



Life Sciences Cybersecurity Executive Roundtable Reporting to the Board September 26, 2023

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 generative AI and the ways it impacts the cybersecurity of an organization. Following the hot topics discussion, CAMS Researcher Mridula Prakash shared research and led a discussion about board reporting using balanced scorecard.

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>

Hot Topics Session

The first hot topics discussion revolved around generative AI. The group discussed how their organizations are constructing policies around ChatGPT. Some have a strict ban on internal use of the application, while others have instilled processes to encourage safe use of it. One method requires involving the legal and cybersecurity departments if an employee makes a case to use AI in their role. There was widespread agreement that a 'second wave' of AI would soon appear in the form of vendors using AI and working it into their contracts. Even if an organization decides to limit its use of AI, it must prepare its supply chain to utilize the growing application. While managing the rapidly expanding use case of AI is on everyone's minds, many organizations are in between being at the forefront and being in the dark.

Another topic discussed was reporting cybersecurity metrics. One angle to approach establishing a "cybersecurity report card" is to benchmark your organization against your industry, size, and business. One step to strategizing Board reporting is to evaluate who is on the Board. Many Board members have witnessed growth in the company over time and are watching closely for growth in areas like cyber risk preparedness. Showing the regression of a maturity model is critical; they want to see a list of security incidents and how they were resolved. How the organization's business was impacted is the most pressing issue for the Board: how long did a cyber incident pause the work? How can that time be improved upon?

CAMS Research Presentation: Board Level Balanced Scorecard

Board reporting often covers too much technology and needs more business context. Reporting tends to be protection-focused rather than resilience-focused. This research focused on answering the appropriate information for boards to receive to execute their oversight and fiduciary responsibilities and ensure their organizations are cyber-resilient, resulting in a board-level balanced scorecard for cyber resilience.

In recent history, the Board are moving towards resilience. Now, Boards are beginning to ask more about response plans. They want to know the organization's biggest risk, even if it cannot be quantified. It can be as simple as the cash flow for a business being compromised due to a cyber incident that temporarily shuts off services. It can be a struggle to focus a Board member's attention on cybersecurity with the current tools showing all the details. The research proposed a focusing on the biggest risk and the action plan associated. The hope is it will spark the right kind of discussion among the leaders and Boards.