Cutting Edge Cybersecurity Leadership Research at MIT's Sloan School

Dr. Keri Pearlson, Dr. Keman Huang and Matt Maloney

SIM Boston Summit • October 23, 2018

CAMS - (IC)³ • https://cams.mit.edu

Cybersecurity at MIT Sloan

200,000 Security events

"The average company handles a bombardment of 200,000 security events a day"

89% of companies say they have been the victim of a cyber attack in the last 12 months. 1 in 3 say they have been hacked more than 5 times in the past year.

2

Source: Harvard Business Review, "Cybersecurity has a serious talent shortage and here's how to fix it", Posted online May 4, 2017

84%

The percent of cyber attacks due to unsafe human behaviors
(such as using easy-to-guess passwords, leaving physical devices in an unsafe areas, failing to apply a patch)

Source: https://securityintelligence.com/news/insider-threats-account-for-nearly-75-percent-of-security-breach-incidents/

3

Cybersecurity is a Big Problem

Cybersecurity at MIT Sloan

- ➔ The Good Guys are good, but the Bad Guys are getting better faster
- ➔ The incidents are increasing in sophistication, frequency and costs
- ➔ Organizations are inadequately prepared
- ➔ Recovery is costly and resource intensive, if even possible

Our BHAG (Big, Hairy Audacious Goal):
Make the Digital World Safe From Cyber Threats

4

Cybersecurity at MIT Sloan

We are a Consortium dedicated to understanding the organizational, managerial, and strategic aspects of cybersecurity.

We do research, teach, publish, and hold events to share our findings and build community.

We were founded by Professor Stuart Madnick and Dr. Michael Siegel in 2015.

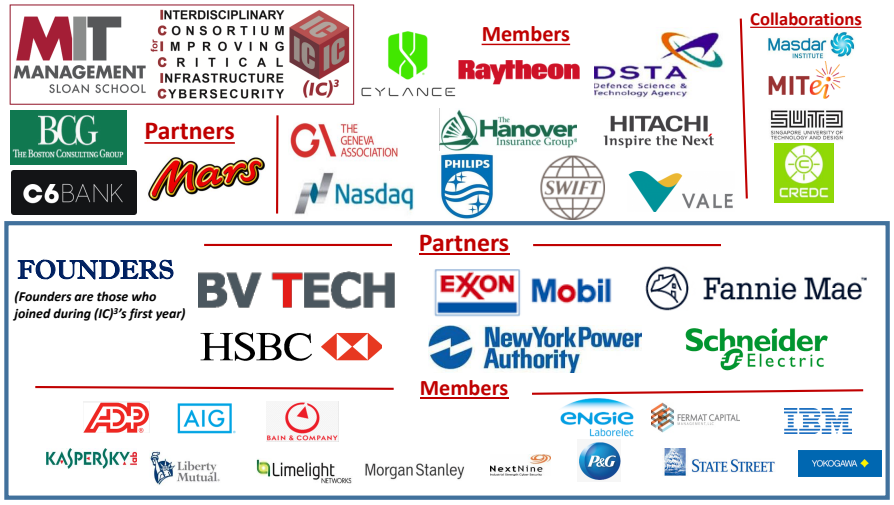
5

We are Interdisciplinary Crossing Schools at MIT (Partial List)

- **Stuart Madnick** – Professor of IT, **MIT Sloan School of Management** and Professor of Engineering Systems, **MIT School of Engineering**
- **Michael Siegel** – Principal Research Scientist, **MIT Sloan School of Management**
- **Nazli Choucri** – Professor of Political Science, **MIT School of Humanities & Social Sciences**
- **Andrew Lo** – Professor of Financial Engineering, **MIT Sloan School of Management**
- **John Williams** – Professor of Civil & Environment Engineering, **MIT School of Engineering**
- **Simon Johnson-** Professor of Entrepreneurship, **MIT Sloan School of Management**
- **John Carroll-** Professor of Entrepreneurship, **MIT Sloan School of Management**
- **David Clark** – Senior Research Scientist, **Computer Science & Artificial Intelligence Laboratory**
- **Michael Coden –** Research Affiliate (former member of **White House cyber study**)
- **Jerrold Grochow** – Research Affiliate (**former MIT CIO** and member of MITei cyber study)
- **James Kirtley** – Professor of Electrical Engineering, **MIT School of Engineering**
- **Keri Pearlson** – Executive Director of (IC)³, **MIT Sloan School of Management**
- **Mohammad Jalali** – Research Scientist, **MIT Sloan School of Management**
- **Keman Huang** – Research Scientist, **MIT Sloan School of Management**
- **Matt Maloney** – Research Scientist, **MIT Sloan School of Management**

6

We are International and Cross-Industry (Partial List)



7

Robust CAMS Research Program

Governance

- Cyber risk evaluation & metrics
- Board governance of cyber
- Cybersecurity leadership in the organization
- Role of cyber insurance in risk mitigation

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

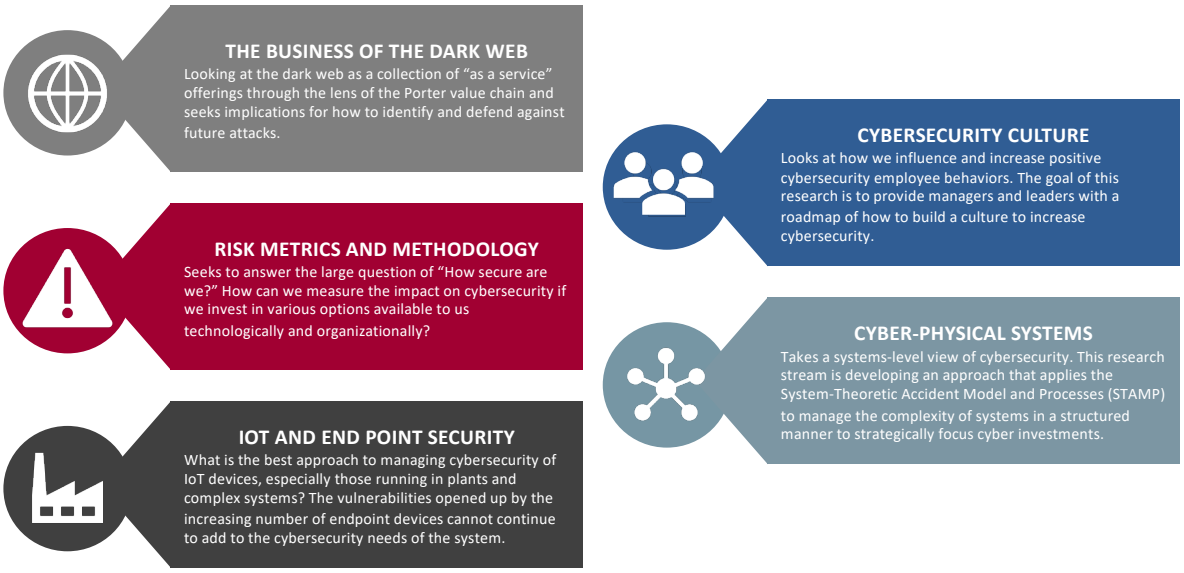
Strategy

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

Organizational

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

Our research priorities for this year



CAMS Research: *Business Innovation in the Cyber Attack Ecosystem*

Cybersecurity at MIT Sloan

Dr. Keman Huang, Dr. Michael Siegel, Dr. Keri Pearlson and Prof Stuart Madnick

Research Question:

How can hackers operate cyber attack as a business?

Why Cyber Attack Business?

Cybersecurity at MIT Sloan

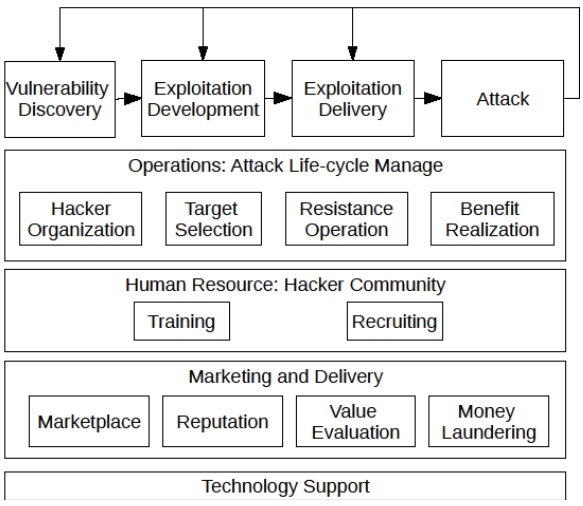
- Cybersecurity is still a game of cat and mouse
- Technologies are good and getting better, but the criminals are getting better faster
  - 2016: DDoS
  - 2017: Ransomware
  - 2018: Cryptojacking
- How to operate a cyber attack? → Rethink the combat strategy.

Dark Web: Cyber Attack Value Chain

Cybersecurity at MIT Sloan

HOBBY VS. BUSINESS

Cyber Threat Capability Supply Chains: consists of not only the primary attack activities, but also the support activities to facilitate the cyber-attack.



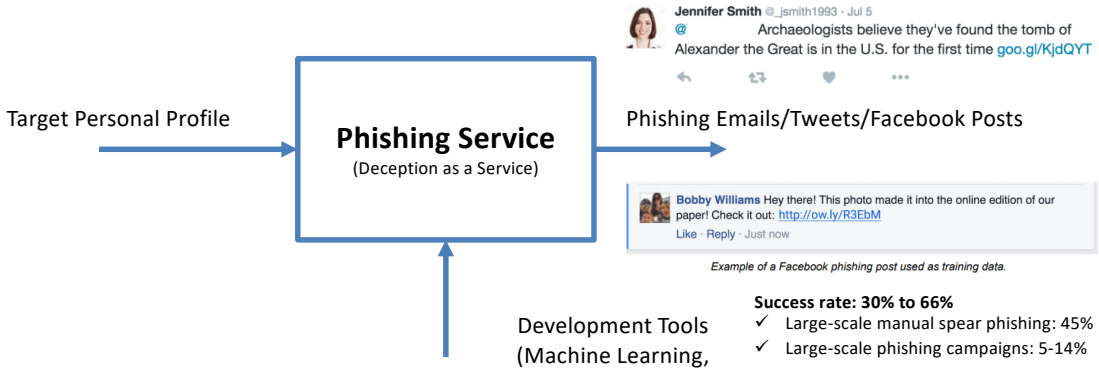
Primary Activities: Attack

Support Activities: Less cost for higher benefit

Cyber Attack as a Service

Cybersecurity at MIT Sloan

Specialization, Commercialization , Collaboration



Example of a Facebook phishing post used as training data.

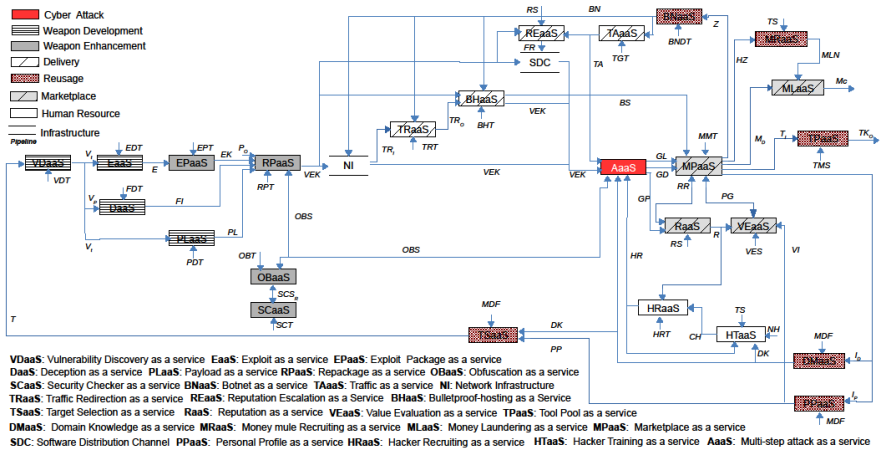
Success rate: 30% to 66%

- ✓ Large-scale manual spear phishing: 45%
- ✓ Large-scale phishing campaigns: 5-14%

Black Hat USA 2016, Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter, https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf

Cyber Attack Service Ecosystem

Cybersecurity at MIT Sloan



VDaaS: Vulnerability Discovery as a service **EaaS**: Exploit as a service **EPaaS**: Exploit Package as a service
DaaS: Deception as a service **PLaaS**: Payload as a service **RPaaS**: Repackage as a service **OBaaS**: Obfuscation as a service
SCaaS: Security Checker as a service **BNaaS**: Botnet as a service **TAaaS**: Traffic as a service **NI**: Network Infrastructure
TRaaS: Traffic Redirection as a service **REaaS**: Reputation Escalation as a Service **BHaaS**: Bulletproof-hosting as a Service
TSaaS: Target Selection as a service **RaaS**: Reputation as a service **VEaaS**: Value Evaluation as a service **TPaaS**: Tool Pool as a service
DMaaS: Domain Knowledge as a service **MRaaS**: Money mule Recruiting as a service **MLaaS**: Money Laundering as a service **MPaaS**: Marketplace as a service
SDC: Software Distribution Channel **PPaaS**: Personal Profile as a service **HRaaS**: Hacker Recruiting as a service **HTaaS**: Hacker Training as a service **AaaS**: Multi-step attack as a service

24 Key Components: Complex, Reinforcement

Cybercrime will become quicker, cheaper, more targeted, more scalable, and more difficult to be considered as crime

Cyber Attack Service Composition

Cybersecurity at MIT Sloan

DDoS Attack

Component	Service Status
Traffic Generation	Existing
Botnet	Existing

Ransomware Attack

Component	Service Status
Payload: Ransomware	Existing
Botnet	Existing
Bulletproof Server	Existing
Exploit Package	Emerging
Traffic Redirection	Existing
Hacker Recruiting	Evolving
Obfuscate	Existing
Money Laundering	Existing

Cryptojacking Attack

Component	Service Status
Payload: Crypto-mining	Existing
Botnet	Existing
Bulletproof Server	Existing
Exploit Package	Emerging
Traffic Redirection	Existing
Hacker Recruiting	Evolving
Obfuscate	Existing
Money Laundering	Existing

Cyber Attack Business Research Next Steps

Cybersecurity at MIT Sloan

Some insights so far

- Cyber-attackers are well-organized & business models are well-defined
- Cyber-Attack-as-a-Service is providing an understanding of innovations taking place on the dark web

Next steps:

- What is the best/most common business model for cyber attacks?
- How can we rethink combat strategy? Should companies compete? “Attack back”?

CAMS Research:
Securing Industrial IoT Devices

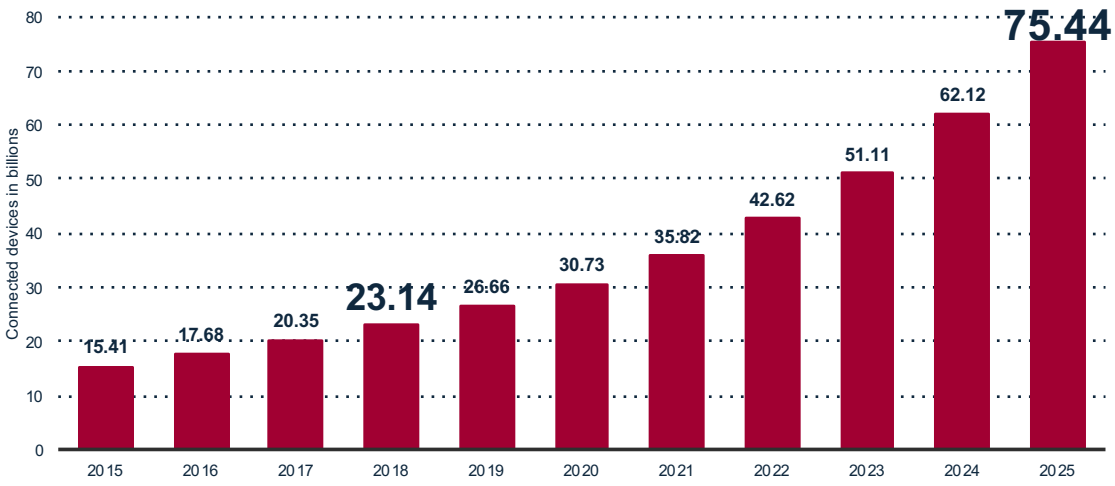
Cybersecurity at MIT Sloan

Matt Maloney, Eliza Riley, Dr. Greg Falco, Dr. Michael Siegel, and Prof Stuart Madnick

Research Question:

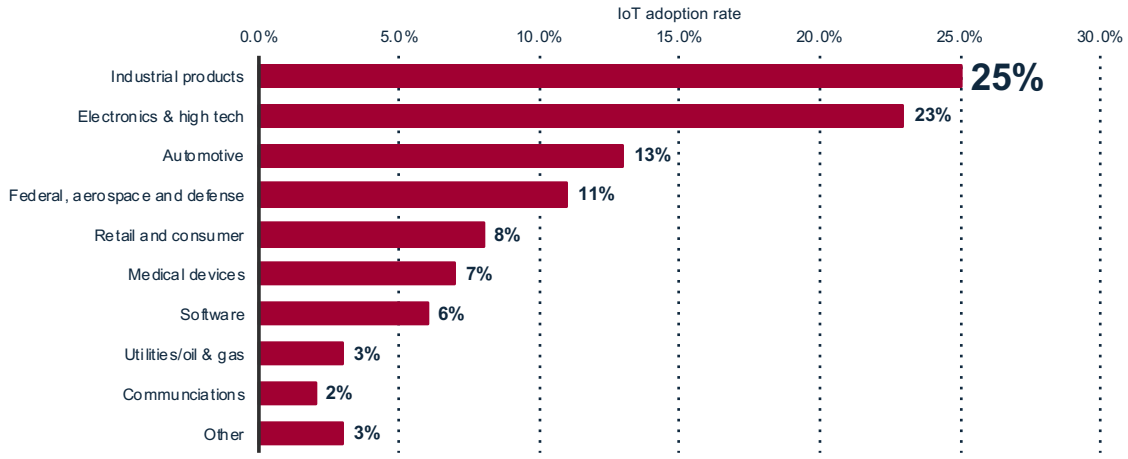
How do we secure industrial IoT devices?

Internet of Things – devices worldwide from 2015 to 2025 (in billions)



IHS. (n.d.). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). In *Statista - The Statistics Portal*. Retrieved October 16, 2018, from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

Industrial IoT adoption worldwide as of 2017, by industry



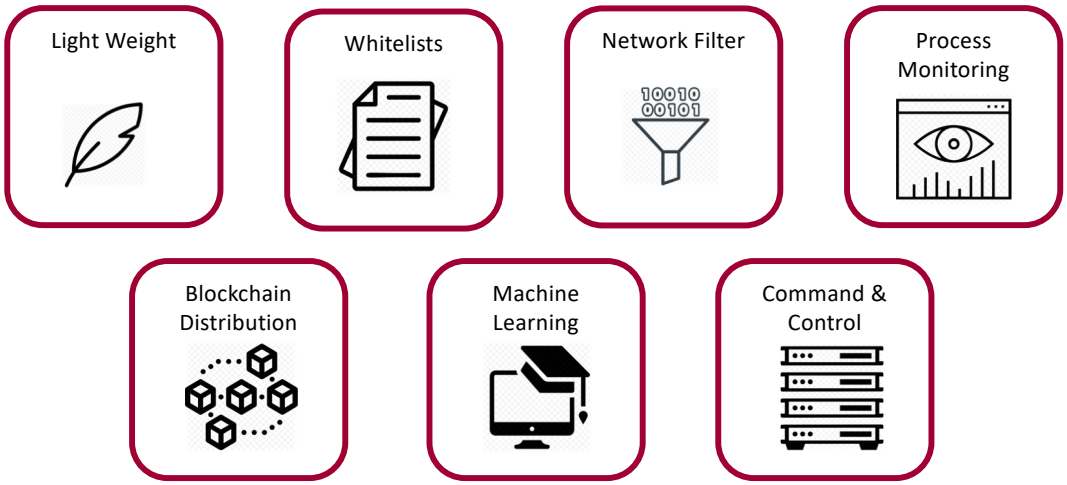
Various sources. (n.d.). Industrial IoT adoption worldwide as of 2017, by industry. In *Statista - The Statistics Portal*. Retrieved October 16, 2018, from https://www.statista.com/statistics/797392/industrial-iot-adoption-worldwide-by-industry/.

Research Question

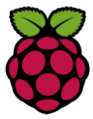
How do we secure industrial IoT devices?

Research Aim

Develop a working prototype of the security agent that can be run on a range of industrial devices

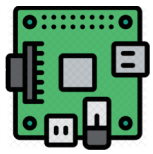


Research Methodology & Roadmap



Phase 1

- Development of Proof of Concept



Phase 2

- Test bed deployments with national labs

Phase 3

- Build models for intelligent whitelisting

IoT Research Next Steps

Cybersecurity at MIT Sloan

Key insights so far

- We have shown that a lightweight tool can be applied to many IoT devices using whitelists
- The code handles both network filtering and process monitoring

Next steps:

- Apply blockchain technology for secure communications and information dissemination
- Use machine learning to intelligently configure security in devices

CAMS Research:
Cyber Security for International Trade

Cybersecurity at MIT Sloan

Dr. Keman Huang, Prof Stuart Madnick and Prof Simon Johnson

Research Question:

How do Cybersecurity Concerns Impact International Trade?

Background & Motivation

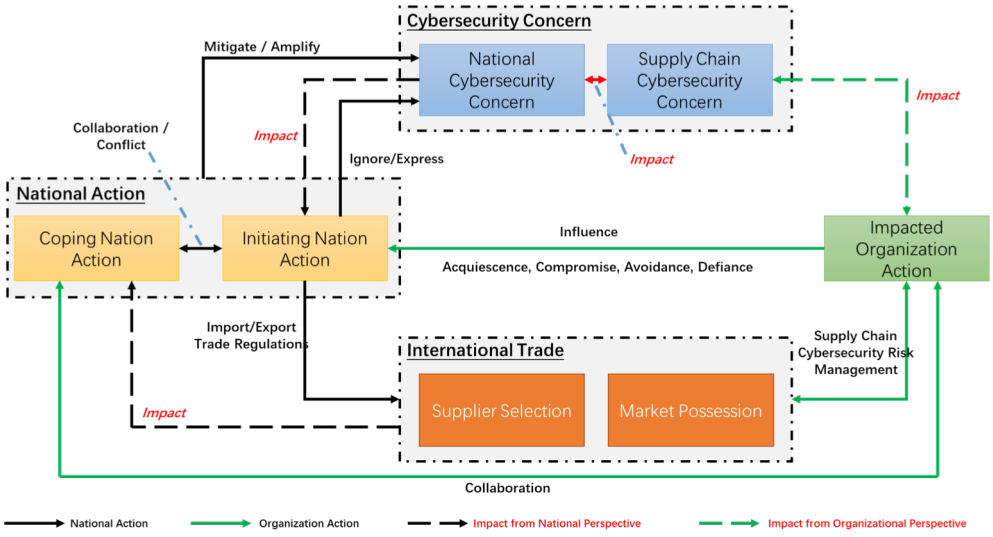
Cybersecurity at MIT Sloan

Cybersecurity issues impact the international trade relations. We want to know ***How, Why*** **and** ***What*** **can be done to reduce negative impact (and improve positive impact).**

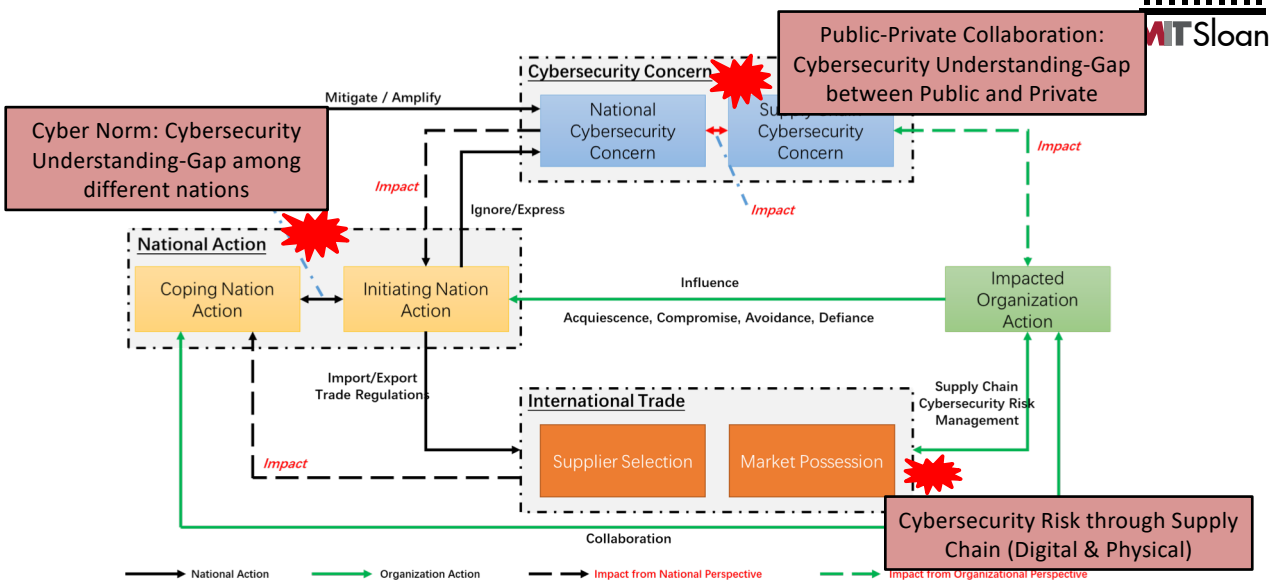
- What are the cybersecurity impacts on the international trade?
- How do cybersecurity impact the international trade evolve?
- What can managers and legislators do to mitigate or prepare for impact?

Model of How Cybersecurity Impacts International Trade

Cybersecurity at MIT Sloan



Gaps in International Trade Model Create Concerns



Interview Data Supports the Concern About the Gaps

Supply Chain Cybersecurity Management (Private)	Public-Private Collaboration (Public-Private)	International Cyber Norm (Public-Public)
"To ensure they work with suppliers better, [A] has a cybersecurity document used during the supplier onboarding process. Unless supplier practices are ascertained, they do not start business with them." "Industry hasn't come up with a good solution. More problematic aspects of supply chain is that distributed IOT devices in remote parts of the world can make them much more vulnerable."	"At an industry level, it can manifest as tampering with our supply chain or counterfeit parts to ultimately impact our war strategy." "On the contrary, the US private sector is extremely suspect of the Government. If these two could talk, there could be better measured responses than ad-hoc." "In some cases there are cyber security response centers that could be based on Public Private Partnerships. These are beneficial, especially for the small company or organizations because they cannot afford expensive procedures."	"In such scenarios, like the Geneva convention for War, we need a baseline convention for Cybersecurity" "Can there be a global, mutual agreement on we will only go this far?"

28

International Trade Research Next Steps

Cybersecurity at MIT Sloan

Insights so far

- We have a general model of how cybersecurity concerns impact international trade (and support to validate this model)
- Clear gaps exist and must be addressed to mitigate cyber risk
  - Cyber norms within and between nations
  - Public/Private collaboration needs and actions
  - Supply Chain expectations and reality

Next Steps

- Look into cybersecurity concerns in the global financial supply chain
- Create a cyber-norm / consensus mechanism

CAMS Research: Building a Culture of Cybersecurity

Cybersecurity at MIT Sloan

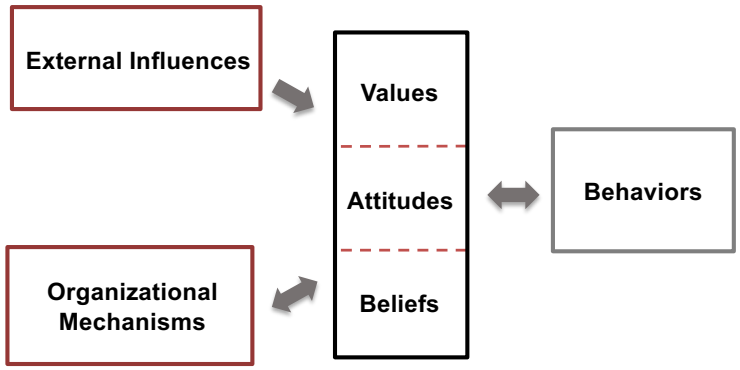
Dr. Keri Pearlson, Dr. Keman Huang, and Gillian McGuire

Research Question:

How can we create a strong cybersecurity culture in our organizations?

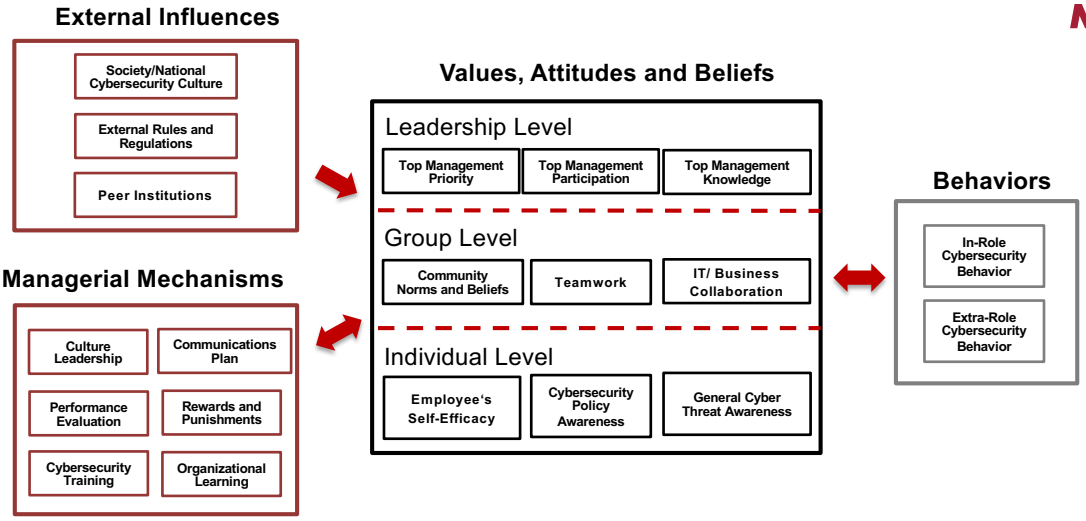
Cybersecurity Culture Model

Cybersecurity at MIT Sloan



Cybersecurity Culture Model

Cybersecurity at MIT Sloan



Culture Research Next Steps

Cybersecurity at MIT Sloan

Insights so far:

- Managerial decisions and org design will influence values, attitudes and beliefs which drive behaviors
- Changing behaviors means changing values, attitudes and beliefs about cybersecurity

Our next steps:

- Validate the model
- Look at different levels of culture maturity

http://bit.ly/mit_isc2_culture

Wrap Up: High Impact Research

Cybersecurity at MIT Sloan

THE BUSINESS OF THE DARK WEB
The Dark Web is a well-structured
set of "as a ser
Looking throug
provide new
an

IOT AND END POINT SECURITY
IoT opens up numerous new
cybersecurity v
Our approach
to protect fro
cyb

CYBERSECURITY CONCERNS IN INTERNATIONAL TRADE
Understanding how Nation
States make dec
ipotentially imp
will l
ma

CYBERSECURITY CULTURE
Managers have mechanisms to influence the values, attitudes and beliefs of their employees which in turn drive cybersecure behaviors

Call to Action: Join Our Consortium!

Cybersecurity at MIT Sloan

Join us! Our research is supported by leaders like you who join our consortium.

Join us at: https://cams.mit.edu

Dr. Stuart Madnick
smadnick@mit.edu

Dr. Michael Siegel
msiegel@mit.edu

Dr. Keri Pearlson
kerip@mit.edu

Matt Maloney
maloneym@mit.edu

Dr. Keman Huang
keman@mit.edu

THANK YOU!