SEAN KEARNEY

CISO
NATIXIS CIB AMERICAS

HEADQUARTERS: New York, New York

EMPLOYEES: 700+

REVENUE: $750 Million

Sean Kearney is a people-focused leader passionate about protecting organizations by leveraging a strategic, business-aligned approach. He began his career in cybersecurity recruitment, exposing him to the industry and sparking his interest in pursuing a more technically-focused career. He then moved to a business security consultant role, working on projects such as identity and access management, risk management and compliance. As he evolved his career, he worked in the financial services industry across many security functions, from security management to architecture, risk management and more. After moving from his home in the United Kingdom to New York, he took on an Information Security Manager role at Natixis and was made CISO after six months.

Natixis is a French multinational financial services firm specializing in asset & wealth management, corporate & investment banking, insurance, and payments. As CISO for the Americas, Kearney helps enable the organization to support corporations, investors, financial institutions, and institutional clients worldwide.

OWNING AND MANAGING THE CYBERSECURITY PROGRAM

Kearney provides oversight for the first line of defense at Natixis. He explains, “First-line of defense is the hands-on security engineers, networking, and IT teams. I lead the second line of defense security risk management team, which provides direction and oversight to all technology and security operations, ranging from patch and vulnerability management to antimalware coverage, from identity and access management to secure development practices. My team and I provide the oversight and monitoring of how effectively these areas, and the controls within them, are performed. My role in a nutshell is to make sure that information security, IT security and anything related to that space is performed appropriately. I do that by owning and managing the cybersecurity program which is made up of a number of different policies and risk management processes including a robust control framework to monitor and test all key technical controls.”

Kearney’s team assesses the effectiveness of the first line of defense by identifying risks and distinguishing plans for remediation. If there is a missing patch or a recent vulnerability, his team figures out how to address it, and if necessary, determines how to report it up the chain. They also help with

> *“We must align with where the risk appetite is for the firm, what are the objectives that they want to achieve, and really get behind them and try to reduce risk as much as possible.”*

framing new and existing security risks to ensure appropriate decisioning regarding budget allocation.

Security awareness also falls under Kearney, a program that involves phishing campaigns, training workshops, seminars, posters, leaflets, and any other pertinent channels.

He continues, "My team also owns data loss prevention across email, web, physical devices, and so on. As the CISO, regulatory compliance, as it pertains to information security, is a key part of my role. I work with our regulators to ensure continued compliance with local, national, and international laws and regulations. I also have consulting responsibilities where I'll sit with the business and IT when they have new projects and new initiatives. Obviously, we need to get security involved as soon as possible to ensure security is baked into the product, by consulting on how best to meet the policy objectives that we're enforcing."

INCREASING SECURITY AWARENESS AND REDUCING TECHNOLOGY RISK

Building out the security awareness program is a top goal for Kearney to solidify a mature security culture, something that requires a large amount of time and resources. Not only does it involve effort from the security team, but the ability to change attitudes and perceptions is not a quick win. He comments, "You can see significant improvements in your risk posture, in the threats that you're facing, your capability to deal with those threats if you've adequately trained your staff. I mean, you look at any of the major breaches in the last couple of months. I'd say at least 50% of them involved the human aspect. More specifically, if we look at the latest Verizon report, 85% of breaches involve the human element. That's why it's at the top of my list."

Another top goal is a heavy focus on technology risk by ensuring their technology keeps pace with the changing threat landscape. With upticks in ransomware, targeted phishing, and social engineering, their risk management processes must be capable of moving with these shifts.

Kearney says, "Then you have compliance too. With regulators right now, cybersecurity is a hot topic as is privacy. So, for both of these, we need to react to stay on top and to stay ahead of that. Keeping a finger on that pulse and making sure that we respond appropriately to the new and expanding regulations is key."

DELIVERING WHAT THE BUSINESS WANTS TO DELIVER

For Kearney, one of his guiding principles is never losing sight of business goals. He believes security is there to support the business. He explains, "At the end of the day we are there to deliver what the business wants to deliver. We must align with where the risk appetite is for the firm, what are the objectives that they want to achieve, and really get behind them and try to reduce risk as much as possible. Doing this while being conscious that sometimes that can be a detriment for delivering those business objectives."

Kearney says to not do security for the sake of it; focus on the business and align with organizational objectives. He also says not to minimize risk just for the sake of it, it could be expensive and unnecessary, you must work with senior management and establish a risk tolerance or risk appetite they are comfortable with and then build around that.

Policies are a strong starting point, because by understanding the business, you may build your support structure to support the business in as secure a way as possible. He comments, "The old adage of "security says no" is not something that we want to reinforce. We want to make sure that security is seen as supportive. For me, I start at the top - what are the business goals? And then build policies and the program underneath that. Aligning the program to what the organization needs to achieve and making sure those control statements within the policies are the way you want them to be. As you're doing that, really start building those relationships across teams. There's no point in writing policy statements that pertain to network security controls without having spoken to anyone in networks about feasibility."

DOING YOUR PART TO INCREASE THE TALENT POOL

"We all see challenges with hiring. Yes, the talent isn't always there, but what are we doing about it on a personal basis? Are we involved in reaching out to the communities? Are we helping pro bono? Are we doing things that can increase the talent pool and encouraging diversity into our industry?

There are so many different mindsets, backgrounds, and perspectives. As a recent parent myself, I know my outlook on a lot of things have changed dramatically. People of different parental status, career experience levels, ethnic backgrounds, genders, sexual preferences and orientations, have all sorts of different outlooks which present an opportunity to solve diverse challenges. For example, who could be better to develop an inclusive and relevant awareness program than a diverse team of people who represent the mindsets, viewpoints, and diversity of the broader organization?"