Cybersecurity at MIT Sloan

Cybersecurity at MIT Sloan
Research Priorities for 2020

Cybersecurity at MIT Sloan brings thought leaders from industry, academia and government together with MIT faculty, researchers and students to address strategy, management, governance and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

Cybersecurity leadership has many challenges. CAMS 2020 research priorities bring MIT research to some of the most difficult.

Research Priorities 2020

Research at CAMS focuses on the difficult leadership and managerial questions of cybersecurity. Our research framework (available here) outlines the broad scope of the areas on the CAMS research agenda. After discussions with cybersecurity leaders, we have chosen to focus this year on six of the biggest world-wide cybersecurity challenges facing both private and public sector organizations:

1. **Managing Business Impacts of Cybersecurity**- This research stream seeks to answer the large questions of "How secure are we?" . How do we manage (and minimize) financial and business impact of cyber incidents. How does cybersecurity maturity map to exposure and risk (are more mature organizations experiencing lower risk)? How can we measure the impact on cybersecurity risk of various organization and technical investments? Can we reduce cyber risk through opposition research (e.g., offensive capabilities on the dark web)?

2. **Developing, Managing and Maintaining a Cybersecurity Culture**- This research studies how we can influence employee attitudes, beliefs and values (the culture of the organization) to increase positive cybersecurity behaviors. Culture is influenced by organizational mechanisms that managers implement and by external factors. The goal of this research is to provide managers and leaders with a roadmap of how to build a culture to increase cybersecurity.

3. **Providing IoT and End Point Cybersecurity**- This research stream focuses on a better way to think about cybersecurity of IoT both at the end points. As industrial environments become more connected, vulnerabilities increase. Managers want a way to make sure all additional cybersecurity vulnerabilities are well managed. Operating in such environments presents a new set of challenges examined in this research.

4. **Providing Cyber-Physical Security Using a Systems Approach**- This research stream takes a systems-level view of cybersecurity to identify critical vulnerabilities and hazards in industrial settings. Applying System-Theoretic Accident Model and Processes (STAMP) approach to cyber-physical systems has highlighted insights to better security and reduction in possible damage caused by a cyber-attack.

5. **Compliance and Cybersecurity**- This research examines how to harmonize compliance and cybersecurity requirements. Most organizations have rules and regulations that must be followed to be in compliance, and sometimes those conflict with cybersecurity needs. Being in compliance does not guarantee cybersecurity; there are many examples of organization in compliance that have still experienced a breach.

Cybersecurity at MIT Sloan welcomes funding from sponsors for general support of the consortium research, and from organizations interested in specific research topics. All members and sponsors receive invitations to consortium events and activities, and access to consortium research, websites, and newsletters. For more information, visit https://cams.mit.edu or contact:

Dr. Stuart Madnick • Professor and Director • smadnick@mit.edu
Dr. Michael Siegel • Director • msiegel@mit.edu
Dr. Keri Pearlson • Executive Director • kerip@mit.edu