Cybersecurity at MIT Sloan
Cybersecurity of Small and Medium Enterprises

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.

The State of SME (Small and Medium Enterprises) Cybersecurity

Small and medium-sized enterprises (SMEs) are key to supply chains, yet often do not have the same level of resources for cybersecurity as larger firms. Major challenges include shortages in staffing, funding, knowledge, detection, response, and recovery. Studies have found 43% of SMEs lack any type of cybersecurity defense plan, while 51% have no cybersecurity measures in place at all. Most SMEs struggle to find breaches within days even though 63% have reported experiencing a data breach within the last year. This can cause significant disruption to global supply chains as research has found approximately 75% of SMEs could not continue operating if hit with ransomware.

"Most companies cannot change vendors all the time- a filtered approach based on a risk profile before acceptance has to be carefully implemented."

No company is immune to cyberattacks; however, SMEs in particular lack vital resources to ensure adequate protection and response. Existing cybersecurity models and frameworks say *what* needs to be done but not *how*. This research focuses on how small and medium enterprises can improve security across their supply chains. We aim to develop a roadmap for helping SMEs achieve high levels of cybermaturity to better secure cybersecurity supply chains. Executives can implement culture-building exercises, establish incentives for good cyber hygiene, and increase accountability when it comes to their employees' cyber habits.

3 Key Weaknesses in SME Cybersecurity

Organizational culture

High levels of cybersecurity are not required when running a business

User Friction

Strengthening organizational cybersecurity was impossible without increasing user friction

Inability to verify 3rd party security

Current patterns of practice discouraged additional verification of 3rd parties and even security testing companies

IMPACT: In order to be a secure, viable vendor for their customers, SMEs need to build cybersecurity into their organizational culture and address long-standing barriers including conflicting incentive models, user friction, and a lack of accountability mechanisms around cybersecurity.

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