Life Sciences Cybersecurity Executive Roundtable Meeting Summary
September 12, 2019

Life sciences cybersecurity executives sat down for a conversation with research scientists from Cybersecurity at MIT Sloan (CAMS) at our fall roundtable, generously hosted by Joe McGrath, Chris Ferrer, and Sage Therapeutics. After a reception and happy hour, participants discussed important challenges their teams encounter during the "burning issues" session. Following this hot topics discussion, CAMS director, Dr. Michael Siegel, shared MIT research and led a discussion about cybersecurity risk metrics.

Hot Topics

The first topic discussed was ***board member confidentiality***: How can we share information with the board and know it will remain secure? Participants voiced concerns, beginning with significant human risk. The level of risk depends the relationship the CEO has with board members: can the CEO ensure that board members will hold information confidential? Beyond leveraging the CEO's influence, participants mentioned several other effective control methods: security awareness and software/system digital restriction of sensitive documents. Document control faces pushback from members who object to online-only viewing (preferring to print out key documents, but are restricted to do so by the software). Awareness training can reduce pushback by educating the board about cybersecurity and privacy activities that everyone in the organization must follow.

The second topic of discussion was ***supply chain cybersecurity*:** How can we best evaluate the security of our vendors? Participants suggested that the first step to managing supply chain cybersecurity was to determine an acceptable level of risk from vendor interactions. To learn more about vendor cybersecurity practices, ask them for reports on their cybersecurity metrics and how they determine how secure they are. Those vendors willing to share these reports indicate an ethos even when reports suggest options for better security. Much like managing board members, a strong relationship with vendors can aid in their sharing the state of their security. A third practice is to set up processes to monitor vendors' activities; software can track activity and use/access of files within the organization and systems can flag unauthorized use or copying of files.

CAMS Research Presentation

Dr. Siegel, CAMS Director, presented research on risk metrics. Risk was defined as *uncertainty X exposure*. Risk management was described as the effort to reduce uncertainty. Risk can be mitigated by buying insurance. Years ago, risk insurance was uncommon, but all participants indicated their organization had risk insurance today. CAMS research on risk insurance indicated that pricing insurance is hard to calculate since risk is not well understood. Distributing risk is another strategy but not always a practical one; using multiple cloud providers is a practical option.

The key to managing risk is finding a solution that aligns convenience and realistic expectations with secure measures. There are many frameworks that provide ways to manage both quantitative and qualitative risk, but most are too costly to implement or require so many assumptions that the results are not reliable. And diverting resources to building a reliable model may mean diverting resources from product development, something most companies are not willing to do. But CAMS research suggests that organizations might find new ways to manage by identifying new threats and dynamically shifting resources based on a heat map of assets within the organization. Understanding an organization's risk profile will enable a reduction in costs for cybersecurity by not investing in unnecessary insurance, correctly protecting key assets within your company, and preparing for how the company will respond to new threats.

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