Life Sciences Cybersecurity Executive Roundtable
Quantifying Cyber Resilience with a Managerial Framework
June 14, 2023

Life sciences cybersecurity executives sat down for a conversation with research scientists from Cybersecurity at MIT Sloan (CAMS) at our virtual summer roundtable. Following introductions, participants engaged in a discussion surrounding phishing and Chat GPT and the threat they pose to the cybersecurity of an organization. Following the hot topics discussion, CAMS Researcher Ranjan Pal shared research and led a discussion on quantifying cyber resilience with a managerial framework.

Hot Topics Session

The first hot topics discussion revolved around Chat GPT. The group discussed the involvement of the legal department in deciding whether or not to allow Chat GPT. One participant commented that it was scary how many people wanted to use it in their workflows. Right now, many view it as a preliminary first-gen technology. Even if the technology is useful, everyone agrees that an abundance of caution is crucial for any usecase. For those who allow the program in their workplace, it is evaluated by legal, security risk management, and leadership. Many fear that if they ban it entirely, it will prevent their teams from learning and growing with a technology that shows no signs of departing.

The topic shifted to phishing and if it could potentially be detected by AI. With the rise of artitifical intelligence, phishing messages are certainly going to increase in quantity and quality. Utilizing AI to pre-screen emails for phishing tactics could elemenate human error. Despite the benefits, that kind of software would expose the AI to personal company information and might lead to an attack.

CAMS Research Presentation: Quantifying Cyber Resilience

For this research, CAMS created the following conceptional definition of cyber resilience: "The ability for an enterprise to anticipate, absorb, adapt, and recover under cyberthreat environments". How to Determine Metrics for Cyber Resilience? This framework outlines five dimensions to a metric: 1) Management Rank 2) Enterprise System Complexity 3) Network Communication type 4) Enterprise type 5) Manager Risk Tolerance

Many enterprises have cyber resilience metrics; these metrics must map to multiple dimensions. CAMS developed a quantification framework where the dimensions fit a quantified metric. Resilience for some is looked at on an asset level; is it available or not? If there is an attack and an asset becomes unavailable, that is the minute you lose power. Quantifying the time it takes to regain power is one way to put a metric to cyber resilience. One example of an enterprise management goal is: "Minimize adverse financial impact upon a cyber-attack" e.g., the monetary value of multi-party loss incurred due to business disruption should be less than $X . Another might be to 'constrain' time to system recovery upon a cyber-attack e.g., the time duration a system is 'down' due to a cyberincident should be less than T.

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