Life Sciences Cybersecurity Executive Roundtable Meeting Summary
May 14, 2020

Life sciences cybersecurity executives sat down for a conversation with research scientists from Cybersecurity at MIT Sloan (CAMS) at our virtual Spring roundtable. Following introductions, participants discussed the roadblocks their teams encounter when dealing with remote work. Following the hot topics discussion, CAMS Research Affiliate Kevin Powers shared MIT research and led a discussion about handling compliance and the idea of "reasonableness" when it comes to protecting data and the FTC's requirements.

Hot Topics Session

The hot topics discussion revolved around the nature of remote work and how it is affecting the security of an organization. One member commented that the security side of things has not slowed down at all- they have doubled down in their efforts. To integrate increased endpoint security in a reasonable timeframe, this organization had people phase out of the office until only the critical infrastructure employees remained. Efforts to increase phishing awareness and share best practices for home security have also been put in place by many organizations.

The pandemic has brought on an influx of cyber attacks on hospitals, attacks aimed at the older population, and a continued increase in phishing attacks at the financial level. These types of attacks often prey on the panic and financial deficits many are suffering from right now. The emotional affects of COVID-19 make easy targets for attackers. Responding to the question of maintaining cybersecurity culture while everyone is remote, a member noted that productivity has been up since March, and they have set every employee up with laptops, monitors, and docking stations to make working from home easier. A worry with the increased productivity, however, is that the psychological effects of this transition will result in a crash sooner rather than later. In an effort to avoid burnout, managers are working with their employees to make sure everyone stays vigilent and on the same page with the resources they need.

CAMS Research Presentation

Kevin Powers J.D, CAMS Affliliate Researcher and founder and Director of the M.S. in Cybersecurity Policy Governance Program at Boston College, presented: *It's Time for the FTC to act 'Reasonable' in its Approach to Data Security.* The challenges of data security compliance are often attributed to the ambiguity of the inherently vague standard for what is "reasonable". The standard is interpreted on a case-by-case basis by the courts or regulators, leaving room for conflicted and outdated interpretations. Powers critiqued the federal oversight of cybersecurity, stating that there is no single, unified federal standard governing or instructing US public companies on cybersecurity "requirements." This means that courts will always find one thing that is below standard, even if there is no defined checklist.

The path forward is for Power's team is to take the lead and define "reasonable" data security. Additionally, it is necessary to recognize certain well established industry standards and frameworks as "reasonable" frameworks. The real issue here is how the FTC enforces data security actions. The FTC needs to act "reasonable"- it cannot continue to move the bar to an unachievable goal.

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