Cyber Norms
CAMS Life Sciences Roundtable
September 14, 2022

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 Hot Topics discussion around access management. Following the hot topics discussion, CAMS Research Assistant Benjamin Madnick shared research and led a discussion surrounding cyber norms and how they are suggested, adopted, or discarded.

Hot Topics Session

The first hot topics discussion revolved around role-based access control. This enables system administrators to regulate access to corporate networks or systems based on individual users' roles, which are defined by their job title, level of authority, and responsibility within the business. Roundtable participants discussed different ways of approaching a limited-access model and different softwares that help block certain access. One of the downsides of identity access management systems is that it can cause frustration within smaller companies where people wear many hats. This could also result in loss of productivity if an employee encounters a block while working on a project. One participant commented that it is difficult for these systems to remain compliant and they could cost a company a hefty noncompliance fine.

Overall, the consensus was that IAM is a necessity for a business, but choosing the right software and configuring it correctly should be a top priority. Only users who absolutely need access to certain data should have the permissions to view it. The security offered by limiting information access outweighs any negatives.

The Hot Topics discussion also involved securing software in a hybrid workforce. When employees work from home, it introduces many new security concerns. Enforcing the security of employee devices connected to a personal home network is critical and relies on employees feeling a sense of personal responsibility for the company.

CAMS Research Presentation: Cyber Norms

This research focused on why cyber norms form and why they maintain or disappear. A cyber norm is a shared belief about expected behavior within the security community.
A norm does not exist until the cybersecurity defenders call for them to secure and stabilize cyberspace. Early adoption of norms by states (or firms) adds credibility and compliance pull to the norm, but norms may be going extinct. The cyber norm development process is moving consistently (but slowly) toward more activities-oriented and law-oriented subjects, revealing progress in the construction of a global cybersecurity governance schema. Which norms may come back in the future? Which norms may come back in the next four years? Think of changes that may come due to the newly elected President of the U.S. Dialogue surrounding some norms decrease for political reasons, and such norms may reappear in discussions as political climates shift. On the other hand, dialogue surrounding some Norms may decrease because they simply weren't practical, and these will most likely stay that way.