Life Sciences Cybersecurity Executive Roundtable Meeting Summary
June 10, 2020

Life sciences cybersecurity executives sat down for a conversation with research scientists from Cybersecurity at MIT Sloan (CAMS) at our virtual roundtable. This meeting kicked off with a discussion about how companies are transitioning 'back-to-normal' post COVID-19. Following the hot topics discussion, Dr. Keri Pearlson, CAMS Executive Director, led a discussion on how managers can prepare for responding to cyber attacks.

Hot Topics Session

This session involved participants discussing what their organization's 'return-to-normal' looks like. The result was a sample of how lifesciences companies are choosing to bring people back to the office or remain remote for the time being. One participant mentioned that management misses the energy back in the office, so they have devised a plan to have employees back in the office 2-3 days a week. Flexibility is important as most attendees mentioned reverting to a hybrid model of work from home and on-site work. Some said returning to the office is entirely voluntary, with many choosing to stay remote. Not every company prioritizes bringing back employees; with higher productivity levels and low support for returning to a 2-hour commute, one company is 100% remote indefinitely. For many, the remote working situation has allowed for management to find talent outside of their city limits. This is a benefit for production, but often a drawback for security. Being remote means security has to take a new format, with different considerations. This is one way that, depending on the size of the company, COVID-19 remains a factor in the mind of operations.

CAMS Research Presentation: Preparing for Cyber Incidents

Dr. Keri Pearlson, CAMS Executive Director, presented CAMS research on preparing the executive suite for cybersecurity leadership. The equivalent of a country preparing itself for war is organizations preparing themselves for a cyber event. No executive wants to face an actual emergency cyber crisis with untested response and continuity plans. This research explores different types of tabletop exercises (TTX) and fire drills, identifying objectives and benefits for each level.

Four Types of TTX/Fire Drills

Target	Objectives
Board of Directors TTX	Awareness, Crisis Management, Education
C-Suite TTX	Crisis Management, Business Continuity
Organization Fire Drill	Test Response Planning and Contingencies
Technical Team Fire Drill	Test Technical Responses (detect and respond)

TTX and fire drills uncover holes in response plans. Basic organizational information necessary for proper response often disappears when a few key individuals are unavailable. Often communication channels can be disrupted. The best exercises produce an "ah-ha!" realization of the weaknesses in the organization's plans and give leaders clear ideas on how to create more robust and resilient teams. Knowing what to practice, who to involve, and how to run these exercises can save an organization from expensive mistakes. TTX and fire drills are important tools to prepare organizations for cyber response. This research helps managers and leaders design appropriate TTX and fire drills for each level of their organization to better prepare their teams in the event of a cyber crisis.

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