Cybersecurity at MIT Sloan

CAMS Cybersecurity Innovation Symposium

MIT MANAGEMENT SLOAN SCHOOL

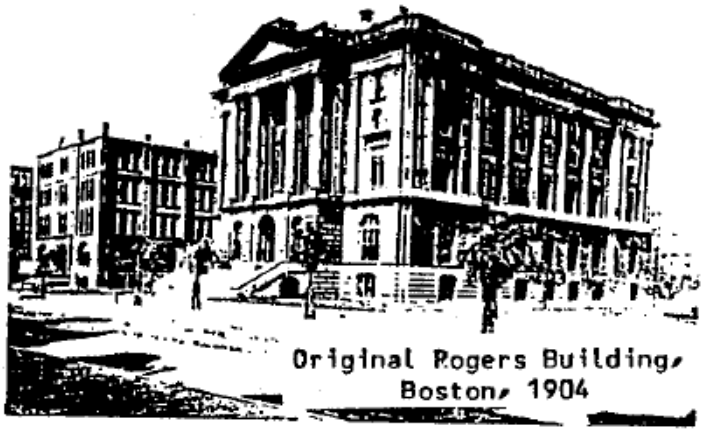
INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (IC)³

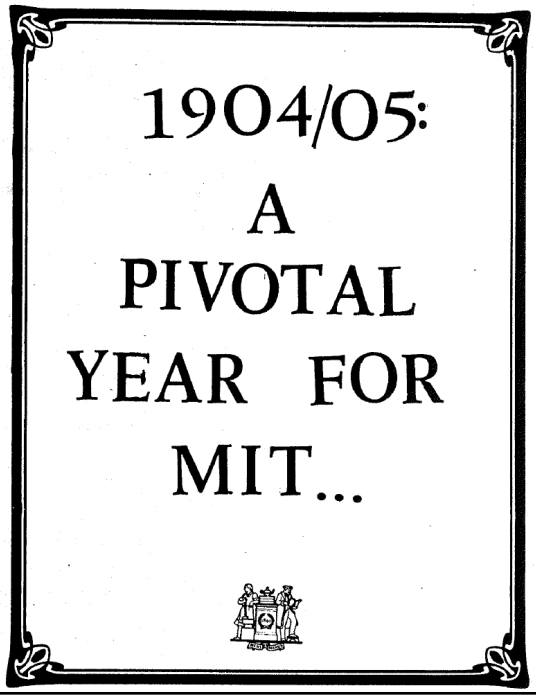
Looking Backward & Looking Forward

Stuart Madnick
John Norris Maguire Professor of Information Technologies,
MIT Sloan School of Management;
Professor of Engineering Systems,
MIT School of Engineering;
Founding Director of Cybersecurity at MIT Sloan (CAMS)
Massachusetts Institute of Technology
smadnick@mit.edu

1

Looking Backward: a hundred years or so





2

Daily Globe.

JUNE 12, 1905—FOURTEEN PAGES.

MOURNING EMBLEM ON ROGERS BUILDING

Expressive of the Feeling of Tech

Q: What is the tragedy?

3

Why ?

Despite the apparent irreconciable differences in educational and ocial attitude, in 1904 Pres. Henry Smith Pritchett began the first ttempt of the twentieth century--but the fourth of Tech's young xistence--to form a merger with Harvard. The chief motive for this ttempt was financial: Tech was in need of money, both to continue perating and to enlarge and/or relocate its physical plant which had ecome too small to support Tech's increasing enrollment. Harvard had eceived under the terms of shoe manufacturer Gordon McKay's will a ubstantial sum to establish a graduate school of engineering within its awrence Scientific School. The apparent solution seemed to be to onsolidate Tech with Harvard, thereby allowing the former to share in ne riches of the McKay legacy and Harvard to benefit by the acquisition f an established and respected school of engineering. A site was osen along the marshy banks of the Charles across from Harvard's mbridge campus (now the site of the Harvard Business School) to which ech would move from its cramped Copley Square location if the merger ook place.

4

What Happened? … a Cliff Hanger!

- Alumni (mostly) not happy!
- But, the MIT Corporation approves the merger!
- But, Mass Supreme Judicial Court rules that MIT CANNOT sell its Boston buildings, since it does not own the land (those funds are needed to build the new campus.)
- So, deal called off.
- So, how did MIT get to its new/current campus in Cambridge in 1916?
- Made possible by a substantial donation from an anonymous donor referred to as "Mr. Smith."
- In January 1920, the identity of the donor was revealed to be George Eastman, founder of Eastman Kodak.

5

Looking Forward: CAMS Research Agenda

Robust CAMS Research Program

Strategy
- Board-level cyber education
- Cybersecurity Impact on International Trade
- Framework for types of cyber education throughout the organization
- Ethics of cybersecurity
- Cyber warfare

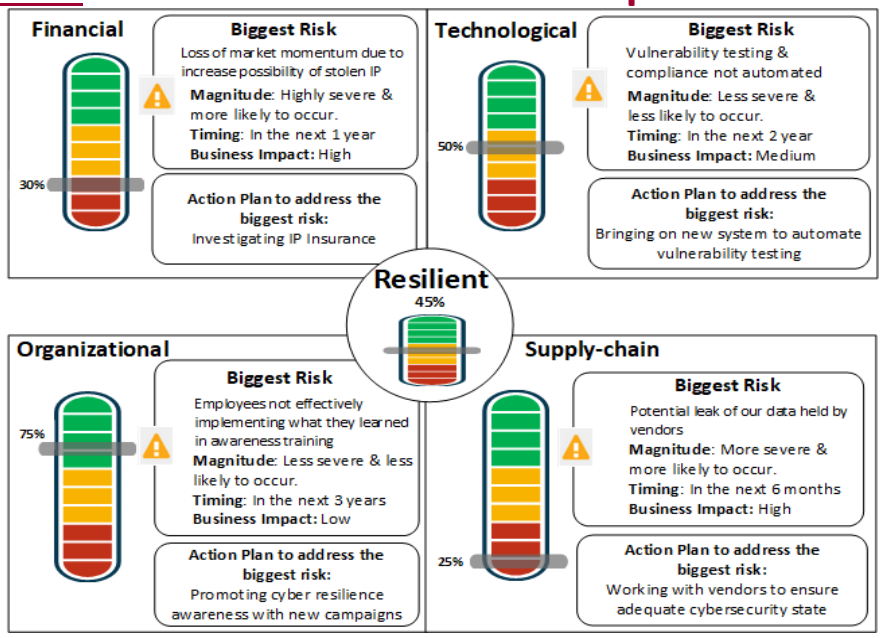
Governance
- Cyber risk evaluation & metrics
- Board governance of cyber
- Cybersecurity leadership in the organization
- Role of cyber insurance in risk mitigation
- Harmonizing compliance and cybersecurity

Management
- Impact of cyber risk concerns on innovations
- Comparing national cybersecurity frameworks
- Usability vs security
- Cyber safety: applying research in accident prevention
- Cybersecurity of Industrial Control Systems (ICS)/Cyber-physical
- Cybersecurity for Cloud-based systems
- Cybersecurity of IoT Using Blockchain
- Autonomous Vehicles

Organizational
- House of Security
- Organizational Cybersecurity Culture
- Bridging the IT/OT Culture Gap
- Success factors for cybersecurity
- Cyber information sharing
- Vulnerability research
- Security workforce

6

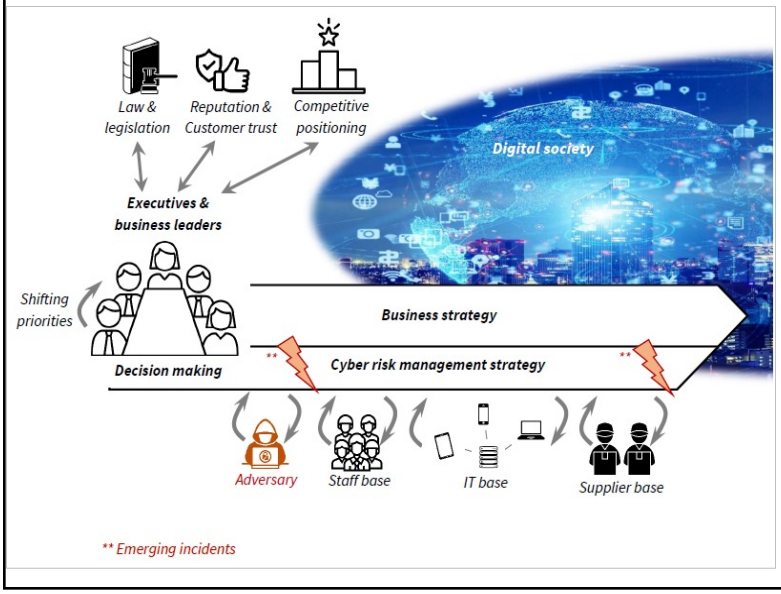
STRATEGY: Balanced Scorecard Concept



Cybersecurity at MIT Sloan

7

GOVERNANCE: Cyber Risk Metrics

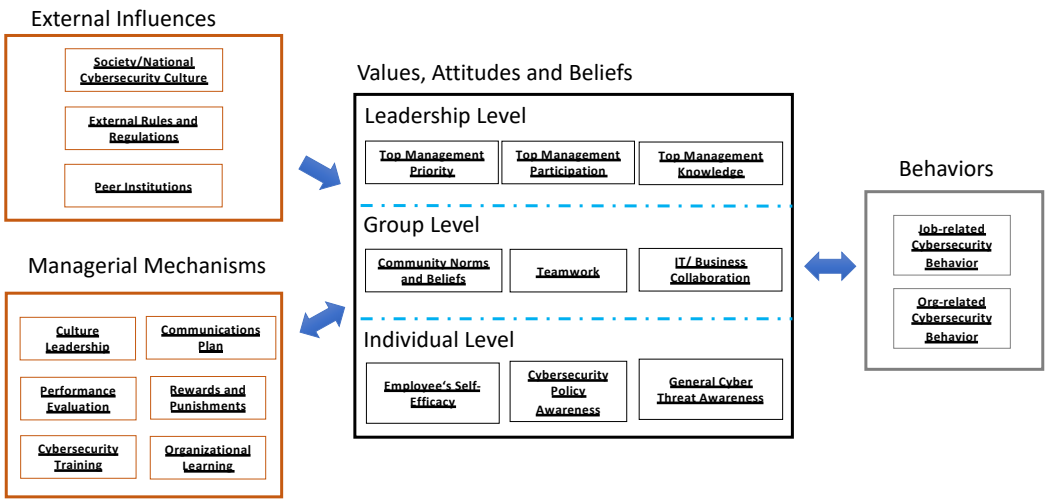


- Grounded in Control Theory and System Dynamics
- +1500 hours of interviews & document analysis
- Validated & back tested over multiple years
- Used at Fortune – 500 company on wide range of strategic cyber challenge
- Contributed to commercial cyber range development

8

8

ORGANIZATIONAL: Cybersecurity Culture Model



9

MANAGEMENT: Cybersafety ("the rest of the story")

EQUIFAX *today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017." **

- How did it happen?
- Oops. Oh, well.
  - Fixed now.
  - No problem.
- In reality,
  one mistake is not enough for a successful breach.


ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

BIZ & IT —

Failure to patch two-month-old bug led to massive Equifax breach

Critical Apache Struts bug was fixed in March. In May, it bit ~143 million US consumers.

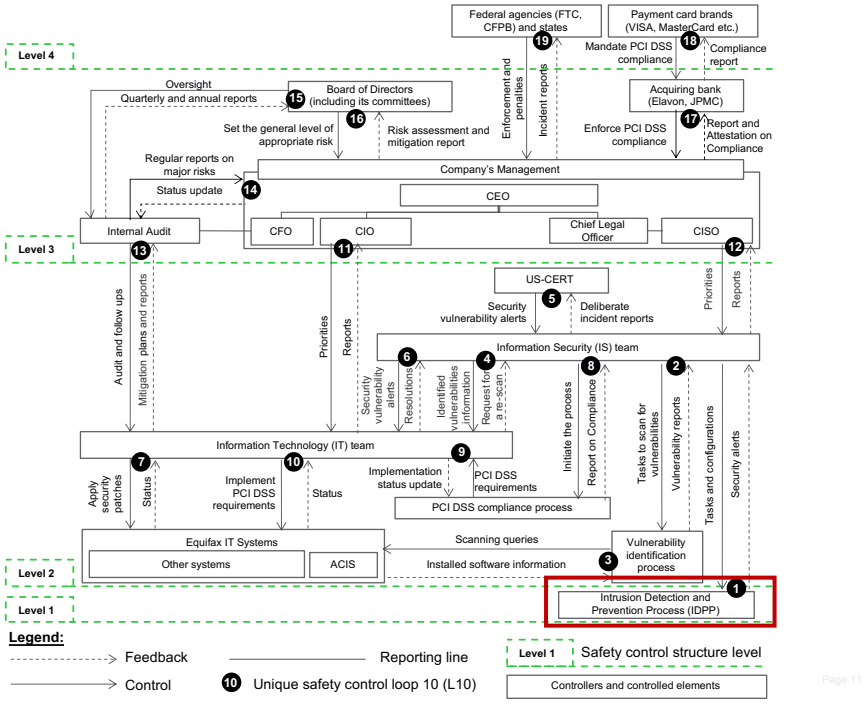
DAN GOODIN - 9/13/2017, 11:12 PM

10

EQUIFAX HIERARCHICAL SAFETY CONTROL STRUCTURE

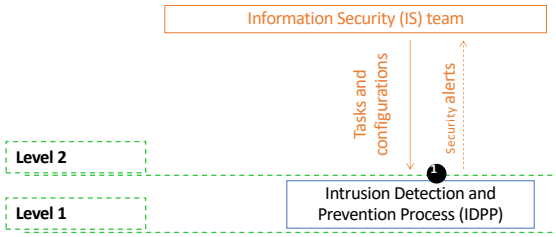
With Control Loops Identified

- We identified 19 control failures at all levels of the organization!



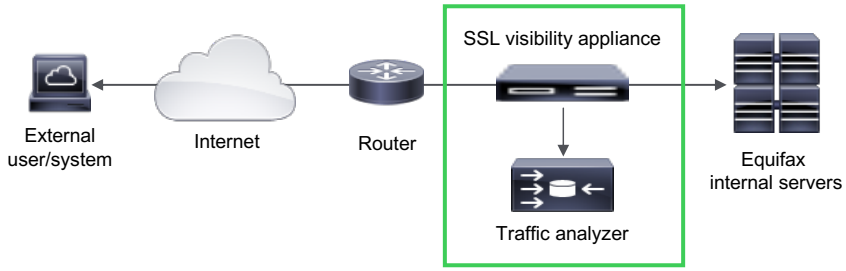
11

LEVEL 1 – Intrusion Detection and Prevention Process (IDPP)



- SSL certificates expired in November 2016
- IDPP was "blind" for almost nine months (until July 29, 2017, after the breach)

Known issues with the manual SSL certificate update process since 2016, but it was not a priority….



- We identified 18 other control failures at other levels of the organization!
- **The incident cost Equifax over $1 billion!**

12

IMPACTS ALL FOUR: New Cybersecurity Regulations

New: Tracking over 170 new regulations …

Common components …

1. *Required Software Bill of Materials (SBOM) by CISA*
2. *Restrictions on Paying Ransomware*
3. *Require "Secure by Design"*
4. *Data Governance*
5. *Required Incident Reporting*
6. **Information Exchange**
7. **Critical Infrastructure Protection**
8. **Supply Chain**
9. **Data Privacy**
10. **Cybersecurity for Emerging Technologies**
11. **Internal Protocols and Practices for Cybersecurity Hygiene**
12. **Risk Assessment and Management**
13. **Operational Resilience Regulations**
14. **Cross-Border Data Transfer Regulations**
15. **Cybersecurity Governance and Leadership**
16. **Cybersecurity Whistleblower Protection Regulations**
17. **Regulations on Cybersecurity Preparedness**
18. **Cybersecurity Regulations for National Security and Public Safety**

13

13

Opportunities for Collaboration with CAMS

- Many more projects … new ones being formed all the time.
- Tremendous mutual benefits from collaborative research.
- Talk to any of us about opportunities: Stuart, Michael, or Keri

- **Be sure to look at the posters for examples of current projects.**

14