Cybersecurity at MIT Sloan

Cybersecurity at MIT Sloan
Managing Cybersecurity of AI Applications

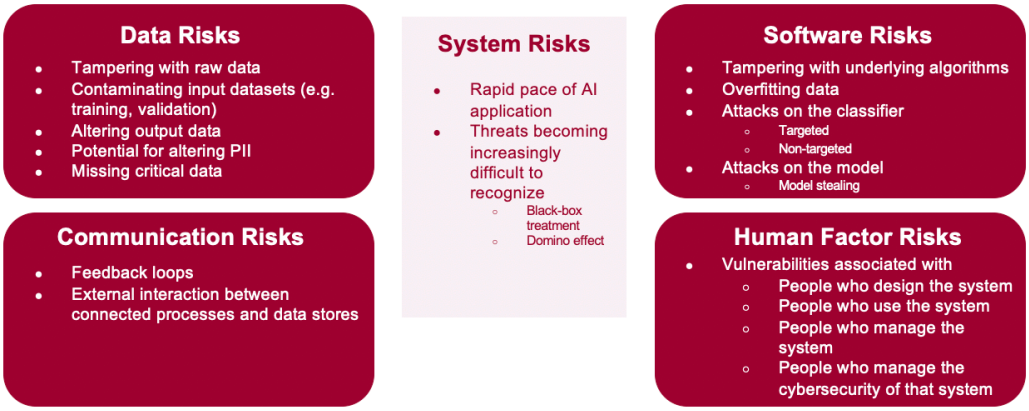
Cybersecurity at MIT Sloan brings thought leaders from industry, academia, and government together with MIT faculty, researchers, and students to address strategy, management, governance, and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

Managing Unique Cybersecurity Concerns in AI Applications

AI applications can operate as a 'black box,' where we just trust the output. How do we make sure it is valid and not the result of a cyber- attack?

Systems that utilize AI/ML technologies do not have the same cybersecurity vulnerabilities as traditional systems. Learning algorithms, test/validation data, processes, inference algorithms, and feedback loops create systems that not only learn, but are designed to find unique, obscure patterns that may not be obvious or easily detected without the AI technology. For those using AI/ML systems for diagnostics or other complex applications, the technology is often a "black box" … data is put in and a diagnosis or other recommendation comes out. But how the black box works is often only the knowledge of the designer of the system.

This poses unique cybersecurity challenges. Compromised AI systems also produce obscure or unanticipated results, making it difficult to evaluate if the unanticipated result is either valid or the result of a hacked system. This research highlights the unique leadership challenges for cybersecurity management of applications that use AI and Machine Learning. Unique vulnerabilities fall into 5 categories: data risks, software risks, communications risks, human factor risks, and system risks.



Cybersecurity vulnerabilities of AI/ML systems

IMPACT: Managers considering systems with AI engines must also understand the unique cybersecurity vulnerabilities. This project highlights the risks and suggests steps for ensuring these systems are trustworthy and reliable.

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 newsletter. For more information visit 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