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 => Cybersecurity Governance and Culture
Who is this important to?  *(Just about Everyone!)*

- **White House Executive Order:** “... cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront ...”
  - $19B proposed in FY2017 budget for Cybersecurity
- **U.S. Secretary of Energy Ernest Moniz:** “… nation's oil and gas industry ... cyber threats continue to increase in frequency and sophistication ...”
  - December 2015 attack on Ukrainian electric distribution
- **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 ...”

---

Initial Interdisciplinary MIT Team Members

- **Stuart Madnick** – 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 and Social Sciences**
- **David Clark** – Senior Research Scientist in Computer Science and Artificial Intelligence Laboratory (CSAIL), **MIT School of Engineering**
- **Michael Coden** – Research Affiliate (former member of White House cyber study)
- **Jerrold Grochow** – Research Affiliate (former MIT CIO and member of MIT Key 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**
- **Michael Siegel** – Principal Research Scientist, **MIT Sloan School of Management**
- **Richard Wang** – Principal Research Scientist, **MIT School of Engineering**
- **John Williams** – Professor of Civil and Environment Engineering and Engineering Systems, **MIT School of Engineering**
Current Active (IC)^3 Projects

* Board governance of cyber
* Board-level cyber education

**Strategy/Governance**
* Where does cybersecurity leadership fit in organization

**Management**

- **Operations**
  * Cyber safety: Applying research in accident prevention to cybersecurity
  * Lessons learned from studying cyber attacks on Industrial Control Systems (ICS)

- **Finance**
  * Impact of cyber risk concerns on innovation
  * Cyber risk evaluation & metrics
  * Role of cyber insurance in risk mitigation

- **Technology**
  * Vulnerability research and the Security workforce
  * Evaluating and comparing national cyber frameworks
  * Usability vs. security

- **Partnering**
  * Comparison of international cyber information sharing processes
  * Success factors for cybersecurity startups

**Organization**

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

* 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.

Some examples of Research on Cybersecurity Governance and Culture

- **MIT House of Security**: Techniques to measure perceptions of security in an organization => Cybersecurity Culture
- **Cybersafety**: Research on accident prevention to prevent cyber events => Management’s role in Governance of Cybersecurity
- **Internet governance: A confused landscape** by David Clark (CSAIL)
- **Complexity of Organizational Cybersecurity Capability Development** by Mohammad Jalali ((IC)^3)
MIT House of Security

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.
Cybersafety: Use of Accident Research to Prevent Cyber Incidents and Understand Management Role

- 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

Cybersafety Methodology

**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.
**NEWS**

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

It eclipses the compromise in June 2005 at CardSystems Solutions

Mar 29, 2007

By Jakumar Vjayan

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-2003 breach at CardSystems Solutions and makes the TJX compromise the worst ever involving the loss of personal data.

---

**FEATURED RESOURCE**

Hierarchical Control Structure

---

**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
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.

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.

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.

---

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. Recall bias where recent experiences strongly influence the decision (i.e., no break-ins so far.)
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.

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

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

FTC = Federal Trade Commission; CPC = Canadian Privacy Commission
* = Indicates recommendations that are close to STAMP/CAST based analysis but also has differences.
To learn more about the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, (IC)³™

See http://ic3.mit.edu or contact Stuart Madnick smadnick@mit.edu or Michael Siegel msiegel@mit.edu or Michael Coden mcoden@mit.edu

Other Speakers in this Session

- **Internet governance: A confused landscape**
  by David Clark of MIT Computer Science and Artificial Intelligence Laboratory (CSAIL)

- **Complexity of Organizational Cybersecurity Capability Development**
  by Mohammad Jalali of (IC)³