Life Sciences Cybersecurity Executive Roundtable
New SEC Cyber Rules and Cybersecurity Governance
February 22, 2023

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 engaged in a discussion surrounding remote hiring and working and the ways it impacts the cybersecurity of an organization. Following the hot topics discussion, CAMS Affiliate Christopher Hetner shared research and led a discussion about SEC cyber rules.

Hot Topics Session

The first hot topics discussion revolved around how to secure the remote and hybrid workforce. With the rise of remote work, managing a diverse workforce has become more challenging than ever. It's difficult to keep track of employees and ensure they're all on the same page with security.

Meanwhile, another participant explained that most of their departments are already global, with employees in Japan, Europe, and across the US. They recognize that working with people you can't reach out and touch is something they have to deal with. They haven't mandated anything, but they believe that in-person interaction is crucial to maintain a team's culture, and they note the importance of culture when it comes to cybersecurity. While remote work can be more productive, one member struggles to navigate the perception of it. Their head of oncology believes that coming in every day is necessary to cure cancer, while the head of quality does not care if employees ever come in.

CAMS Research Presentation: New SEC Cyber Rules

As cyber risk continues to become an empirical threat to the global economy, organizations, academia, business leaders, shareholders, and regulators expect transparent and quantitative means for evaluating and understanding an organization's cyber risk exposure. To address these heightened expectations, organizations need to understand the financial and business impact associated with cyber event risk. Boards of directors and management are also expected to demonstrate to investors due care in the governance and oversight of cyber risk. Moreover, global regulators continue to roll out privacy rules that are underpinned by the need for strong cyber hygiene with severe consequences for failure. This represents a rising tide in the need for strong cyber risk oversight and will impact the decision-making and expectations from investors during the next decade.

According to the Cyber Ventures Report, cybercrime will cost the global economy $10.5 trillion annually by 2025. In response to this challenge, the Department of Homeland Security has been expanding cybersecurity regulations to new sectors. Directives are now requiring critical sectors to respond and report incidents, expanding across the 16 critical sectors. However, a lack of cyber governance and the presence of cybersecurity blind spots pose an increased risk of a fragmented cyberspace. Additionally, competing technology regulations create complex challenges. New regulatory expectations (SEC) are now being placed on executive management and board of directors. For instance, Sen. Reed's bill mandates the disclosure of cyber expertise on the board. Additionally, increased focus on transparency is now evident in companies like Twitter and Uber, who have been disclosing material business interruptions causing write-downs.

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