Stuart Madnick
John Norris Maguire Professor of Information Technologies
& Professor of Engineering Systems
Massachusetts Institute of Technology

BATTLING CYBERCRIME:
What Every Manager Should Know About Cybersecurity:
Popular Myths and Misunderstandings Exposed

MIT Sloan Reunion Weekend 2018
11:45 AM - 12:45 PM Faculty Session 2a
E52-6th Floor, Samberg Conference Center
Audience Participation

Q: Do you know if your organization has experienced a cyber-attack?
Key Misconceptions and Myths

• Isn’t it just a matter of some credit card numbers stolen? – Big Deal!
• Isn’t the problem being solved, going away?
• Isn’t it just a technology problem, best left to the IT folks?
• Simple solution? = Just don’t click on email about an offering from a Nigerian prince.
• Best Practices?
• What can you do? What is MIT doing?
Equifax's chief information officer and chief security officer are out

by Julia Horowitz and Danielle Wiener-Bronner  @CNNMoney
① September 15, 2017: 7:30 PM ET

Equifax CEO Rick Smith Needs to Be Fired

Douglas A. McIntyre
24/7 Wall St. September 16, 2017

It may only be a matter of time before the board of Equifax Inc. (EFX) fires its long-time chair and chief executive, Rick Smith. However, the move cannot come too soon to satisfy investors, regulators and customers. All the problems that built up to the hacking of 143 million Equifax accounts happened on his watch.
What is “WannaCry”?  
What happened on Friday, May 12, 2017?

• One example:
  – Ransomware attack on Telefónica blocked 80% of its computers!
  – Hackers demand $300 per computer
  – All employees sent home!

• Over 300,000 computers attacked in over 100 countries within hours
Not just stolen credit card numbers

• Had you heard of Ransomware before?

• Have you heard of SWIFT?

SWIFT reveals new cyber-attacks on its money transfer system

• It is not just about money:

FBI says foreign hackers penetrated state election systems

Michael Isikoff, Chief Investigative Correspondent, August 29, 2016

• … it could be your property or your life …
Cyber to Physical Risks with Major Consequences to Life and Property

German steel mill suffered "massive damage" following a cyber attack

U.S. Electric Grid Vulnerable to Unprecedented Waves of Attack
Threats increase as industry scrambles to boost security
By Adam Kredo, March 27, 2018 12:45 pm
Lights Out by Ted Koppel

In this tour de force of investigative reporting, Ted Koppel reveals that a devastating cyberattack on America’s power grid is not only possible but likely and that the United States is shockingly unprepared.

“This is not science fiction. Hats off to Ted Koppel for putting us all on alert.” – TOM BROKAW

"Without a single bullet, bomb, or missile, a foreign enemy can now launch a devastating attack on the United States... I hope he’s wrong about the danger but fear he's right on the mark."

– ERIC SCHLOSSER, author of ‘Command and Control’ and ‘Fast Food Nation’
Key Misconceptions and Myths

• Isn’t it just a matter of some credit card numbers stolen? – Big Deal!
• Isn’t the problem being solved, going away?
• Isn’t it just a technology problem, best left to the IT folks?
• Simple solution? = Just don’t click on email about an offering from a Nigerian prince.
• Best Practices?
• What can you do? What is MIT doing?
Problem going away? Good News / Bad News

**Good News:** The Good Guys are getting better.

**Bad News:** The Bad Guys are getting badder faster!

**Gap growing**

![Graph showing increasing effectiveness over time with two lines, one for effectiveness and one for time, with the gap between them growing.]

---

The Switch

Hackers are getting better at offense. Companies aren’t getting better at defense.
You don’t need to be a super techie hacker, you can buy what you need!

• You can buy on Dark Web all the tools developed by NSA to spy on other countries? => Used in WannaCry
Key Misconceptions and Myths

• Isn’t it just a matter of some credit card numbers stolen? – Big Deal!
• Isn’t the problem being solved, going away?
• Isn’t it just a technology problem, best left to the IT folks?
• Simple solution? = Just don’t click on email about an offering from a Nigerian prince.

• Best Practices?
• What can you do? What is MIT doing?
Isn’t cybersecurity a technology problem best left to the IT folks?

- Most research and industry efforts focused on improving hardware and software
  - Helpful, but ...

- **Majority of events** (estimates 70-80%) are aided or abetted by insiders (usually unintentional)

- **Need to address** managerial, organizational, and strategic aspects of cybersecurity
  - Consistent with responsibilities of the CEO and C-Suite (and all management)
Key Misconceptions and Myths

• Isn’t it just a matter of some credit card numbers stolen? – Big Deal!
• Isn’t the problem being solved, going away?
• Isn’t it just a technology problem, best left to the IT folks?
• Simple solution? = Just don’t click on email about an offering from a Nigerian prince.

• Best Practices?
• What can you do? What is MIT doing?
“Prevention is Futile” [Gartner report]

• What is Phishing?

• How effective?
  – Mass phishing spam emails: open rate of 1-3%.
  – Generic well-crafted Phishing: 10%
    • “Notice from IT Help Desk, we're updating all staff and student mailbox from 500MB to 5GB. Click HERE for re-validation and increase.”
  – Use of first and last name Phishing: 18%

Q: How many know what is Spear Phishing?
  – Spear phishing is very targeted email.
  – It is one of the biggest cyber security threats facing organizations today, because it works!
  – open rate of 70%

Key Misconceptions and Myths

• Isn’t it just a matter of some credit card numbers stolen? – Big Deal!
• Isn’t the problem being solved, going away?
• Isn’t it just a technology problem, best left to the IT folks?
• Simple solution? = Just don’t click on email about an offering from a Nigerian prince.

• Best Practices?
• What can you do? What is MIT doing?
Best Practices?

My personal view:
  – There are no Best Practices!

• There are poor practices,
• And less poor practices

Not just my view: (see 2016 NIST report at

“participants recommended NIST more properly
describe “best practice” sharing as “current practice”
sharing or simply “practice sharing.”

• If NSA, Pentagon, Israel Defense Force can be broken
  into ... why do you think you are so much better?
• But, there are things you can do ...
White House / NIST Cybersecurity Framework

• 5 Areas to consider:

  - Develop the **organizational understanding** of cybersecurity risk
  - Develop and implement the appropriate **safeguards**
  - Develop activities to **identify the occurrence** of a cybersecurity event.
  - Develop activities to **take action** on a detected cybersecurity event.
  - Develop plans to **restore** capabilities impaired due to a cybersecurity event.

**Q: Is NIST being used in your organization?**

Ref: [https://www.nist.gov/cyberframework](https://www.nist.gov/cyberframework)
Shortcomings of the NIST Framework

• **Good news:** For those organizations that have previously done very little => gives directions for improvement.

• **Bad news:** For many, it becomes a lower upper bound.
  – That is, that is all that they do.
  – And that is not enough.

• From [http://www.digitalcrazytown.com/2014/08/nist-cybersecurity-framework-is-good.html](http://www.digitalcrazytown.com/2014/08/nist-cybersecurity-framework-is-good.html)
  “... assessment of the framework ranged from "pleased" to "failed," with a general sense that the framework doesn't replace the hard work of implementing adequate cybersecurity controls. ...”
  “... success ... if you have very low expectations ...”
  “... "framework is way to have a discussion about managing risk ...”

• **Something new to consider:** *Wall Street Journal*, May 31, 2018:
  "How Companies Can Create a Cybersafe Culture at Work" at [https://www.wsj.com/articles/how-companies-can-create-a-cybersafe-culture-at-work-1527646320](https://www.wsj.com/articles/how-companies-can-create-a-cybersafe-culture-at-work-1527646320)
Key Misconceptions and Myths

• Isn’t it just a matter of some credit card numbers stolen? – Big Deal!
• Isn’t the problem being solved, going away?
• Isn’t it just a technology problem, best left to the IT folks?
• Simple solution? = Just don’t click on email about an offering from a Nigerian prince.

• Best Practices?
• What can you do? What is MIT doing?
What is MIT doing?

Cybersecurity at MIT Sloan

Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)³
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, energy systems, 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 on improving hardware and software
  - Helpful, but ...
  - Majority of events are aided or abetted by insiders
- Need to address managerial, organizational, and strategic aspects of cybersecurity
Current (IC)³ Projects

**Strategy/Governance**
- * Board governance of cyber
- * Board-level cyber education
- * Where does cybersecurity leadership fit in organization

**Operations**
- * Cyber safety: Applying research in accident prevention to cybersecurity
- * Cybersecurity of Industrial Control Systems (ICS)
- * Moving to the Cloud

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

**Technology**
- * Vulnerability research
- * Security workforce
- * Comparing national cyber frameworks
- * Usability vs security
- * Cybersecurity of IoT & Autonomous Vehicle

**Partnering**
- * International cyber information sharing
- * Cybersecurity startups success factors
- * Cyber impact on international trade
- * Cyber warfare

**Organization**
- * Home of Security: Organizational Cybersecurity Culture
- * Bridging IT/OT culture gap
- * Framework for types of cyber education throughout organization
- * Ethics of Cybersecurity

* Mature research (papers available)
* In-progress research (informal initial results)
* Start-up research
A Few Examples of (IC)\(^3\) 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 cybercrime “dark web” ecosystem.
- **Many Others**: Cyberinsurance, Board of Director Cyber Education, Information Sharing, NIST Framework, Tipping Point Analysis, etc. ...
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.
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.

Current State Assessments by Three Companies: Big Differences
Which have largest Gaps?
Top Execs vs Middle Managers vs Professionals

Construct Gaps Absolute Values

(MI-MA by Roles)

Gaps are on average 60% greater for executives & top level managers
Cybersafety: Use of Accident Research to Prevent Cyber Incidents

- Apply “accident” and safety research to “cyber security” failures.
- MIT has researched how to prevent industrial accidents (e.g., 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
Unique Aspects of Attack on Industrial Control Systems

• Real, Physical Damage can occur
• Not always Possible to Convert to Manual Control
• Often the Safety (shut-off) is in Software
  – Which can be turned off or changed
• Failures no Longer Independent
  – If have 8 generators, one might fail mechanically ...
    The other 7 should continue to operated
  – But, a cyber-attack that damages one generated can
    just as easily damage the other 7 at the same time
• “Recovery” from physical damage can take long time
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
Example: Water & Energy Systems

• Familiar with the Maroochy Shire Sewage Spill in Australia in 2000?

• Some (non-obvious) Cybersafety insights:
  – Concerns about insiders (on purpose or accidental) not well addressed. ... Often hear “we are air-gapped, so safe.”
  – Weak oversight and policy/procedures of contract personnel.
    • Role of 3rd party hardware, software, and personnel an increasing concern; often referred to as the “supply chain” vulnerability
  – For 2 months, engineers blamed faults on installation errors.
  – Maroochy Shire City Council lacked Emergency / Contingency response plan to deal with security attacks or sewage release

... Has much actually changed since then?
Example: IT Systems

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

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.

Mar 29, 2007
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 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 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.
Q: Heard of “Bug Bounty” Programs?

- MIT is studying methods of vulnerability detection, such as “bug bounty” programs, using techniques such as System Dynamics modeling
  - Many firms now offer public bug bounty programs, such as 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”
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.
Conclusions

• Increasing automation / computerization:
  – Internet of Things (IoT)
  – e.g., “smart” refrigerator, autonomous cars

• => More attack surfaces

• The worse is yet to come …

• ... but you can be better prepared than others,

• ... but management needs to take the lead.

• Questions?
New project: “Leadership in a Cyber Crisis”

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 Keri Pearlson kerip@mit.edu

This material is based, in part, upon work supported by the MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, (IC)³, and the Department of Energy under Award Number DE-OE0000780. Some of this material was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.