

Cybersecurity at MIT Sloan

Interdisciplinary Consortium  
for Improving Critical  
Infrastructure Cybersecurity™

MIT  
Massachusetts  
Institute of  
Technology

(IC)<sup>3</sup>™

MIT  
MANAGEMENT  
SLOAN SCHOOL

Copyright (IC)<sup>3</sup>, 2018 (v28)

## Filling Important Need for Improved Security of Critical Infrastructure



- **Security of conventional information systems is recognized as important ...**
  - But still not fully effective (e.g., Target, Sony, HSBC, US OPM, etc.)
- **Security of our Cyber-Physical Infrastructure and IoT ...**
  - E.g., computer controlled utilities, home sensors, oil & gas sites, chemical, water, financial services, autonomous vehicles, telecom, infrastructure, etc.
  - ... **is even more important, but much less research has been done.**
- **Most research focused on improving hardware and software**
  - Helpful, but ...
  - Majority of events (estimates 70-80%) are aided or abetted by insiders
- **Need to address managerial, organizational, and strategic aspects of cybersecurity**

## Who is this important to? *(Just about Everyone!)*



- **White House Executive Order (2014, 2015, 2016):** “... cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront ...”
- **SEC Commissioner Luis A. Aguilar** ... warned that “boards that choose to ignore, or minimize the importance of cybersecurity oversight responsibility, do so at their own peril ...”

3

## Interdisciplinary MIT Team Members



- **Stuart Madnick** – Director of (IC)<sup>3</sup>, Professor of Information Technologies, **MIT Sloan School of Management** & Professor of Engineering Systems, **MIT School of Engineering**
- **Nazli Choucri** – Professor of Political Science, **MIT School of Humanities & Social Sciences**
- **David Clark** – Senior Research Scientist in Computer Science and Artificial Intelligence Laboratory (CSAIL)
- **Michael Coden** – Research Affiliate (former member of White House cyber study)
- **Jerrold Grochow** – Research Affiliate (former MIT CIO and member of MITeI cyber study)
- **Mohammad Jalali** – Research Scientist, **MIT Sloan School of Management**
- **James Kirtley** – Professor of Electrical Engineering, **MIT School of Engineering**
- **Andrew Lo** – Professor of Financial Engineering, **MIT Sloan School of Management**
- **Allen Moulton** – Research Scientist, **MIT School of Engineering**
- **Keri Pearson** – Executive Director of (IC)<sup>3</sup>, **MIT Sloan School of Management**
- **Michael Siegel** – Principal Research Scientist, **MIT Sloan School of Management**
- **Richard Wang** – Principal Research Scientist, **MIT Sloan School of Management**
- **John Williams** – Professor of Civil and Environment Engineering, **MIT School of Engineering**
- **Raphael Yahalom** - Research Affiliate, **MIT Sloan School of Management**

4

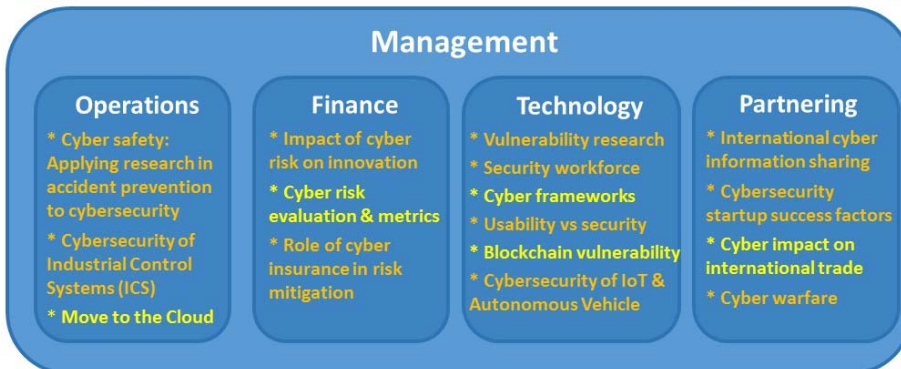
## Current (IC)<sup>3</sup> Projects



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

**Strategy/Governance**

\* Where does cybersecurity leadership fit in organization



\* Mature research (papers available)  
\* In-progress research (informal initial results)  
\* Start-up research

*Note: Most projects fit into multiple categories. Only the primary category is shown.*

\* Home of Security: Organizational Cybersecurity Culture  
\* Bridging IT/OT culture gap

**Organization**

\* Framework for types of cyber education throughout organization  
\* Ethics of Cybersecurity

5

## Examples of (IC)<sup>3</sup> Research



- **MIT House of Security:** Techniques to measure perceptions of security in an organization.
- **Cybersafety:** Extend research on accident prevention to prevent cyber events.
- **Vulnerability Research and Workforce:** Enlarge cybersecurity workforce through crowd source methods of, such as “bug bounty” programs, and understand the vulnerability ecosystem.
- **Many Others:** Cyberinsurance, Board of Director Cyber Education, Information Sharing, NIST Framework, Tipping Point Analysis, etc. ...

6

## MIT House of Security Approach: Survey security attitudes and Gap Analysis

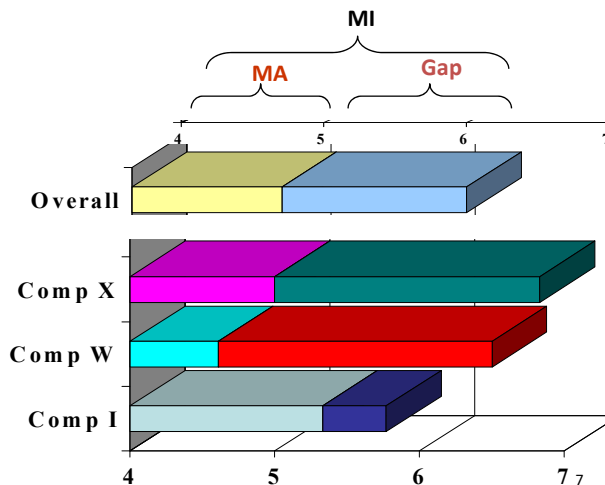
Pilot survey instrument developed.

E.g., Survey Question: **In our organization, people are aware of good security practices.**

**MA = Assessment of "My" organization**  
(5.1)

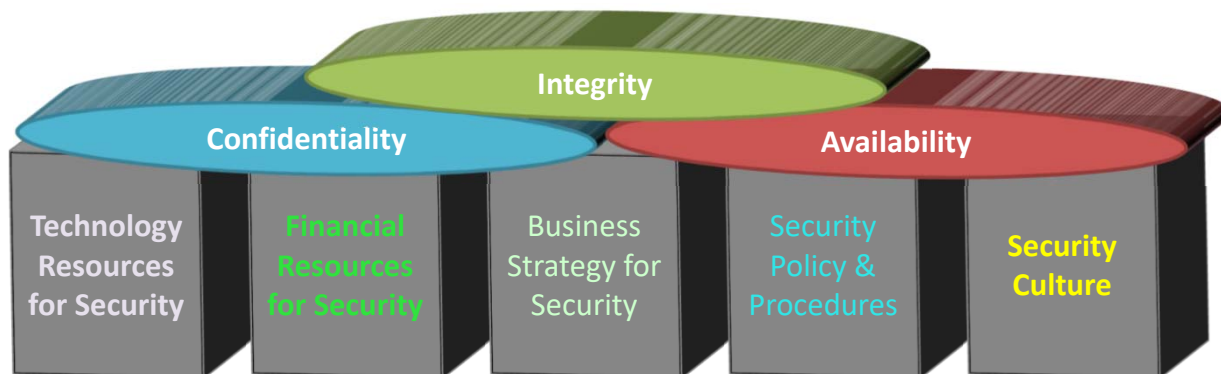
**MI = Importance for "My" organization**  
(6.3)

**Gap = difference between Assessment and Importance – for "My" organization** (1.2)



Observation: Big differences between companies. Why?

## MIT House of Security Constructs



**A Fundamental Model for Measuring Cybersecurity Effectiveness**

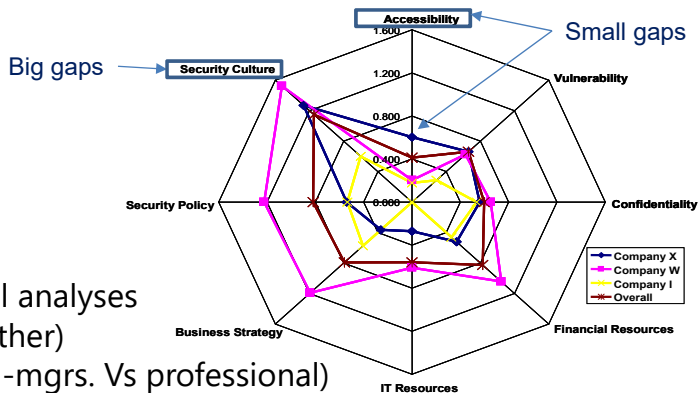
- *The House of Security has been shown to be able to provide measurements of perceptions, awareness, profile, tier, maturity, and gaps in Cybersecurity.*
- *It will be further developed to provide economic measurements of cyber-risk and the value of Cybersecurity activities allowing a calculation of Cyber-ROI.*

## Example Results from Using the MIT House of Security



- Using survey questions we assessed perception of the current state of security in the organization ... and the desired state.
- The delta is the measureable gap between desired and actual.**
- Differences between companies, but some general trends..

### Gap Assessments by Three Companies: Big Differences



Also perform intra-organizational analyses

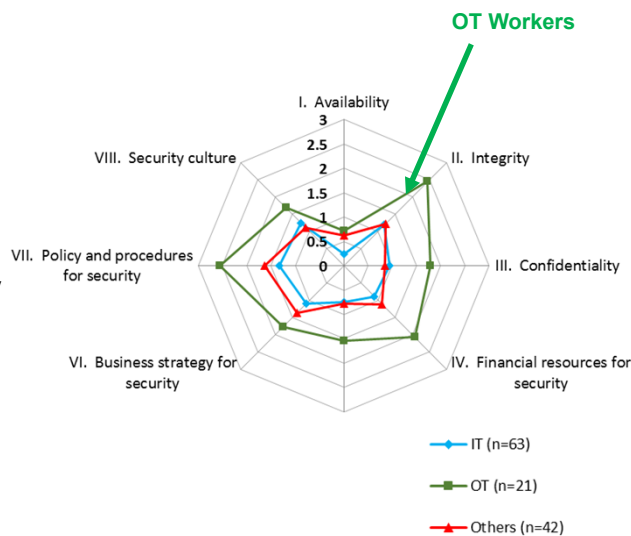
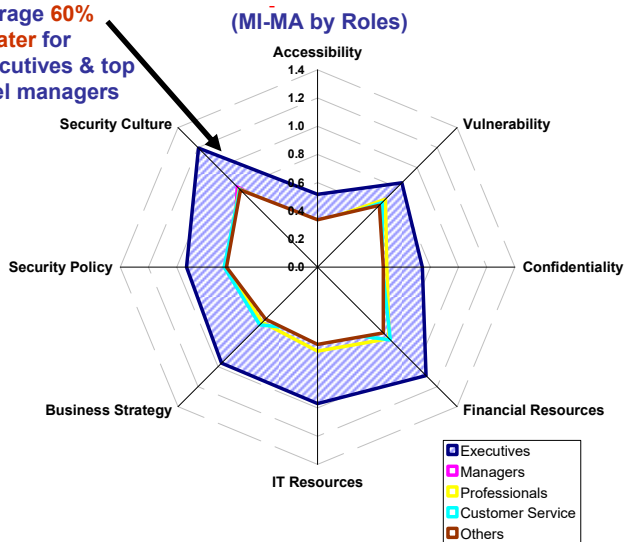
- By function (e.g., IT vs OT vs other)
- By level (e.g., top execs vs mid-mgrs. Vs professional)

9

## Which have largest Gaps?

- Top Execs vs Middle Managers vs Professionals?
- IT workers vs OT workers vs Others?

Gaps are on average 60% greater for executives & top level managers



10

## Cybersafety: Use of Accident Research to Prevent Cyber Incidents



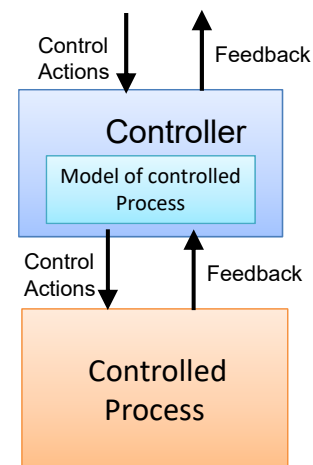
- **Apply “accident” and safety research to “cyber security” failures.**
- MIT has researched accidents and how to prevent them (including studying NASA problems) for many years.
- We are now treating a cyber incident/event as a type of “accident” and using prior research to identify, understand, and mitigate possible “cyber-hazards.”
  - Examples, such as Stuxnet and TJX, have been analyzed.
  - Uncovered vulnerabilities not in previous reports

11

## Cybersafety Hierarchical Process Model

### Key principles:

- **Top-down:**
  - What are you trying to protect / prevent?
- **Based on process model:**
  - There are Processes, and Controllers for those Processes, with “sensors” and “actuators”
- **The Processes are Hierarchical:**
  - The Controllers are processes and are controlled by higher level controllers, etc.



**This is why the management structure, leadership, and controls are so important.**

12



NEWS

# TJX data breach: At 45.6M card numbers, it's the biggest ever

Mar 29, 2007

It eclipses the compromise in June 2005 at CardSystems Solutions



By Jaikumar Vijayan [FOLLOW](#)  
Computerworld | Mar 29, 2007 1:00 PM PT

After more than two months of refusing to reveal the size and scope of its data breach, TJX Companies Inc. is finally offering more details about the extent of the compromise.

In filings with the U.S. Securities and Exchange Commission yesterday, the company said 45.6 million credit and debit card numbers were stolen from one of its systems over a period of more than 18 months by an unknown number of intruders. That number eclipses the 40 million records compromised in the mid-2005 breach at CardSystems Solutions and makes the TJX compromise the worst ever involving the loss of personal data.

## Stay Smart

Get the latest Android news, trends and apps and tips.



[Sign up for the Greenbot newsletter](#)

### FEATURED RESOURCE



PRESENTED BY SCRIBE SOFTWARE

### MORE LIKE THIS

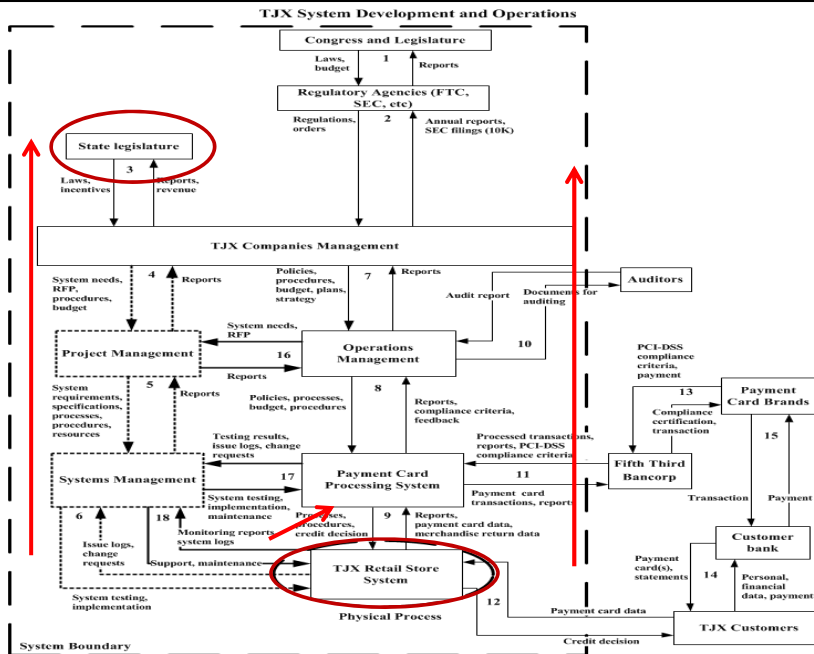
Theft of 45.6M Card Numbers Largest Heist Yet

Update: Retail breach may have exposed card data in four countries

Stolen TJX data used in Florida crime spree

13

## Hierarchical Control Structure



- Legend:**
- Each **number** indicates a unique loop.
  - **Bold-dashed square** indicates TJX system boundary.
  - **Bold-dashed oval** indicates the physical system.
  - **Downward arrow** represents reference channel for imposing safety constraints.
  - **Upward arrow** represents feedback channel and reports the effectiveness of constraints.

14

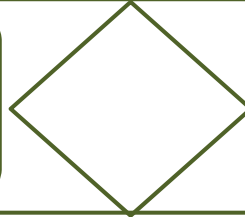
## Analysis of Higher Levels of the Hierarchical Safety Control Structure

### 1. Safety-Related Responsibilities:

- a. Payment card data is encrypted.
- b. TJX systems should be PCI-DSS compliant. (Compliance with PCI-DSS is required by retailers accepting credit cards).
- c. Provide data retention process/procedures.
- d. Systems pass rigorous testing.

### 4. Process Model Flaws:

- a. Belief that processors compliance with PCI-DSS implies compliance by TJX.
- b. Inadequate understanding of full scope of PCI-DSS



### 2. Context:

TJX not in compliance with PCI-DSS.

### 3. Unsafe Decisions and Control Actions:

- a. Inadequate **compliance** with PCI-DSS.
- b. Retained **more customer data** than needed/for **longer periods** than required.
- c. Inadequate **testing** of systems/lack of awareness of PCI-DSS.
- d. Payment data **briefly stored and then transmitted unencrypted** to the bank.
- e. Visa **issued a warning** to processor that TJX needed to be fully compliant, but (a) it had **limited influence on TJX** and (b) Visa had already granted TJX suspended fines until 2008

15

## Dynamics and Migration to a High-Risk State

*Leveson: “most major accidents are a result of **migration** of a system to a **high-risk state over time**. Understanding the **dynamics of migration** will help in redesigning the system.”*

### 1. A major change contributing to the cyber-attack was TJX’s move from wired to wireless networking (Wi-Fi) in 2000 in a short span of one year.

- a. Initially cyber security risk was low because vulnerabilities were unknown to everyone – experts, businesses, **and hackers**.
- b. TJX decided against upgrading to a more secure encryption algorithm for cost reasons.

### 2. Flaws in managerial decision making process.

- a. **Ease of recall bias** where recent experiences strongly influence the decision (i.e., no break-ins so far.)

16



## Dynamics and Migration to a High-Risk State

**3. Confirmation trap** is a decision maker’s tendency to favor information that confirms existing beliefs and discount contradicting information.

“My understanding is that we can be PCI-compliant without the planned FY07 upgrade to WPA technology for encryption because most of our stores do not have WPA capability without some changes. WPA is clearly best practice and may ultimately become a requirement for PCI compliance sometime in the future. I think we have an opportunity to defer some spending from FY07’s budget by removing the money for the WPA upgrade, but would want us all to agree that the risks are small or negligible.”

- a. Above is a message from CIO to his staff, requesting agreement on his belief that cyber security risk is low. -- a majority of his staff agreed.
- b. This confirmation trap led to postponing upgrades.

17

## Comparison of Results from FTC and CTC Investigations and Cybersafety STAMP/CAST Analysis

No.	Recommendation	CPC	FTC	STAMP/CAST
1	Create an executive level role for managing cyber security risks.	No	*	Yes
2	PCI-DSS integration with TJX processes.	No	No	Yes
3	Develop a safety culture.	No	No	Yes
4	Understand limitations of PCI-DSS and standards in general.	No	No	Yes
5	Review system architecture.	No	No	Yes
6	Upgrade encryption technology.	Yes	No	*
7	Implement vigorous monitoring of systems.	Yes	No	*
8	Implement information security program.	No	Yes	*

FTC = Federal Trade Commission; CPC = Canadian Privacy Commission

\* = Indicates recommendations that are close to STAMP/CAST based analysis but also has differences.

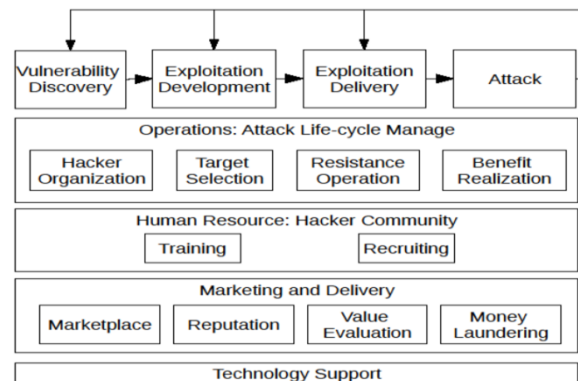
18

## Vulnerability Research and Workforce Development (Defenders & Attackers)



- Vulnerability Research and Workforce Development (Defenders & Attackers) including “bug bounty,” open source, and other approaches.
  - Develop cyberspace culture – see WSJ, [“How Companies Can Create a Cybersafe Culture at Work”](#)
  - Understand “Cybercrime-as-a-Service” on the Dark Web

**Cybercrime Capability Value Chain => Services available of the Dark Web including primary attack services and support services.**



**Primary Activities:**  
Construct Attack

**Support Activities:**  
Less cost for higher payoff

19

## Vulnerability Detection and Reduction



- Heard of “Bug Bounty” Programs?
- MIT is studying methods of vulnerability detection, such as “bug bounty” programs, using techniques such as System Dynamics modeling
  - Over 100 firms offer public bug bounty programs, recently United Airlines
  - Facebook has had over \$3.5 million in payouts
  - HackerOne runs bug bounty programs for about 72 companies
  - Represents “defensive capability” and some insight to “offensive capability”
- Can determine best types of vulnerability discovery and detection techniques, including “bug bounty,” open source, and other approaches.

20



## Example: "Hack the Pentagon"

- The DOD had paid **\$5 million** over three years to one vendor, which found less than **10 vulnerabilities**.



- In "Hack the Pentagon": 1,400 eligible ethical hackers (aka as "white hats") were invited, 250 of them found at least one vulnerability.
- Of these, **138 were found** to be "legitimate, unique, and eligible for a bounty," said Secretary Carter. ... Cost? About **\$150,000**.
- Also, it frees up the US military's own cyberspecialists "to spend more time fixing them than finding them. ... way to streamline what we do to defend out networks and correct vulnerabilities more quickly."

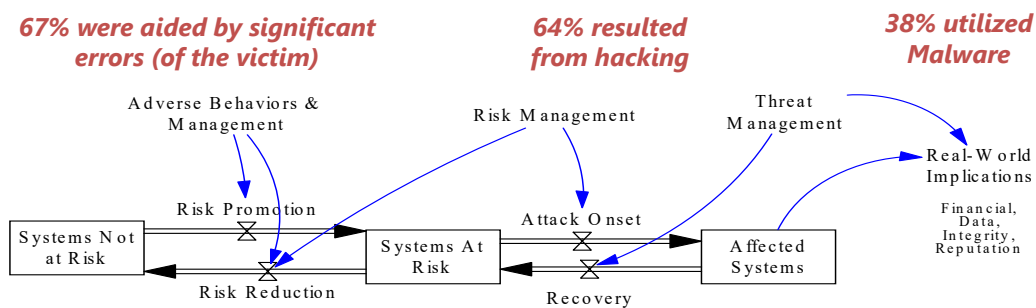
21

## Dynamics of Threats and Resilience

(using System Dynamics modeling)



### How did breaches (threats) occur? \*



### How are security and threat processes (resilience) managed? \*

*Over 80% of the breaches had patches available for more than 1 year*

*75% of cases go undiscovered or uncontained for weeks or months*

\* Verizon Data Breach Report

22

## Some Findings



- Solving security problems “upstream” is more effective than fixing them “downstream.”
- Models help understand the security issues in patching and software release dynamics
- Understanding the tools and techniques of finding vulnerabilities helps to improve security
- Understanding the researcher/hacker/security workforce will help with defense
- All organizations can learn from bug bounty programs

23

## Why Join (IC)<sup>3</sup> ?



- Existing organizations are trying to address today’s threat and plan for future threats, but:
  - “The CSO/CISO is too busy bailing water to plug the holes in the boat”
- (IC)<sup>3</sup> is focusing MIT’s uniquely qualified interdisciplinary faculty and researchers on the fundamental principles of cybersecurity applied to Critical Infrastructure:
  - “Enabling the CSO/CISO to plug the holes in the boat”
  - Creating tools to
    - Strategically develop measureable, cost effective, cybersecurity strategies
    - Implement Cybersafety awareness and culture change
    - A confidential academic forum in which to benefit from the experiences of CSO/CISOs from multiple sectors

24

## Operation of (IC)<sup>3</sup>



- The day-to-day operation of (IC)<sup>3</sup> is managed by the Director of (IC)<sup>3</sup> with the support of the (IC)<sup>3</sup> Associate Directors.
- The (IC)<sup>3</sup> Advisory Board, in consultation with the Director of (IC)<sup>3</sup>, will determine the research focus areas for each year.
- The (IC)<sup>3</sup> faculty working with full-time MIT research staff and graduate students, often in cooperation with Member organizations, will conduct the research.
- (IC)<sup>3</sup> will organize and conduct two research topic-specific workshops each year.
- (IC)<sup>3</sup> will organize and conduct its Annual Conference, covering the wide range of its research topics, each year.

25

## Types of Sponsors and Benefits \*




- **Members:** \$35,000 if three year commitment or \$45,000 if one year commitment
  - Send 2 people to annual conference and 2 workshops per year
  - Access to research in the MIT-(IC)<sup>3</sup> research database<sup>1</sup>
- **Partners:** \$120,00 per year – commitment for 3 years (can be 1 year for first year)  
Includes all items above plus:
  - Ability to suggest research areas
  - Ability to re-distribute select research content to existing clients and customers<sup>1</sup> Ability to contact designated faculty via telephone
- **Patrons:** \$450,000 per year – commitment for 3 years (can be 1 year for first year)  
Includes all items above plus:
  - Ability to suggest research projects and refinements, be considered for inclusion
  - A dedicated faculty contact, with monthly consultations
  - One on-site faculty presentation to the organization's governing board

\* Details on additional benefits contained in the Sponsorship Agreement

<sup>1</sup> Subject to 3<sup>rd</sup> party rights and bearing appropriate legends

From more information, go to <http://ic3.mit.edu>

26










**MIT MANAGEMENT SLOAN SCHOOL**









**INTERDISCIPLINARY CONSORTIUM  
IMPROVING  
CRITICAL INFRASTRUCTURE  
CYBERSECURITY (IC)<sup>3</sup>**

**Collaborations**

**Members**















**Partners**















**FOUNDERS**  
*(Founders are those who joined during (IC)<sup>3</sup>'s first year)*


**Partners**




**Members**



**MIT Sloan MANAGEMENT**

**INTERDISCIPLINARY CONSORTIUM  
IMPROVING  
CRITICAL INFRASTRUCTURE  
CYBERSECURITY (IC)<sup>3</sup>**



**To learn more about Cybersecurity at MIT Sloan:  
the Interdisciplinary Consortium for  
Improving Critical Infrastructure Cybersecurity,  
(IC)<sup>3</sup>™**

See <http://ic3.mit.edu> or contact Stuart Madnick [smadnick@mit.edu](mailto:smadnick@mit.edu)  
or Michael Siegel [msiegel@mit.edu](mailto:msiegel@mit.edu) or Keri Pearlson [kerip@mit.edu](mailto:kerip@mit.edu)

14