MIT Sloan MANAGEMENT

INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (IC)^{3}

Newsletter #1: July 2015

Introduction!

The (IC)^{3} official launch took place as part of the "Cybersecurity at MIT" event at MIT on March 12, 2015. Photos, videos, and extensive press coverage of that event are posted on the (IC)^{3} home page at http://ic3.mit.edu

Upcoming Events – Hold these dates

We have two workshops planned, in collaboration with the MIT Cybersecurity@CSAIL research group.

These are planned to be 2 ½ day events. The first ½ day will be an afternoon joint panel session focused on a specific topic, for first workshop it will be on Cyber Insurance. Then followed by a one day workshop organized by (IC)^{3} and a one day workshop organized by CSAIL. An official notice will be sent out shortly, final arrangements for these dates is still underway.

Sept 22-24, 2015:

- Tues, Sept 22 joint panel - topic: Cyber insurance
- Wed, Sept 23 - (IC)^{3} member day
- Thurs, Sept 24 - CSAIL member day

(IC)^{3} Partner members are invited to attend the CSAIL meeting on the 24th.

Early November (date to be determined):

Joint workshop - topic: Cybersecurity of Legacy Systems - especially Industrial Control Systems (ICS).

Issues to be addressed include: ICS Constraints? Long-term Architecture? What to do now? How transition? Role of industry standards?

(IC)^{3} in the News

(IC)^{3} has been featured in several publications, most recently in the June 2015 article "New tactics for improving critical infrastructure cybersecurity pushed by MIT consortium" by Mary K. Pratt in TechTarget

Recent Events

MIT CIO Symposium – May 20, 2015: Panel on Cybersecurity

(IC)^{3} was asked to organize a panel on cybersecurity for the popular MIT CIO Forum. Information about the session can be found at: http://mitcio.com/cybersecurity-new-approaches-assessing-and-maximizing-your-protection and a video of the session is at https://youtu.be/DlRqD0GI560?list=PLwjjyiP72rZrljIh132_Ay6kv8eDhFtuS

Panel (from left to right): Prof. Stuart Madnick (standing), Director of (IC)^{3}; Shuman Ghosemajumder, Shape Security; George Wrenn, Schneider Electric; Nick Milne-Home, 1E; Roland Cloutier, ADP.

There was lively discussion around topics, such as:

1. Most important new positive development this year?
2. The pace of cyberattacks has been accelerating in the past three years. What has changed? What lessons learned?
3. What role does the CIO have regarding cybersecurity? Should CISO report to CIO, CEO, or Board?
4. Education for next generation of CIO (re: cybersecurity?)
5. Can businesses do better? (e.g., cybersafety culture)?
6. How get the attention, support, and resources needed from top management? What matters most: (a) financial risk to firm? (b) reputational risk?, (c) liable (criminal/civil) risk?
7. To what degree are internal IT staff a threat to security?
8. New laws, regulations, standards? E.g., White House/NIST Cybersecurity Framework – good, bad, or ugly?
10. Dangers of Internet of Thing (IoT) – threats now jump the gap from cyber to physical?
11. What do you expect to be the cybersecurity situation in ten years? Better or worse? Why?

RSA Conference - April 20 - 24, 2015, San Francisco

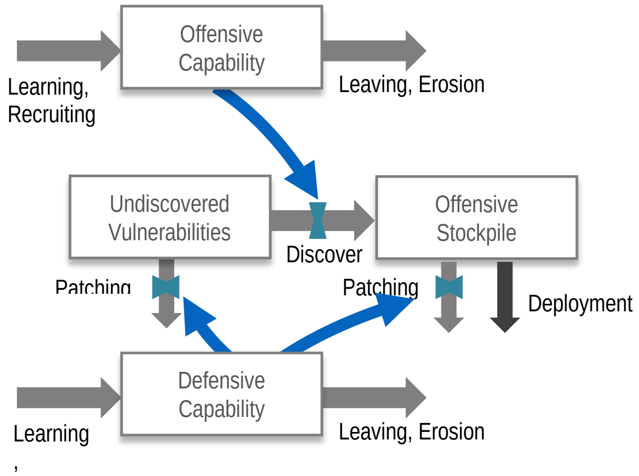
Michael Siegel of (IC)^{3} and Katie Moussouris of HackerOne presented their research titled, "The Wolves of Vuln Street: The 1st Dynamic Systems Model of the 0-day Market", at this year's RSA Conference.

What policy levers do we have for reducing vulnerability?
Which has the most leverage?

(At right) Michael Siegel, Associate Director of (IC)^{3}

The RSA conference is attended by over 30,000 security academics and professionals and is the largest gathering of its kind in the world.

Zero-day (or 0-day) vulnerabilities have been traded for decades for defense & offense. A market ecosystem has evolved that contains a number of players and a varying array of dynamics. Recent bug bounty programs, where companies pay people who find bugs, have also helped to changed market dynamics. The research presented examined the various levers in the market as is represented in the model below.



Results suggest that although there is value in additional defensive capabilities, there is more value in improving tools and techniques to better track the offensive capabilities. This insight has led to the launch of a new bounty program for tools and techniques for vulnerability discovery.

The presentation was very well attended with significant follow-on with both government and commercial organizations.

International Conference on Computer Security in a Nuclear World - June 1-5, 2015, Vienna, Austria

(IC)^3 was invited to present some of its current research at the International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange held by the International Atomic Energy Commission (IAEA).

The conference, held in Vienna, Austria, was attended by over 700 nuclear cyber security experts from over 100 different countries. (IC)^3 presented our work on "Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks."

In addition, (IC)^3 also presented 3 poster sessions on Cybersecurity Metrics, Modeling the Vulnerability Markets, and Modeling System Resilience. The oral PowerPoint presentation was well received, as were the poster presentations. (IC)^3 also had a complementary recruiting booth at the conference enabling more extended discussions with cybersecurity experts and potential sponsors.

MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity – (IC)³
Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks
IAEA

(At left) Michael Coden, Associate Director of (IC)^3

It was quite interesting that there were 7 additional cyber-safety presentations, from countries as diverse as France, Ukraine, Germany, and Korea, discussing both the safety issues of cybersecurity in nuclear facilities and the relationship between safety and cybersecurity. The (IC)^3 approach however was quite novel, and much more comprehensive than the other presentations. We expect a number of these countries to be contacting (IC)^3 in the near future.

This was the first cybersecurity conference held by the IAEA. The next one will be held in December 2016. The purpose of the conference was to: (a) review the international community's experience and achievements in strengthening computer security within the framework of nuclear security; (b) enhance understanding of current approaches for computer security worldwide within nuclear regimes, and identify trends; and (c) provide a global forum for competent authorities, operators and other entities engaged in computer security activities relevant to nuclear security.

Clearly nuclear facilities are among the most important to make secure. (IC)^3 was pleased to be invited to participate in this conference and believes that through the contacts we made in Vienna, we will be able to help make the world a much safer place. Details about the conference can be found at: http://www-pub.iaea.org/iaeameetings/46530/International-Conference-on-Computer-Security-in-a-Nuclear-World-Expert-Discussion-and-Exchange

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.