(ISC)²

SECURITY CONGRESS 2018

ENRICH
ENABLE
EXCEL

congress.isc2.org
#ISC2Congress

Creating a Cybersecurity Culture: (ISC)² Survey Responses

Dr. Keri Pearlson

(ISC)² Conference • October 8, 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.

3

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/*

4

Cybersecurity is a Big Problem

- 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

5

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.

6

We are Interdisciplinary Crossing Schools at MIT (Partial List)

Cybersecurity at MIT Sloan

- **Stuart Madnick** – Professor of Information Technologies, **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**

7

We are International and Cross-Industry (Partial List)

MIT Management Sloan School — Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)^3

Members: Cylance, Raytheon, DSTA Defence Science & Technology Agency

Collaborations: Masdar Institute, MITei, SUTD Singapore University of Technology and Design, CREDC

Partners: BCG The Boston Consulting Group, C6 Bank, Mars, The Geneva Association, Nasdaq, The Hanover Insurance Group, Philips, SWIFT, Hitachi Inspire the Next, Vale

Partners

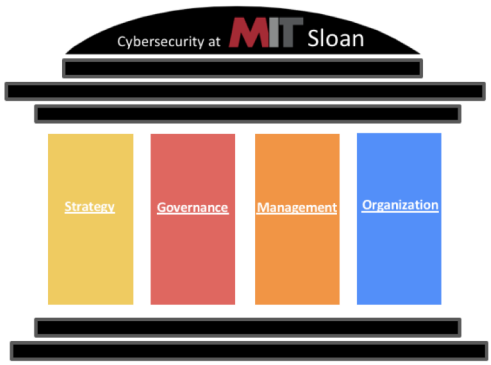
FOUNDERS *(Founders are those who joined during (IC)^3's first year)*: BV TECH, HSBC, ExxonMobil, Fannie Mae, New York Power Authority, Schneider Electric

Members

ADP, AIG, Bain & Company, Engie Laborelec, Fermat Capital, IBM, Kaspersky Lab, Liberty Mutual, Limelight Networks, Morgan Stanley, NextNine, P&G, State Street, Yokogawa

8

CAMS Research Framework



Governance

- Cyber safety: applying research in accident prevention
- Cybersecurity of Industrial Control Systems (ICS)
- Moving to the Cloud
- Cybersecurity of IoT & Autonomous Vehicles
- Comparison of international cyber information sharing processes
- Vulnerability research

Management

- Board governance of cyber
- Board-level cyber education
- Cybersecurity leadership in the organization
- Cyber risk evaluation & metrics

Strategy

- House of Security
- Organizational Cybersecurity Culture
- Bridging the IT/OT Culture Gap
- Framework for types of cyber education throughout the organization
- Ethics of cybersecurity
- Security workforce

Organization

- Cybersecurity Impact on International Trade
- Impact of cyber risk concerns on innovations
- Role of cyber insurance in risk mitigation
- Comparing national cybersecurity frameworks
- Usability vs security
- Success factors for cybersecurity
- Cyber warfare

Our research priorities for this year

THE BUSINESS OF THE DARK WEB
Looking at the dark web as a collection of "as a service" offerings through the lens of the Porter value chain and seeks implications for how to identify and defend against future attacks.

RISK METRICS AND METHODOLOGY
Seeks to answer the large question of "How secure are we?" How can we measure the impact on cybersecurity if we invest in various options available to us technologically and organizationally?

IOT AND END POINT SECURITY
What is the best approach to managing cybersecurity of IoT devices, especially those running in plants and complex systems? The vulnerabilities opened up by the increasing number of endpoint devices cannot continue to add to the cybersecurity needs of the system.

CYBERSECURITY CULTURE
Looks at how we influence and increase positive cybersecurity employee behaviors. The goal of this research is to provide managers and leaders with a roadmap of how to build a culture to increase cybersecurity.

CYBER-PHYSICAL SYSTEMS
Takes a systems-level view of cybersecurity. This research stream is developing an approach that applies the System-Theoretic Accident Model and Processes (STAMP) to manage the complexity of systems in a structured manner to strategically focus cyber investments.

CAMS Research

Cybersecurity at MIT Sloan

Organizational Cybersecurity Culture Research
Dr. Keri Pearlson, Dr. Keman Huang, and Gillian McGuire

Research Question:

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

Help Us Validate Our Model

Cybersecurity at MIT Sloan

http://bit.ly/mit_isc2_culture

Defining Cybersecurity Culture

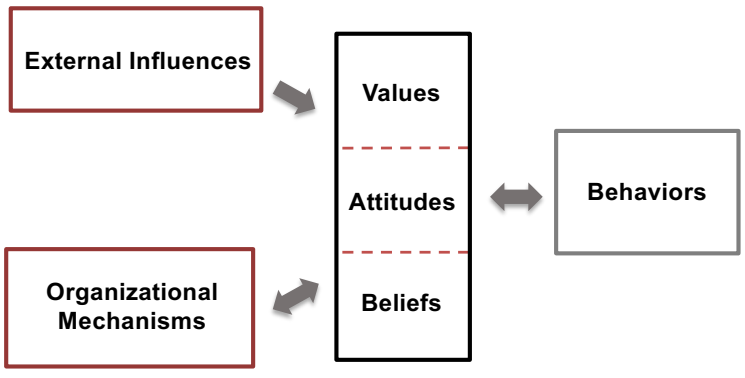
Cybersecurity at MIT Sloan

- Culture: The **Attitudes**, **Beliefs**, and **Values** (unwritten rules) that drive **Behaviors** in an organization

- Cybersecurity Culture: the attitudes, beliefs and values that drive behaviors to create cybersecurity in an organization

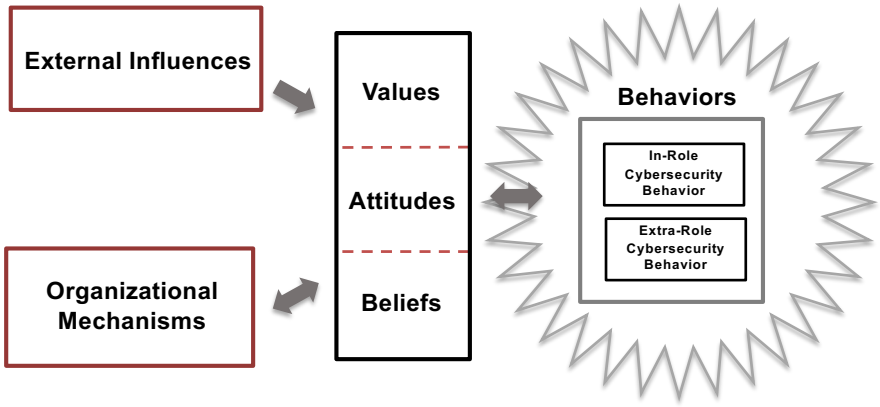
Cybersecurity Culture Model

Cybersecurity at MIT Sloan



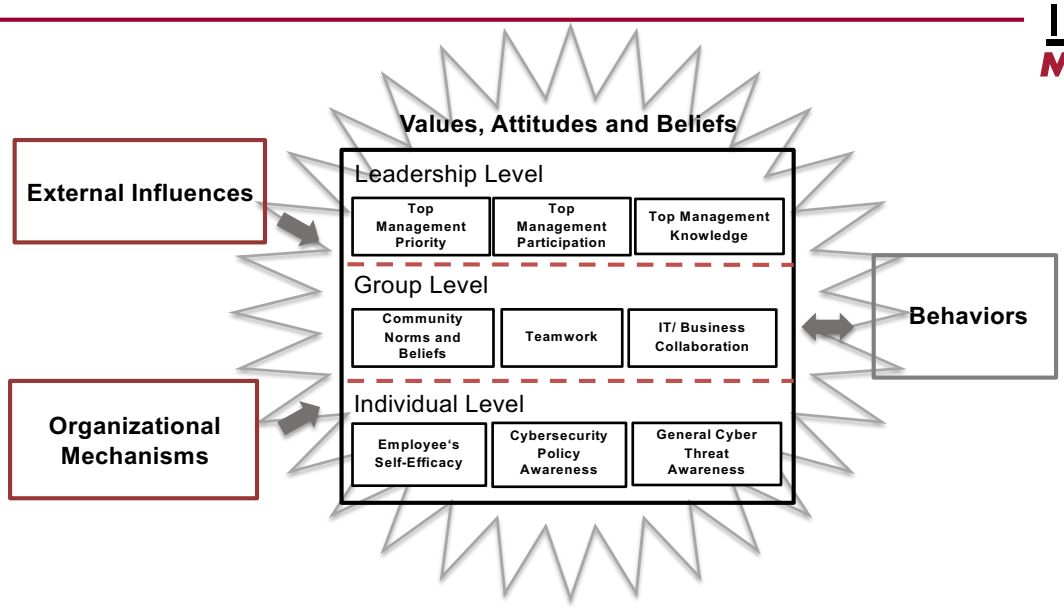
Cybersecurity Culture Model

Cybersecurity at MIT Sloan



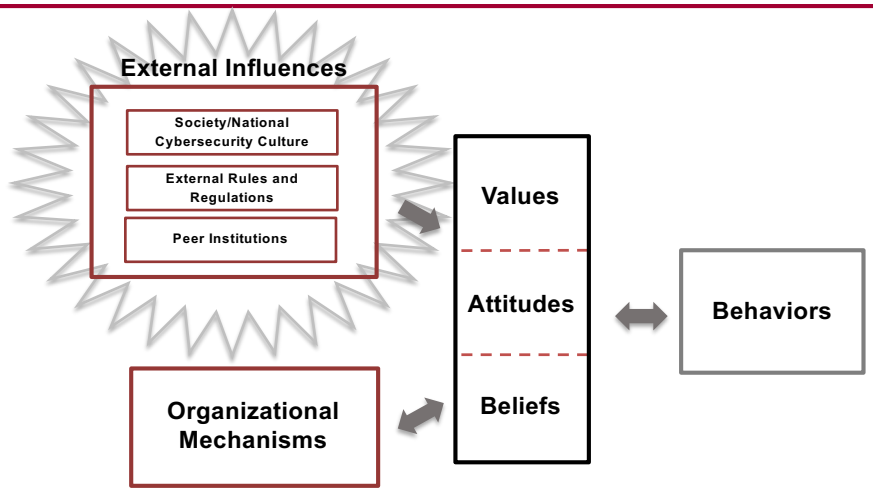
Cybersecurity Culture Model

Cybersecurity at MIT Sloan



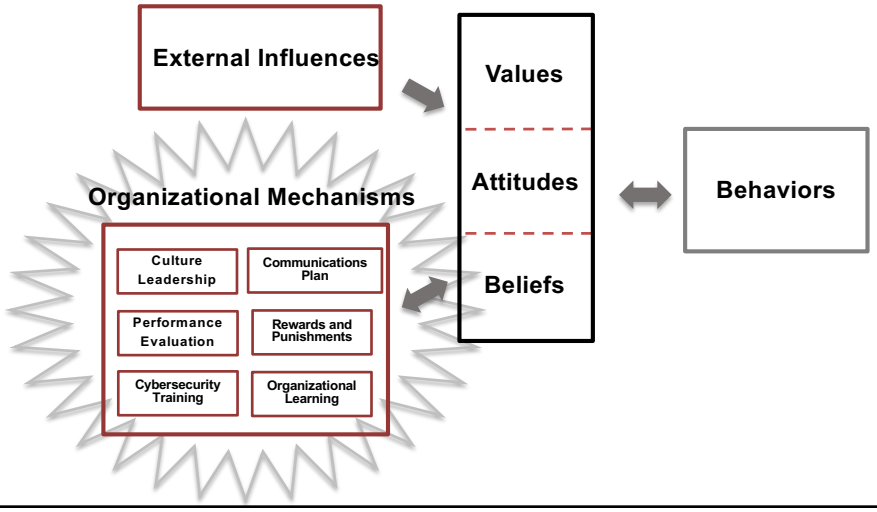
Cybersecurity Culture Model

Cybersecurity at MIT Sloan



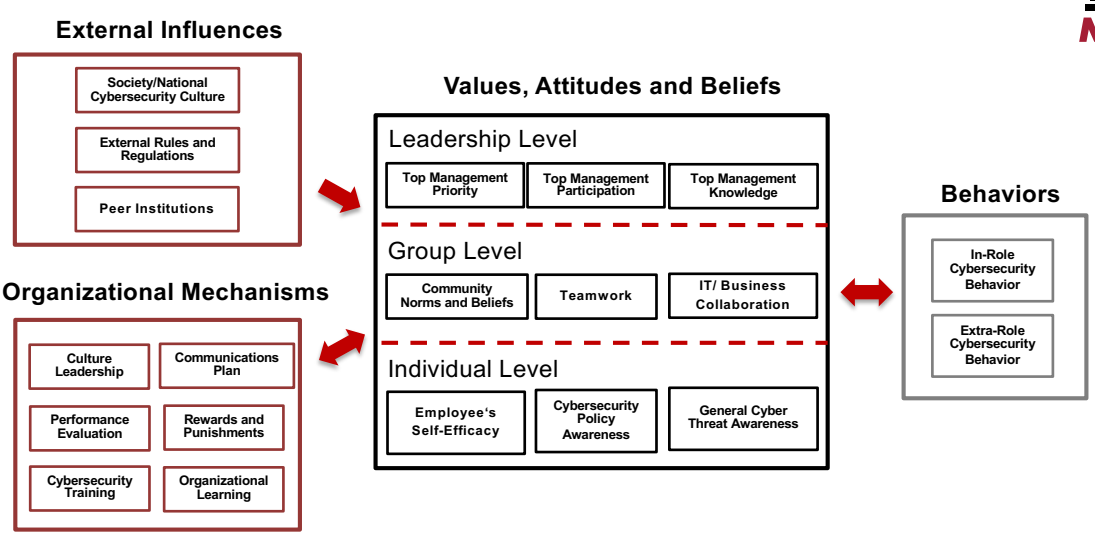
Cybersecurity Culture Model

Cybersecurity at MIT Sloan



Cybersecurity Culture Model

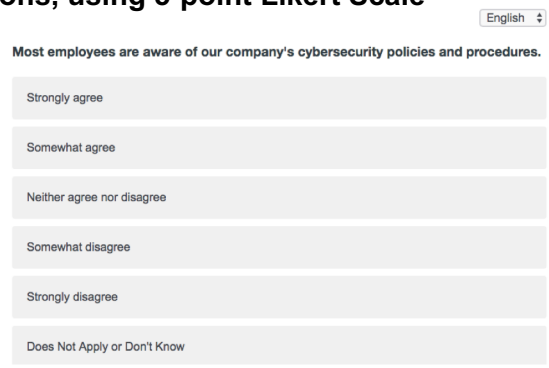
Cybersecurity at MIT Sloan



We Were Invited to Post a Survey on (ISC)^2 Website

Cybersecurity at MIT Sloan

- **Survey created on Qualtrics to assess the constructs in the model**
  - **25 questions, using 5-point Likert Scale**



  - **General demographic questions (industry, company size, etc.)**
  - **Received 50 responses from (ISC)^2 community**

The Respondents

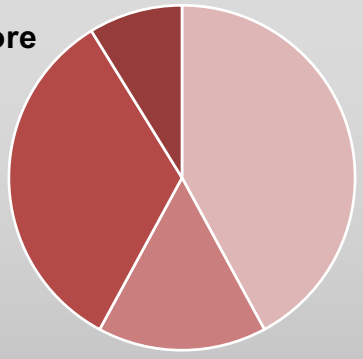
Cybersecurity at MIT Sloan

19 states and 12 countries represented

83% of subjects work at mature companies

Many Industries

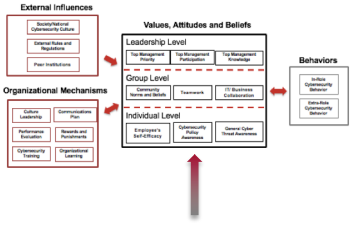
Large Companies of 5000 or More



Raise Your Hand if you Agree:

Cybersecurity at MIT Sloan

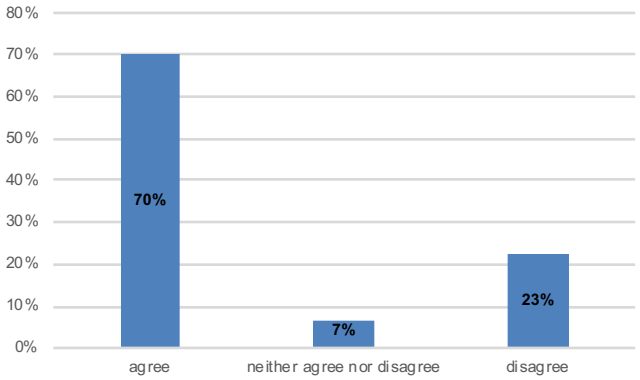
Cybersecurity is an important part of our company's strategy.

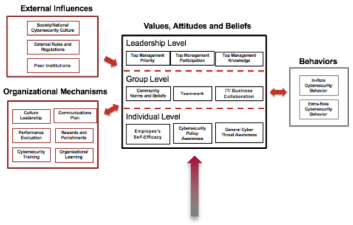


Survey Responses

Cybersecurity at MIT Sloan

Cybersecurity is an important part of our company's strategy.

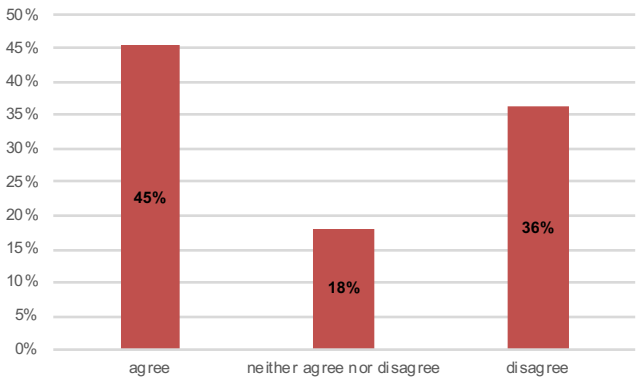


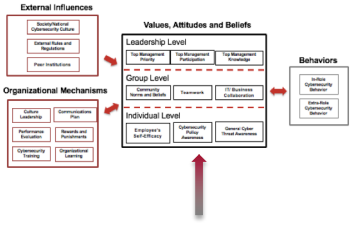


Survey Responses

Cybersecurity at MIT Sloan

Our employees have the skills and capabilities they need to follow our cybersecurity rules and procedures

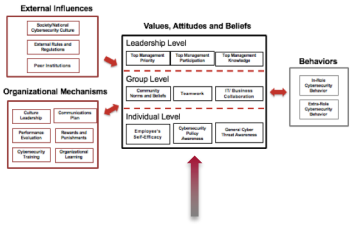




Raise Your Hand if You Agree:

Cybersecurity at MIT Sloan

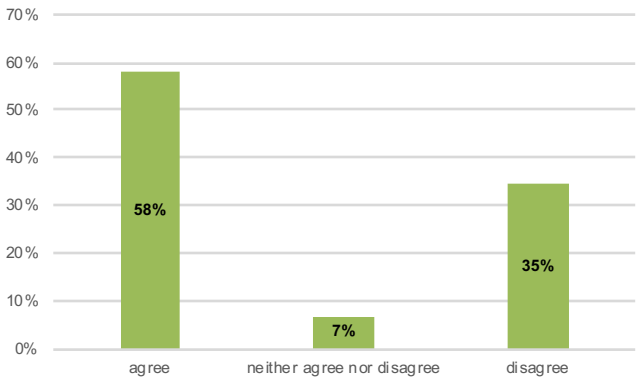
It is difficult for our cybersecurity team and business units to work together to improve cybersecurity.

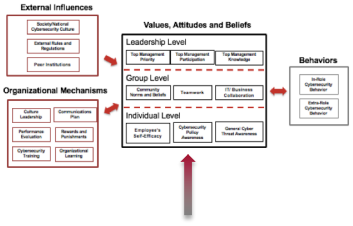


Survey Responses

Cybersecurity at MIT Sloan

It is difficult for our cybersecurity team and business units to work together to improve cybersecurity.

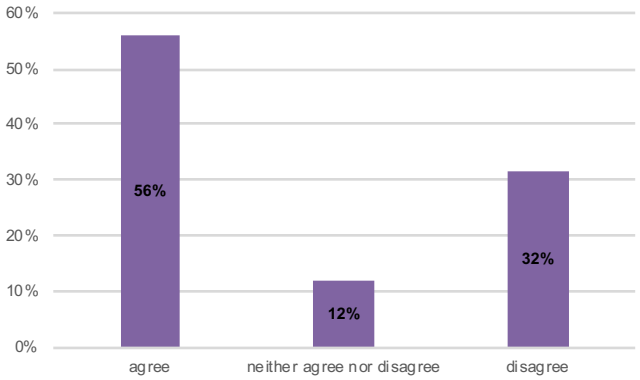


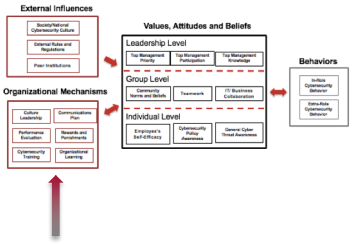


Survey Responses

Cybersecurity at MIT Sloan

We get regular communications from our cybersecurity team about prevention, incidents, and/or responses.

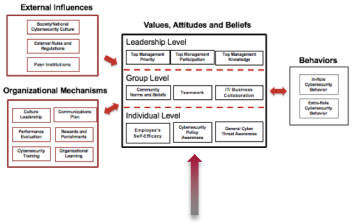




Raise Your Hand if You Agree:

Cybersecurity at MIT Sloan

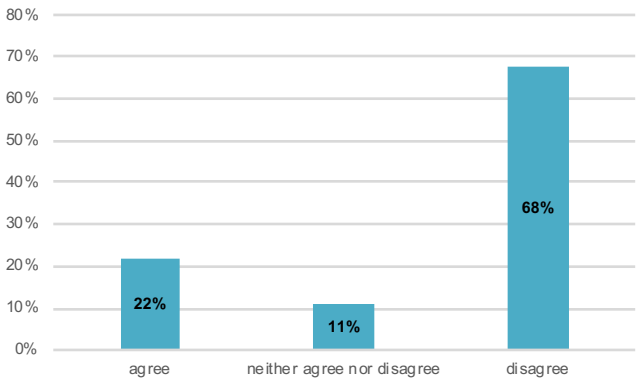
Part of our performance review includes an assessment of whether or not we follow proper cybersecurity guidelines.

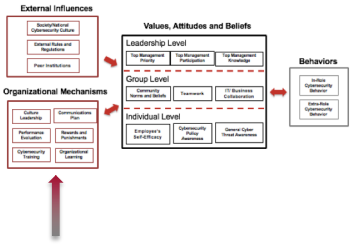


Survey Responses

Cybersecurity at MIT Sloan

Part of our performance review includes an assessment of whether or not we follow proper cybersecurity guidelines.

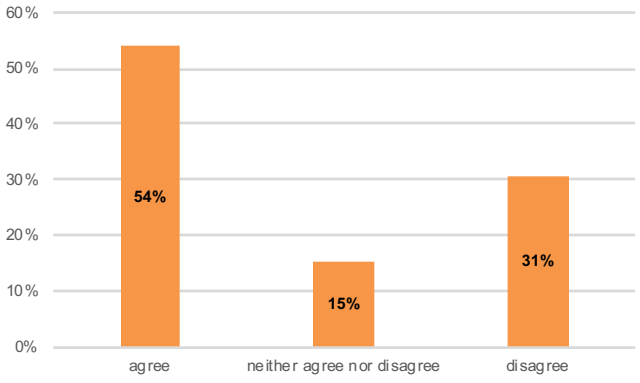


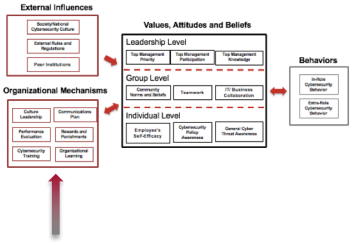


Survey Responses

Cybersecurity at MIT Sloan

Our organization has a leader whose MAIN JOB it is to create and maintain a cybersecurity culture.

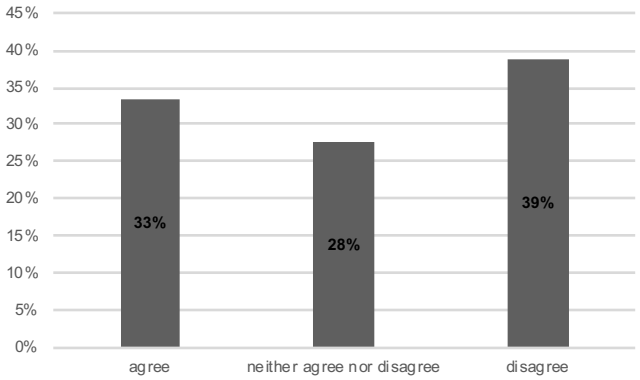


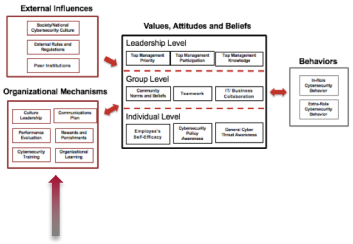


Survey Responses

Cybersecurity at MIT Sloan

Most employees feel our cybersecurity training programs are relevant and effective.

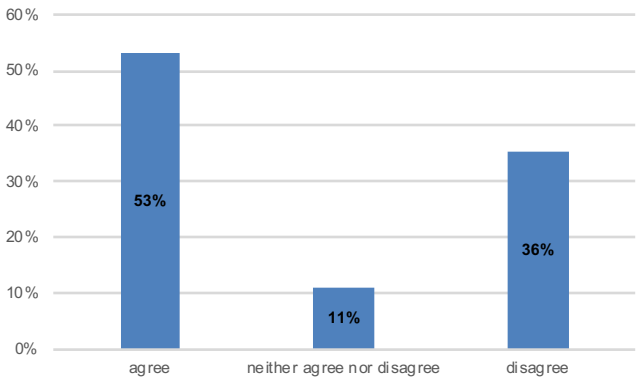


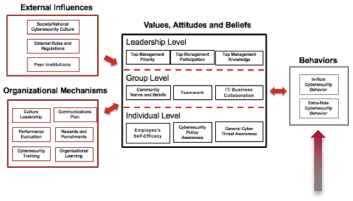


Survey Responses

Cybersecurity at MIT Sloan

Most employees do what is required for their job role to keep our company cyber secure.

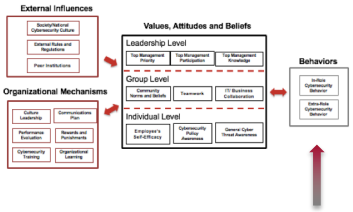




Raise Your Hand if You Agree:

Cybersecurity at MIT Sloan

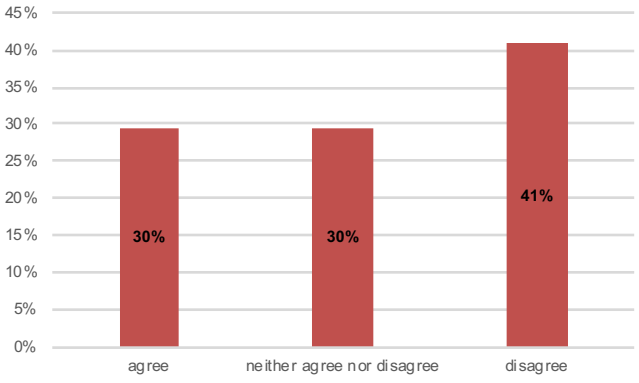
Many employees voluntarily do more than what is expected in their job role to keep our company cyber secure.

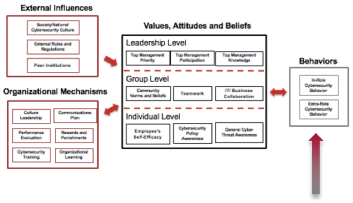


Survey Responses

Cybersecurity at MIT Sloan

Many employees voluntarily do more than what is expected in their job role to keep our company cyber secure.





Conclusions

Cybersecurity at MIT Sloan

- Potential disconnect between importance of culture of cybersecurity and measurable practices
- Companies appropriately put a strong emphasis on training, but the substance of that training may need improvement
- Employees don't seem to *voluntarily* do things to keep their companies secure
- Managers need to measure and reward/punish or at least report back performance in individual annual reviews

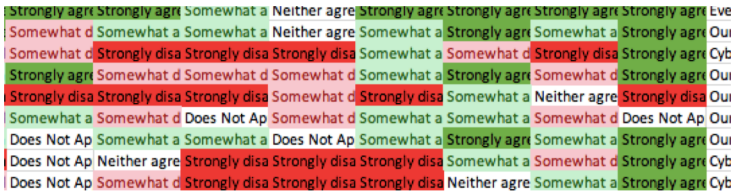
Live Case Study:
Liberty Mutual

Robbie Meitler
CISSP, CIPP,
AVP- Global Data Protection & Privacy
Liberty Mutual Insurance

Next Steps

Cybersecurity at MIT Sloan

- Gather additional data from more diverse group of participants
- Analyze data for correlations
- Understand if/how organizational mechanisms are impacting cybersecurity culture and 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.

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

Dr. Stuart Madnick
smadnick@mit.edu

Dr. Michael Siegel
msiegel@mit.edu

Dr. Keri Pearlson
kerip@mit.edu

Participate in our survey:

http://bit.ly/mit_isc2_culture

THANK YOU!