Life Sciences Cybersecurity Executive Roundtable Meeting Summary
February 10, 2020

Life sciences cybersecurity executives sat down for a conversation with research scientists from Cybersecurity at MIT Sloan (CAMS) at our virtual roundtable. Following introductions, participants engaged in a discussion surrounding security in a remote workforce and on moving to cloud applications. Following the hot topics discussion, CAMS Researcher Rebecca Spiewak shared research and led a discussion about securing healthcare data.

Hot Topics Session

The hot topics discussion revolved around the roadblocks of building a cybersecurity culture while the majority of the workforce is still operating remotely. One participant noted the difficulty of creating and managing a cybersecurity culture when he has never met a number of his newer employees and they are all working off mailed-in laptops. When companies are completely reliant on SaaS and IT infrastructure, coupled with remote management of devices, education becomes a big factor in security. Knowing who has what access is a starting point. One effort is to re-architect a network to put in segmented firewalls with multi-factor authentication throughout that environment. Discussions with VPN vendors bring up security concerns of their own. Another member expressed a need for a cloud-based firewall to conduct secure practices beyond physical devices. Having software hosted in the cloud means protecting and managing an internet connection, VLAN, and all that accompanies it. The question of how to push the life sciences industry in the direction of better practices without regulations deterring security persists. When asked what their top priorities were, participants said tackling the human element of cyber in terms of insider threats, backing up and storing data in the cloud, and establishing liability in vendor contracts.

CAMS Research Presentation: Securing Healthcare Data

Rebecca Spiewak, a CAMS Research Assistant, joined us to present her work on securing healthcare data and security controls for medical devices. The focus of this work is to create a technology roadmap for ways to secure healthcare data from internet-connected medical devices, and to suggest places to invest in security technologies for the future. There lacks an actionable, objective, and standard way to measure IoMT security effectiveness. Think of security controls as a vendor, so device security is the manufacture's responsibility. The threat landscape outlines the severity and frequency of threats in this area. This is dependent on criminal incentive and the risk to patient safety. These devices are getting hit with ransomware, DDoS, and other attacks. There is a lot of espionage where people want to steal blueprints for pharmaceutical solutions; there is a lot of incentive to steal information that would be expensive to develop on their own. Effective security controls often require tradeoffs; medical devices are built for safety over security. The FDA regulates and audits platforms that are fed clinical information from devices, creating a distinct conversation between the security control devices and where the information is stored. As for where the industry is going to invest and build in security over time, right now it learns more towards the security control vectors where there is a huge startup industry for medical device security. As regulations increase, companies will be incentivized to embed security within their products.

About Cybersecurity at MIT Sloan

Cybersecurity at MIT Sloan brings together thought leaders from industry, academia, and government with MIT faculty, researchers and students to address strategy, management, governance and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

For more information, visit https://cams.mit.edu