INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

MIT Sloan MANAGEMENT

(IC)³

Newsletter #4: October 2015

(IC)³ Workshop – Wednesday, 2 December 2015

By Invitation only

This workshop is organized in collaboration with the MIT Center for International Studies (CIS)

Cybersecurity@CSAIL Sponsors are invited to attend

Location: MIT Sloan School – 100 Main Street, Cambridge, MA 02142; 3rd Floor, Room E62-350

Draft Agenda – Subject to Change

9:00-1:45pm Research Progress Reports

- MIT-(IC)3 Cybersafety research methodology – examples from TJX and Stuxnet (Stuart Madnick)
- Report from Research Collaborators at Masdar Institute (Abu Dhabi) on a Multilayered Approach to Assessing the Vulnerability of Critical Infrastructure (Sameh El Khatib)
- Overview of the Cyber Resilient Energy Delivery Consortium (CREDC)
- Lessons learned from Studying Attacks on Critical Infrastructure
- Reactions and Impacts of the White House and NIST Cybersecurity Frameworks (Michael Coden)

1:45-3:45pm Panel on Cybersecurity of Industrial Control Systems (ICS)

Panel to discuss issues such as: ICS Constraints, Long-term Architecture, What to do now, How to transition, Role of industry standards

- Stuart Madnick introduces and moderates panel (tentative panelists):
  - **ExxonMobil** (Johan B. Nye, Senior Engineering Advisor)
  - **Idaho National Laboratory** (Andrew Bochman, Sr. Cyber & Energy Security Strategist)
  - **Limelight Networks** (Kurt Silverman, Senior Vice President, Development & Delivery)
  - **New York Power Authority** (Lena Smart, Vice President, CIO)
  - **Yokogawa Electric** (Jeff Melrose, Sr. Principal Technology Specialist – Cybersecurity)
- Panelists Introductions and Opening Comments (8-10 minute position statements)
- Moderated Questions followed by Q&A with audience
- Closing remarks

4:00-6:00pm Informal Discussions, Plans for Future Events, and Reception

@ MIT Sloan School Faculty Lounge, Building E62, 5th Floor, Room E62-456

Recent Events and Activities

(IC)³ presentations were made at the I-4 (International Information Integrity Institute Cybersecurity) Forum 86 on October 20 in Boston and at the ICS Cybersecurity Conference, October 27-29 in Atlanta (Georgia Tech). Both presentations described approaches to harden ICS facilities, and further how Systems Dynamics could be used to optimize plant architecture to enable many or all of the 13 controls. The presentations were well received by an audience of cybersecurity professionals from many areas of critical infrastructure.

Upcoming Events – November 18

(IC)³ will be presented by Prof. Madnick in the Cybersecurity session of the MIT ILP Research & Development conference on November 18.

(IC)³ in the News

Bloomberg Business News

On October 26, (IC)³ appeared on Bloomberg Taking Stock, hosted by hosts Kathleen Hays and Pimm Fox, and discussed its goals and the cybersecurity challenges to the nation's critical infrastructure (click to hear).

MIT Sloan cybersecurity consortium (IC)³ receives $3.5 million from U.S. Dept. of Energy

CAMBRIDGE, Mass., Oct. 20, 2015 – "Today's enterprise cybersecurity defenses are like a bank vault with six-inch-thick steel doors and plywood walls -- heavily fortified and terribly vulnerable at the same time." This is how MIT Sloan School of Management Prof. Stuart Madnick describes the cybersecurity challenges facing the nation, particularly its energy infrastructure. To address this issue, the U.S. Department of Energy recently announced a $34-million initiative to improve the protection of the U.S. electric grid and oil and natural

gas infrastructure from cyber threats. The MIT Sloan School of Management's Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, $(IC)^3$, directed by Madnick, will receive $3.5 million from the DOE as part of this initiative.

The DOE funding comes through the MIT Sloan Consortium's participation in the University of Illinois Cyber Resilient Energy Delivery Consortium (CREDC), which consists of 11 universities and national laboratories. The CREDC undertakes research, development, education, and outreach activities with industry engagement to develop cyber-resilient energy delivery systems. The consortium seeks to generate research results and take them through to evaluation and deployment of prototypes in industrial settings, with a handoff to the energy sector through licensing, startups, and open-source mechanisms. As part of the DOE's new initiative, the CREDC was awarded $22.5 million with an additional $5.6 million for recipient cost-share. MIT Sloan's $(IC)^3$ will receive $3.5 million of that award plus $1 million for recipient cost-share.

"Cybersecurity of our critical infrastructure is a serious national security challenge. This funding from the DOE will help MIT Sloan's $(IC)^3$ make a deep and lasting impact in this area through interdisciplinary research and industry partnerships," says MIT Sloan Dean David Schmittlein.

Patricia Hoffman, assistant secretary for DOE's Office of Electricity Delivery and Energy Reliability, says, "Cybersecurity is one of the most serious challenges facing grid modernization, which is why maintaining a robust, ever-growing pipeline of cutting-edge technologies is essential to helping the energy sector continue adapting to the evolving landscape. To meet this challenge, we must continue investing in innovative, next-generation technologies that can be transitioned to the energy sector to reduce the risk of a power disruption resulting from a cyber incident."

MIT Sloan Prof. Stuart Madnick, director of $(IC)^3$, observes, "We are facing a global crisis with the cybersecurity of our critical infrastructure that requires collaboration across a range of disciplines to find solutions. We are very pleased to be a major partner in the CREDC and appreciative of the DOE funding, which will facilitate our work in this area."

University of Illinois Prof. David Nicol, CREDC principal investigator, notes that the CREDC will focus on making energy delivery systems resilient to cyber-anomalies, whether accidental or from malicious intent. "The challenge is that increased efficiencies and capabilities in energy delivery rely on greater use of computers and communication networks, which simultaneously raises the potential for serious problems."

In addition, the CREDC will look at business aspects of cyber resiliency. Nicol explains, "A major impediment to more resilient systems is the cost of upgrading legacy equipment. Researchers will identify reasons for companies to invest in new technology and design models that will help businesses choose the most cost-effective, high-impact solutions."

$(IC)^3$, which is pronounced "IC-cube", focuses on the managerial, organizational, and strategic issues related to cybersecurity. It includes diverse and interdisciplinary faculty with professors from MIT Sloan as well as the departments of Political Science, Aeronautics, Civil Engineering, Electrical Engineering, and Computer Science. The initiative also works in collaboration with industry partners across the entire infrastructure value chain. Partners include companies, such as ExxonMobil in the discovery and processing of energy, Schneider Electric in the development of systems to control energy, automation, and manufacturing, and NextNine which provides cybersecurity software for hardening industrial control systems.

Madnick and MIT Prof. Munther Dahleh, director of the MIT Institute for Data, Systems, and Society, will be the co-principal investors for MIT's activities through the CREDC. They note that some planned projects at $(IC)^3$ include:

- developing metrics and models for organizations for cyber-risk analysis, better protection, and return on investment calculations;
- applying lessons learned from "accident" prevention research to prevent cybersecurity failures;
- simulation and modeling of cybersecurity resilience;
- developing incentives for more effective information sharing; and
- measuring and increasing corporate (cultural) adoption and top-management commitment to cybersecurity efforts.

About Cybersecurity at MIT:

The MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, $(IC)^3$, is one of three cybersecurity programs at MIT. It is focused on the managerial, organizational, and strategic aspects of cybersecurity. The other two programs are Cybersecurity and Internet Policy Initiative (CIPI), focused on policy, and Cybersecurity@CSAIL, focused on improved hardware and software. More information on $(IC)^3$ can be found at http://ic3.mit.edu