PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

CHRISTOPHER PORTER
CISO, FANNIE MAE

HEADQUARTERS: Washington DC

EMPLOYEES: 7,200

ANNUAL REVENUE: $23 Billion

"The entire organization is passionate about improving the security program. When I started, I was really pleased with the support from the top to bottom."

- CHRISTOPHER PORTER

In the late 1990s, Christopher Porter visited a friend working in IT at Cisco in Silicon Valley where he had the opportunity to witness innovative IT work first-hand. This experience sparked his interest in the IT field and he went on to work at a law firm specializing in a wide range of technical support. He then took a position at the LSU Health Sciences Center in the early 2000s where a malware incident, SQL Slammer, prompted the organization to place an entire network behind firewalls in a period of a few days. It was through this incident that Porter developed a passion for information security.

Porter continued his career working at an information security consulting firm, where he traveled throughout the U.S. working with clients to provide them baselines of security and help build programs from the ground up. He then landed a formidable, yet rewarding role, working on the Verizon Data Breach Investigations Report (DBIR) for over seven years. Porter comments, "My work on the DBIR opened my eyes to a lot of different issues in this industry. I saw there was a clear lack of data across the industry when it came to security incidents. I was reading thousands of incident reports about how data breaches were happening and it was my job to break them down and analyze what happened."

TRANSITIONING INTO CISO

Porter decided to move over to operations and work in a role to protect an actual organization. Before becoming CISO of Fannie Mae, the leading source of financing for mortgage lenders, his first role was that of their Deputy CISO. He says, "What I really like about Fannie Mae are the people and the mission of the organization. Those are intertwined with one another. One aspect of the mission is that we are ultimately putting people in houses. When we create liquidity in the market, we make it possible for people to buy homes."

GROWING AND LEARNING

Porter emphasizes the value of having mentors throughout your career, something he has had the opportunity of experiencing. He says, "I have several mentors I talk to regularly, some I've worked with directly as my bosses in the past. It's a way I can continuously improve. My mentors' expertise and insight are invaluable to helping my career."

He continues, "The entire organization is passionate about improving the security program. When I started, I was really pleased with the support from the top to bottom. It also coincided with a transformation in the overall strategy. Fannie Mae wanted to focus on delivering a strong customer experience, and part of that means always being available for our customers. Developing a strong cyber resiliency was, and still is, a huge component of that."

Mission and culture were key components of Porter's interview process and he recommends understanding these facets of a business by asking how a company generates profits and the level of support it provides for information security. Porter explains, "You must ask business-oriented questions to understand how the company makes money and what kind of data they are protecting. It is also really important to understand the culture and what kind of program you will be coming into."

GET RIGHT, GET SMALL, SEE BIG

Coming in as a Deputy CISO enabled Porter to establish a strong relationship with the previous CISO. Porter worked diligently alongside the CISO to define and create an information security strategy. He says, "Our mission was to get right, get small and see big. This meant to fix things in the environment that needed fixing, shrink the attack surface and get better insight into the business, technology and network so we can be more proactive. We then had to build the right team and get the right people in the organization to lead. We were in build mode at that time." After the prior CISO left, Porter took on his role and now carries on this mission of building a world-class information security program.

Porter describes culture and education as key components of a strong information security program. He comments, "Our CEO talks about cyber risk as a top concern in our town hall meetings. There's a clear message from the top down that security is important to the organization." This support includes board meetings where security dominates a large portion of the conversation. Porter says, "Our board has a packed agenda, but security is something they have a great interest in covering. They always want to understand more about what we are doing."

Porter works hard to be direct and transparent with his senior leadership. He explains, "They want to understand the risk to the organization. Often, there will be one or two technologists on the board who are good allies. If you keep it simple and provide strong metaphors to explain complex security issues, you will send a direct, clear message to them."

KEY POINTS FROM PORTER'S PHILOSOPHY

Porter believes CISOs should focus on innovation, collecting data and aligning to the business as they continue to positively mature in their roles.

Innovation. "Innovation is one of the most important aspects of their role that CISOs can engage in. We have to start doing things differently and start looking at our security problems in different ways. Some of that is leveraging more early stage venture-backed technologies. There is a lot of funding going into cyber security in order to solve problems and there are some really good partners we can work with."

Collecting data. "It is important to measure findings across the organization and the security program, and baseline that activity to really drive data-driven decision making. We can't make decisions based on gut, and it is easier to influence people across the organization when you have data as support. When you can show how something actually helped save money or prevent fraud, you gain more backing. If you know your audience well, you will know what kind of metrics to present to them. It's all about using your best judgement."

Aligning with the business. "It is important to understand what your business does so you know what to protect. I can't stress that enough. When I was at Verizon, each report had a table focusing on which threats impact which industries. If you know your organization, you can increase your understanding of the threat profile you are facing. If you understand your business and the threats that affect your business and industry, it will help guide the decisions you need to make so your program runs strategically."