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 board reporting and compliance. Following the hot topics discussion, CAMS Researcher Jillian Kwong shared research and led a discussion around supply chain cybersecurity concerns and third-party risk management with small and medium enterprises (SMEs).

Hot Topics Session

The first hot topics discussion revolved around Board reporting and communicating with the C-Suite. One of the participants expressed concern that their Board lacks expertise in technology and infrastructure, making it challenging to convey cybersecurity threats and information in a way that they can comprehend. To address this issue, one team had decided to collaborate with auditors, including one of their cybersecurity auditors, to provide insight into what they are observing and how they can address those concerns. While this approach presents a potential conflict of interest, it is necessary to expose the auditors to their vulnerabilities to develop an effective fix. The team is also exploring the possibility of engaging consultants to assist their audit community and Board.

According to other participants, there is a notable trend of Board members becoming more knowledgeable and understanding about asset allocation to enhance cybersecurity resilience. This encourages organizations to invest in cybersecurity, including both technology and talent. By strengthening the cyber team and allowing them to present directly to the Board, trust can be established, reducing the frequency of questioning decisions.

CAMS Research Presentation: Cybersecurity and SME's

Small and medium-sized enterprises (SMEs) are key to supply chains, yet often do not have the same level of resources for cybersecurity as larger firms. Major challenges include shortages in staffing, funding, knowledge, detection, response, and recovery. Studies have found 43% of SMEs lack any type of cybersecurity defense plan, while 51% have no cybersecurity measures in place at all. Most SMEs struggle to find breaches within days even though 63% have reported experiencing a data breach within the last year. This can cause significant disruption to global supply chains as research has found approximately 75% of SMEs could not continue operating if hit with ransomware.

No company is immune to cyberattacks; however, SMEs in particular lack vital resources to ensure adequate protection and response. Existing cybersecurity models and frameworks say what needs to be done but not how. This research focuses on how small and medium enterprises can improve security across their supply chains. We aim to develop a roadmap for helping SMEs achieve high levels of cybermaturity to better secure cybersecurity supply chains. Executives can implement culture-building exercises, establish incentives for good cyber hygiene, and increase accountability when it comes to their employees' cyber habits.

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