the importance of avoiding fear, uncertainty, and doubt when presenting to executives or the board. His advice is to avoid this because scaring people only gets you money one time and runs the potential of your board or executives losing confidence in your abilities as a strategic leader. He says you must educate them on what is considered best practices to credible risks.

He explains, "Make it about risk-based decisions. They're not good decisions, they're not bad decisions, they are decisions that are centered around managing risk to the organization financially and operationally. Because you want to make sure they understand that you understand there is a dollar amount associated with whatever it is you're trying to deal with. Also, there is an operational risk that would then lead into reputational damage and things like that if you fail to produce your product or keep your servers up and running."

BATTLEFIELD MANAGEMENT AND TECHNOLOGY ROADMAPS

To address the clutter of security products, both those already in an organization's environment, and the myriad of options when looking to invest, Margolis believes in a strong strategy of what technologies you are trying to manage and basing your program on a few core pillars. He says one pillar should be leveraging cyber threat intelligence to understand and respond to threats. He views cybersecurity and investing in technology as a paramilitary science in a sense that he is doing battlefield management.

He says, "Cybersecurity is not hierarchical like police or fire, which is commonly associated with paramilitary. But I consider cyber to be paramilitary because you must apply a certain amount of military science to do battlefield management. You must understand who the bad guy is, what their techniques are, how they're going to approach you, and how you're going to defend against them. And then when they do launch their attack, how is that attack managed and how do you respond. Understanding all of that allows me to understand what technologies I need."

Margolis suggests leveraging strategic documentation such as ISO 27001 and 2, NIST 853, the MITRE Attack Framework, and CIS Controls. He explains, "The technologies and capabilities we have are arrayed against an ability to manage part of the cyber-attack kill chain. And the better I can leverage technology to do that, the more easily I'm going to see gaps, because if I start seeing that one technology is doing too many things in that management, then I start recognizing single points of failure. And then I realize I need augmenting technology. So that helps me develop a technology roadmap."

TOP CHALLENGE

"I would say the one of the top challenges for me in the public sector is job classification issues and getting the right people hired into jobs. And this would resonate with the federal government and state government. In the public sector we must deal with job classification constraints. Say I have a job opening and I want to hire somebody to be a SOC analyst. That's a common job these days, but I look at the skillsets for a SOC analyst and I look at my current job classifications. I must try to figure out how I'm going to pigeonhole that into an existing classification. So, some skills that I want, I may not be able to get. That's one thing. I think that's a challenge for a lot of public sector folks. There are ways around it, but it's a challenge."