PROFILES IN CONFIDENCE

Highlighting information security leaders who are leading the way for confident security programs

DANIEL CONROY

CISO
Synchrony Financial

Company size: 11,000+
Headquarters: Stamford, CT
Revenue: $2.11 Billion

PRIORITIZING SECURITY AT SYNCHRONY FINANCIAL

Daniel Conroy, CISO at Synchrony Financial, is an engineer by education and brings an analytical and practical approach to all aspects of planning, delivering, and managing teams. His primary areas of focus are: intelligence collection, defending Synchrony Financial's network, effective communication, and providing the bank's clients with security assurance. According to Conroy, among the many institutions he has worked for, Synchrony Financial is the most focused and engaged in information security. He says, "The energy is different here. People are excited about the positive impact security can have on business, and use it as a true business enabler to provide a competitive advantage to Synchrony Financial."

Conroy states that Synchrony Financial's Board understands the value of security - including related threats, challenges, and opportunity. Information security is a priority for senior management. They ask informed and intelligent questions about the security strategy, which Conroy states is focused on enhancing and maintaining a proactive, agile, and adaptive security program that delivers a sustainable competitive advantage.

"We chose the name Synchrony for a reason – we are in sync with our clients and customers. That promotes a security culture as well." In addition to cyber intelligence and infrastructure defense, Conroy considers client engagement a key pillar of the security organization. "We share our security knowledge and cyber intelligence with our clients, who may not have the resources we have. By sharing information with them we are helping to protect the entire payment ecosystem, which not only improves our customer relationships but also better secures all aspects of our transactions." In addition, we engage with our customers to educate them on information protection techniques and regularly remind them to remain vigilant for incidents of fraud or identity theft.

Some of the information shared with clients

comes from the company's Cyber Intelligence group, which collects and analyzes threats by leveraging both internal and external resources. Action is key to this group's success. The group has prioritized threats and is continually evolving its knowledge of adversaries, who are improving their attack methods at lightning speed.

For Conroy, much of security comes down to what he can control, and identifying and accepting risks associated with what he cannot control. "When I stopped playing rugby, I started doing triathlons. I quickly learned that there are only so many things you can control. You can't control the waves, your competitors, or the weather. What you can control is your training and your state of mind. You can study your past performances and make changes to your approach to improve your position. You can prepare yourself to address certain unplanned elements – like a flat tire, by bringing a spare. The more you prepare and the manner in which you address the things you can control can make the difference in your performance. You have to be laser focused on maximizing performance and minimizing risks in the environment. It's the same for information security. A successful security team is one that exercises control where it can. They should be able to minimize the impact of the unexpected by making decisions based on research, intelligence, practice and training."

THE FUTURE OF SECURITY

"Information security used to be an afterthought to systems and processes. Today, security needs to be inherent in the DNA of all systems to work effectively. Some information security issues exist because of flaws in the solution architecture, which was created 25 or more years ago. Technology was not architected with today's business in mind, so many are looking to retrofit security. There will be these types of threats until we get to a point where everyone is working from a secure architecture and following the same standards. It is going to take time, but we will get there."

SHARING INFORMATION WITH COMPETITORS

"In the financial services industry, we actively share cyber threat information and attack vectors with partners and peer banks. The Financial Services Information Sharing and Analysis Center (FS-ISAC) plays a key role in it and is serving as the primary channel for receiving timely cyber security threats notifications. All financial services organizations need the Internet to be secure because we need consumers and businesses to feel safe about their private data. It is in the best interests of us all to share cyber threat information to maintain a safe and secure Internet experience for all businesses and consumers."