2015 MIT Research and Development Conference
Leading Disruption - November 18-19, 2015

The MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, (IC)³

Stuart Madnick
Professor of Information Technologies, MIT Sloan School of Management and Professor of Engineering Systems, MIT School of Engineering
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, 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):** “... cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront ...”
- **U.S. Secretary of Energy Ernest Moniz:** “... From producing wells to tank batteries to pipelines, computer networks are playing an increasingly important role in the operations of the nation's oil and gas industry ... cyber threats continue to increase in frequency and sophistication ...”
- **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)
- **Michael Coden** – Research Affiliate (former member of White House cyber study)
- **Jerrold Grochow** – Research Affiliate (former MIT CIO and member of MITei cyber study)
- **Nancy Leveson** – Professor of Aeronautics and Engineering Systems, 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
Examples of (IC)3 Research

- **MIT House of Security**: Techniques to measure perceptions of security in an organization.
- **Cybersafety**: Research on accident prevention to prevent cyber events.
- **Control Points**: Best “choke points” to interrupt a criminal enterprise.
- **Information Sharing & Improving CERTs**: Ways to improve and better coordinate the CERTs and other information sharing mechanisms.
- **Vulnerability Reduction**: Crowd source methods of bug detection, such as “bug bounty” programs, and the vulnerability ecosystem.
- **Tipping Point Analysis**: Using System Dynamics to understand what will make complex systems unstable.
- **Simulation**: Simulation of complex systems under a variety of circumstances.
- **Others**: Cyberinsurance, Board of Director Cyber Education, NIST Framework, etc ...
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 measurable gap between desired and actual.

![Current State Assessments by Three Companies: Big Differences](image1)

![Gap Analysis](image2)

Largest Gap = .82
Smallest Gap = .33

[Company X], [Company W], [Company I], Overall
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
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.
TJX data breach: At 45.6M card numbers, it's the biggest ever

It eclipses the compromise in June 2005 at CardSystems Solutions

By Jaikumar Vijayan

Mar 29, 2007

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.
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.

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. **Ease of 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/seek information that confirms his/her own 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.
Some Recommendations from Cybersafety Analysis

1. According to PCI Security Standards Council, compliance is a business issue requiring management attention and need to integrate PCI-DSS requirements within appropriate components on development and operations parts of the control structure.

2. PCI-DSS not fully adequate.
   a. Data must be encrypted when sent over a public network, but not when transmitted within TJX.
   b. PCI-DSS did not mandate using stronger encryption WPA until 2006, even though WPA was available in 2003.

3. Building a safety culture at TJX including a dedicated executive role with cyber security responsibilities.
## 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>

CPC = Canadian Privacy Commission  
FTC = Federal Trade Commission  
* = Indicates recommendations that are close to STAMP/CAST based analysis but also has differences.
Vulnerability Detection and Reduction

• Improving Vulnerability Discovery and Detection:
  • 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 provides some insight into “offensive capability”
  • MIT (IC)^3 research can determine which types of vulnerability discovery and detection techniques provide the results with the greatest value, including “bug bounty,” open source, and other approaches.
Dynamics of Threats and Resilience
(using System Dynamics modeling)

How did breaches (threats) occur? *

67% were aided by significant errors (of the victim)
64% resulted from hacking
38% utilized Malware

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
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.
To learn more about the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, (IC)³™

See http://ic3.mit.edu