Cybersecurity at MIT Sloan

Cybersecurity at MIT Sloan
The Convergence and Divergence of Regulatory Compliance and Cybersecurity

Dr. Angelica Marotta and Prof. Stuart Madnick

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.

"In an organization where there is alignment between regulations and their values, it is easier to raise or disclose difficulties with compliance regulations."

The Relationship between Compliance and Cybersecurity

The need to secure information and other digital assets at various levels and in various sectors is more crucial than ever. Not only is cybersecurity important for industries, companies, and individuals, but also for countries. Regulations in several organizational and cultural contexts are requiring increased and improved cybersecurity strategies. CAMS performed a comparative analysis drawing on eight interview-based case studies. This research examines the conditions under which compliance presents issues impacting cybersecurity and which areas are affected, in both positive and negative ways. The table below categorizes stakeholders and features the cultural, regulatory, financial, and technical factors contributing to compliance problems.

Table 2. Stakeholders' Category and Conflicting Goals

	Stakeholders' categories				
	Legal and Compliance	**Security professionals**	**Leadership and governance**	**Organizations**	**Countries/International actors**
Goals	Meet political, legal, and industry expectations	Implement modern and scalable regulations	Balance compliance and cybersecurity costs	Have a comprehensive overview of cybersecurity and compliance	Comply with national and international regulations
Observed Problems	Poor compliance oversight and management	Difficulty in developing/ implementing regulations	Challenging to allocate resources and budget	Lack of compliance culture (responsibility, collaboration, metrics, etc.)	Geographical implications cause high systemic risk

Findings: Solutions and Actionable Items for Management

The results of the analysis revealed that improving responsibility and implementing transparency seems to be the most efficient way to handle management issues related to compliance. The technique used to improve fragmented and unclear information, outdated regulations, and overly technical language is to implement proactive compliance strategies to anticipate and fill regulatory gaps. To address the problem of committing the appropriate resources to compliance and cybersecurity efforts, most participants agreed that all assets in the organization do not have to be addressed and protected the same way. Two frequent approaches to addressing unclear organizational roles and responsibilities are to engage the full set of stakeholders to ensure appropriate compliance support and promoting information sharing and collaboration.

IMPACT: Because of the scale, variety of risks, and problems deriving from cybersecurity issues, effective self-regulation is difficult to implement. Establishing an approach based on common grounds would provide a useful lens through which to solve the problems in self-regulated industries. It is essential to implement a well-functioning management system that exercises reasonable control to ensure a stable financial system and a level cross-border playing field.

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