MIT MANAGEMENT SLOAN SCHOOL
INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY
(IC)^3

Newsletter #12: January-February 2017

(IC)^3 Spring Workshop on April 5, 2017

Latest agenda for the 2017 Spring Workshop can be found at http://ic3.mit.edu/ic3docs/2017-04-05Agenda.pdf

Note: This workshop is by invitation-only for our (IC)^3 members and a few prospective members.

The URL for EventBrite registration has been sent to your organization. If you have not received it, please contact either smadnick@mit.edu or jcliment@mit.edu .

Agenda

Tuesday, April 4, 2017

4-5pm Cybersecurity@CSAIL Lecture:
BlackEnergy, The Russian Cyber Attacks

Registration and other information for just this lecture: https://csailcyberlectureapril2017.eventbrite.com

Note: All MIT-(IC)^3 Members are invited to the above Cybersecurity@CSAIL Lecture

6-8pm MIT-(IC)^3 Informal Dinner

Location: TBD

Wednesday, April 5, 2017

8:30am-5:30pm MIT-(IC)^3 Fall Workshop

Location: MIT Sloan School of Management
100 Main Street, Room E62-550, Cambridge, MA 02142
Map at http://whereis.mit.edu/?go=E62

8:30-9:00 Registration & Continental Breakfast

- Welcome and Introduction to MIT-(IC)^3
- Member introductions and updates on major new developments (up to 4 minutes each)
- Proposed new initiative: Cybersecurity Impact on International Trade (Simon Johnson)

10:15-10:30 Break

- Cybersecurity Impact on Adoption of New Technologies (TBD)
- Cyberinsurance as a Risk Mitigation Strategy (Juan Jose Carrascosa Pulido)

12:00-12:45 Lunch

- Benefits and Vulnerabilities of Blockchain Usage (Jae Lee)
- Security vs Usability (Saurabh Dutta)
- Using Hacker Tools to Defeat the Hackers for IoT Devices (Greg Falco)

2:15-2:30 Break

Panel: "Cybersecurity Risk Metrics"
Moderator: Michael Siegel
Panelists (*tentative*): **BCG** (Michael Coden), **Liberty Mutual** (Jim Cupps), **Limelight Network** (Kurt Silverman), **MIT** (Jerry Grochow), **Phillips Health Care** (Praveen Sharma)

4:00-4:15 Break

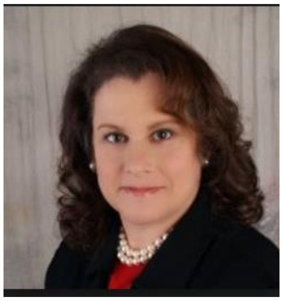
- Example Table Top Exercise for Executive Cybersecurity Education (TBD)
- Discussion: Planning for future workshops and research agenda

5:30 End of Conference

5:30-7:00 Post-Conference Reception, Informal Discussion & Student Posters

Location: E62-546

Welcome to Dr. Keri Pearlson, the first Executive Director of (IC)^3



We welcome Dr. Keri Pearlson as the first Executive Director of (IC)^3. Her prior research has focused on information technology strategy and the impact of technology on organizations. Her textbook, *Managing and Using Information Systems: A Strategic Approach*, is widely used to teach about MIS, and many of her case studies have been published at Harvard Business School.

After getting her Doctorate at HBS in information systems, she joined the faculty at the University of Texas in Austin. Since then, she has been a consultant, then an entrepreneur. Most recently she worked in the data and analytics field, leading a consortium of executives in a think-tank for analytics strategy.

She will be a valuable resource at (IC)^3 and looks forward to meeting all of you.

Recent (IC)^3 Conference & Workshop Appearances

Think Security event at MIT IAP in conjunction with Kaspersky (January 30 – February 3, 2017)

This event, organized by Kaspersky Academy and (IC)^3, was open to students during MIT's Independent Activities Period (IAP). A diverse set of students participated ranging from undergraduates to post-doctorates and from many department, including computer science, physics, Technology & Policy to MBA's.

During the weeklong seminar, students analyzed industrial control systems (ICS), typically used in the electric, water, oil and gas industries, while taking a closer look at Advanced Persistent Threats (APT) that continue to plague organizations of all sizes and sectors. At the event, students participated in both a Capture the Flag challenge and the Kaspersky Interactive Protection Simulation (KIPS) game, where participants selected suitable cybersecurity technologies for an industrial power plant and resolve specific challenges.

We thank Kaspersky for offering this course at MIT.

Student playing the game.

Packed classroom

ARC Industry Forum, Orlando (February 6, 2017)

Prof. Madnick was invited to make a presentation on our (IC)^3 research on "Studying cyber attacks and hazards of Industrial Control Systems in the Energy Sector" at the ARC Industry Forum, one of the largest gatherings of Industrial Control specialists.

He was also asked to participate on a panel on "Addressing Energy Sector Challenges and Opportunities" with Alan Farmer of Burns & McDonnell, John Maloney of Kansas City Power & Light, and Jay Cribb of Southern Company, along with Sid Snitkin of ARC.

AGENDA AT A GLANCE
Example Industrial Capacitor Explosion
(not caused by cyber attack)
• RMS Queen Mary II
• Harmonic filter capacitor bank

Left: The IC)^3 team: Stuart Madnick, Keri Pearlson, and Michael Siegel. *Right*: Stuart Madnick presenting (IC)^3 research.

Upcoming Events

FT Cyber Security Summit USA: "Is America Losing the Cyber War?" is in Washington DC., March 15, 2017. (IC)^3 will be participating and presenting in the session on "Panel: The Internet of Things – Attack Vulnerabilities and Solutions." As a feature to our (IC)^3 members, you can get a 50% discount by using the code CS50 when registering.

MIT Sloan CIO Symposium will be May 24, 2017. There will be two sessions on cybersecurity being organized by (IC)^3: "Measuring ROI for Cybersecurity: Is It Real or a Mirage?" moderated by Prof. Stuart Madnick and "You Were Hacked—Now What?" moderated by Dr. Keri Pearlson. For our (IC)^3 members, you can get discounted $99 registration fee by using the code IC3-VIP-17.

(IC)^3 in the News

Sloan Management Review (Jan 2017) features a lengthy interview with Madnick about: "What Executives Get Wrong About Cybersecurity."

Some examples of the questions discussed included:

SMR: Why did the MIT cybersecurity consortium you lead choose to focus on the nation's critical infrastructure?

MADNICK: Much of the attention about cybersecurity has been focused on things like stealing credit cards — which is important, and we don't neglect that. But surprisingly little attention has been paid to cyberattacks on critical infrastructure. You don't hear much about the Turkish pipeline explosion or the German steel mill meltdown. You may have heard a little bit about the cyberattack on the Ukrainian power grid that happened around Christmas in 2015. Generally, these events involving attacks on infrastructure do not get much attention; they're not quite as sexy as movie stars' emails being revealed. But they have the potential to have far bigger impact.

SMR: What are the most important things business executives can do to decrease their companies' cybersecurity vulnerabilities?

MADNICK: If you don't address the managerial, organizational, and strategic aspects of cybersecurity, you're missing the most important parts. A lot of people are working on developing better hardware and software, and that's good. That's important. But that's only a piece of the puzzle. Estimates are that between 50% and 80% of all cyberattacks are aided or abetted by insiders, usually unintentionally — typically through some kind of "phishing" expedition [involving emails containing a link or attachment to click on].

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 the Internet Policy Research Initiative (IPRI), focused on policy, and Cybersecurity@CSAIL, focused on improved hardware and software. More information on (IC)^3 at http://ic3.mit.edu or by contacting smadnick@mit.edu