Life Sciences Cybersecurity Executive Roundtable
Managing the Cyber Risk of AI/ML
Meeting Summary
September 2, 2020

Life sciences cybersecurity executives sat down for a conversation with research scientists from Cybersecurity at MIT Sloan (CAMS) at our virtual fall roundtable. Following introductions, participants engaged in a discussion surrounding remote work and the cyber risks associated with it. Following the hot topics discussion, CAMS Research Affiliate George Wrenn, CAMS Research Assistant Sanjana Shukla, and CAMS Executive Director Keri Pearlson shared MIT research and led a discussion on the topic of Cybersecurity of AI Applications.

Hot Topics Session

The hot topics discussion revolved around the pressing cyber risks of remote work six months into a pandemic. The chaos from COVID-19 increases cyber risk in the work from home environment because of remote IT support, increased levels of financial fraud, and an unprecedented rapid march into digitalization. One participant asked what measures might need to be implemented differently than at the beginning of the COVID-19 pandemic. Wrenn responded that a crucial action item that enables remote workers to have better security is to ensure that employees are removed from as many decisions around security as possible. Tighten loose screws so the majority of the risk is in fewer, and more capable, hands.

Some organizations are equiped to handle digitalization more successfully than others; some companies have nearly perfected remote security while others have been struggling to update their employees' laptops remotely for the past six months. The tools change frequently and implementing a VDI (Virtual Desktop Infrastructure) can be more secure than a laptop, and clients for iPads and mobile device management are available. Providing devices for your employees makes managing remote cybersecurity easier, and many executives consider that to be well worth the budget. One CAMS member, preparing to roll out a COVID app for their employees, says they are a ways off from letting employees use their own devices. The reluctance comes from a combination of tightened security and a legal standpoint of being able to have full access to the device and wipe it if necessary.

CAMS Research Presentation: Managing the Cyber Risk of AI/ML

This research asked two questions: How can senior management control risk associated with AI? and What are the unique attack vectors associated with applications using AI? Systems that utilize AI/ML technologies have unique vulnerabilities compared to traditional systems. Learning algorithms, validation data, processes, inference algorithms, and feedback loops create systems that not only learn, but are designed to find unique, obscure patterns that may not be obvious or easily detected without the AI technology. Managing the cyber risk of these systems is unique: did the system find the 'needle in the haystack' or was this obscure finding a result of a compromised system? This research creates a new management strategy to mitigate cyber risks caused by the unique features of AI/ML. To learn more, access the CAMS research brief at: https://bit.ly/32PaWbg

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