PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

KEVIN PAIGE
CISO, FLEXPORT

HEADQUARTERS: San Francisco, CA

EMPLOYEES: 1,600+

ANNUAL REVENUE: $471 Million+

SIZE OF SECURITY TEAM: Undisclosed

At the beginning of Kevin Paige's career in the Air Force, he focused on law enforcement and physical security. He had the opportunity to work with some investigations related to computers, and then was given the opportunity to move into computer operations. During this transition he realized he had a deep passion for technology. While working in technology in those early days, many people correlated his early security work with computer security work, so before he knew it, he was assigned to the network security team. This was Paige's first experience with information security and sparked his passion and desire to follow this path as he progressed in his career.

After leaving the Air Force, he then moved on to government consulting, working on building security capabilities, and later transitioned into a network and systems operations security architect for the Navy and Army. He then became a civil service employee, running data centers and created one of the first cloud-based infrastructure-as-a-service offerings for the federal government.

"Flexport takes a security-first approach on IT and data security. And instead of hiring a CIO, they wanted to hire a CISO with a security-first mindset to make sure that we're making all of our decisions with risk and security in mind, to make sure that we're protecting our data and goods, and protecting our people in a forward thinking manner."

With a desire to leave the public sector, Paige moved on to work at a small disaster recovery startup before joining Salesforce. During his time at Salesforce, Paige helped establish their infrastructure security capability. Paige eventually left Salesforce and worked at MuleSoft as their first CISO, building out security holistically from the ground up for the company, before his current role as CISO for Flexport.

As CISO at Flexport, Paige oversees the entire security function as the organization focuses on their mission of moving freight globally by air, ocean, rail, and truck for the world's leading brands. He comments, "I own IT, physical security, and logical security. Flexport takes a security-first approach on IT and data security. And instead of hiring a CIO, they wanted to hire a CISO with a security-first mindset to make sure that we're making all of our decisions with risk and security in mind, to make sure that we're protecting our data and goods, and protecting our people in a forward thinking manner."

BUILDING A SOLID SECURITY FOUNDATION

In order to build a solid security foundation, Paige emphasizes

the importance of a risk-based approach, strong security culture, motivated team, and robust identity and access management program.

Risk-based Approach. Paige focuses on risk and building a maturity model based on where he is today, and what the path looks like to increase maturity, especially around data security and data protection. By taking this approach he understands where gaps exist, areas of strength, ways to become stronger, and how to prioritize resources, while also tying everything to compliance.

Security Culture. Paige believes in a cohesive approach to security awareness, that makes protecting the organization interesting to all employees. He says, "Making security awareness interesting is very important to me because the security team is always going to be small compared to the company's relative size. We need eyes and ears all around the company that know how to ask the right questions and know who the people are that they need to ask those questions to. Establishing the security culture was my top priority. But it's always a continuous process."

Motivated Team. Paige says hiring team players is consistently one of his top priorities. He explains, "Hiring is hard, there's no doubt, but from my perspective, I like to operate as a team, not as individuals. Depending on each other, communicating with each other, and making it about more than just the technology. Every company in the world needs the same type of security people, but are you treating them like people, are you giving them the career advancements they need? Are you giving them the education? Do they feel like they're part of a team or do they feel like they're just showing up to work nine to five to run their security tools?"

Identity and Access Management. Paige says, "Security begins with strong identity and access management capabilities. Across the company, I took a strong look at making sure that we've got great identity when it comes to accessing IT systems, when it comes to accessing our product capabilities, and when it comes to accessing our infrastructure. Holistically, I wanted to look at how we were doing it, what our gaps were, and then make solid plans to make sure that we're doing the right things. Strong identity and access management capabilities are critical to having a solid security foundation."

MEASURING PROGRESS

"In the very beginning, the easiest thing to do when you're building programs from scratch is really a project management approach. I built a 12 to 18-month roadmap using the V2MOM approach - vision, values, method, obstacles, and measures. And then we hyper focus using Objectives and Key Results (OKRs) for each quarter, based on priority, risks and capabilities, and we measure those OKRs based on project capability to see where we're at and how we're doing," explains Paige.

He leverages this agile methodology to measure where his program is and how they are doing based on the project capability. This enables him to gain valuable visibility around the process in place, tracking the overall security health, and the maturity level over time to ensure they are improving.

Paige values the ability to continuously show progress while continuously improving. He explains, "We have to set good rules and capabilities that we're measuring ourselves against. In security, we must stay ahead of the curve. We must stay at least on par with our technology brethren as they're bringing in these new technologies such as new cloud type capabilities. We have to stay on top from a technology perspective and really understand the technology they want to bring in, why they want to bring the technologies in, what problems they're solving, so that we can really understand the risk and give them meaningful security responses in order to help them."

The Competitive Advantage of Trust

"A lot of the times I don't even use the word security anymore. When I'm talking to business partners, I use the word trust. It's all about trust, right? We want our customers to trust us. We want our employees to trust us. We want our business partners to trust us. Everything is all about trust. Especially if you're a cloud platform or you want somebody to use a new cloud platform or technology or capability. You've got to trust it, and how do you trust it? How do you create that trust? How do we evolve that trust? People are going to use what they trust. If you have a brand that's trusted, if you have capabilities that are trusted, if you have people that you work with who are trusted, that is the key. That is the competitive advantage, right? I worked at Salesforce, and for their CEO Mark Benioff, trust has always been one of his core company values. And I've seen firsthand how a company like Salesforce has built that level of trust with their customers and that's what keeps them coming back. That's what keeps them buying more. Customers see and feel the trust value in all aspects of how Salesforce operates and I believe that more companies will adopt this approach as the future of security because the old-fashioned ways we have been doing security in isolation for the last 20+ years are not effective, it's time to evolve with a trust first mindset."