

Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)³ A Research Overview

If you don't address the

(IC)³ brings together thought leaders from industry, academia and government with MIT faculty, researchers and students to address strategy, management, governance and organization of cybersecurity for critical infrastructure.

people issues, you're missing

Cybersecurity Must Be Actively Managed Throughout The Organization

the hard cybersecurity problems.

All the technology available won't stop a cyber-attack if someone inside the organization 'leaves the door open.' Estimates are that between 50% and 80% of all cyberattacks are aided or abetted by insiders, usually unintentionally. If you don't address the people issues, you're missing the hard cybersecurity problems. A lot of the vulnerabilities in organizations come from the corporate culture and the practices. For example, in most industrial organizations, a safety mindset permeates the organization. Industrial plants display signs touting the number of days since the last accident as a badge of pride and a reminder of a safety mindset. But organizations have not gotten to this level with cybersecurity. Clicking on an inappropriate email which might release a virus into the corporate systems does not seem to elicit the same level of attention to safety as the physical plant signs. The consequences are not often as obvious or as immediate. But they can be just as devastating. Research at (IC)³ covers these and other topics, graphically depicted in the diagram below.

-Stuart Madnick

- * Board governance of cyber
- * Board-level cyber education

Strategy/Governance

* Cybersecurity leadership in the organization

Management

Operations

- *Cyber safety: Applying research in accident prevention to cybersecurity
- * Cybersecurity of **Industrial Control** Systems (ICS)
- * Moving to the Cloud

- *Impact of cyber risk concerns on
- *Cyber risk
- * Role of cyber insurance in risk

Technology

- *Vulnerability research
- *Security workforce
- *Comparing national
- *Usability vs security *Cybersecurity of IoT & Autonomous

Partnering

- *Comparison of international cyber processes
- *Success factors for startups
- *Cyber warfare

*House of Security: Organizational cybersecurity Culture

- *Framework for types of cyber Organization education throughout the organization
 - *Ethics of cybersecurity

*Bridging IT/OT culture gap

(IC)³ welcomes funding from sponsors for general support of the Consortium research, and from organizations interested in funding specific research topics. All sponsors receive invitations to (IC)³ events, websites, newsletters, and other Consortium activities. For more information, contact:

Professor Stuart Madnick • Director • smadnick@mit.edu

Dr. Michael Siegel • Director • msiegel@mit.edu

Dr. Keri Pearlson • Executive Director (IC)³ • kerip@mit.edu