## Cybersecurity at MIT Sloan

Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)³

# Human Risk Management SIG: The Culture Club
### April 1, 2025

Cybersecurity at
**MIT** Sloan

0

# Culture Club Agenda

Cybersecurity at
**MIT** Sloan

| 11:30am | Kick Off |
|---------|----------|
| 5 Min | Introduction |
| 40 Min | Hot Topics Discussion |
| 40 Min | Case Study Discussion |
| 5 Min | Wrap Up |
| 1:00pm | Adjourn |

1

# Chatham House Rule

To encourage interactivity, we will use the Chatham House Rule:

"Under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

2

# Introductions

**Please introduce yourself. Tell us your:**

**Name**
**Company**
**Position (your role in your company)**

3

---

## Hot Topics Discussion: What's On Your Mind Today?

Audience Participation:
What question would you like to discuss with this group today?

4

## Hot Topics Discussion: Questions submitted with registration

1. How do you build bridges with organizations within the company that view Cyber as a blocker instead of an enabler? (Jeremiah, Premera)
2. How do you get management buy-in on the importance of cybersecurity (awareness)? (Michaela, Mondi)
3. Do you have a risk score?(Betsy, B of A)
4. How are others introducing HRM and HRI(Human Risk Index/Score) to senior leaders?  Are you providing a HRM score to employees? (Tim, Mastercard)
5. Non-punitive recommendations on handling and changing behaviors of Repeat Offenders (Laurie, Liberty)
6. How do you keep coworkers engaged in cyber awareness? (Cherisse, HPE)
7. How is everyone feeling about AI now, several years in? (Kevin, MongoDB)
8. Best ways to watch/keep up with new issues without relying on too many sources.(Kathi, Liberty)
9. What are some uses cases on GenAI being used to assess and produce metrics around cyber culture? (Jay, KPMG)
10. What are other ways that people in the industry measure culture? (Sarah, Microsoft)
11. What are the key indicators of a strong or weak cyber culture? What are the most effective metrics to track cyber culture over time? (Elodie, SE)
12. Methodologies and criteria to measure CS culture. (Jos, Engie) Baseline metrics (Amy, MongoDB)
13. How to measure the impacts of the efforts made on cybersecurity culture (Piret, Engie)

5

Measuring Cybersecurity Culture:
The MAPS Framework
April. 01, 2025 • Dr. Keri Pearlson • Principal Research Scientist
Cybersecurity at MIT Sloan
Formerly The Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity

cams.mit.edu

6

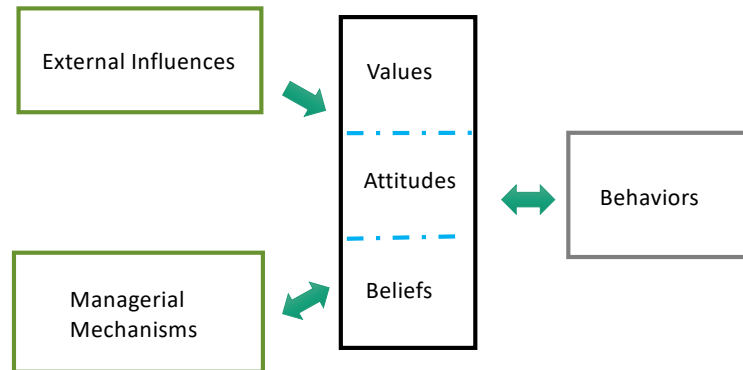## We want to drive strong cybersecurity behaviors

A Cybersecurity Culture:

The **Beliefs**, **Values and Attitudes** that drive cybersecure **Behaviors** in an organization

7

7

# Cybersecurity Culture Model



External Influences → Values

Attitudes ↔ Behaviors

Managerial Mechanisms ↔ Beliefs

8

8

# Our culture model research sparked a number of other projects:

- **Secure by Design: a culture of designing secure products**
- **Liberty Mutual Case study (used to illustrate and discuss culture)**
- **Banca Popolare di Sondrio Case Study (Italian case study)**
- **C6 Bank Case Study (building a cyber culture from the ground up)**
- **Verizon Media/Yahoo Case Study (measuring the success of culture initiatives)**
- **AI's Impact on Cyber Culture**
- **A Culture Maturity Model**
- **Measuring Cyber Culture Maturity**
- **Sharing Culture in Our Supply Chains**

**Plus many more research projects outside of MIT**
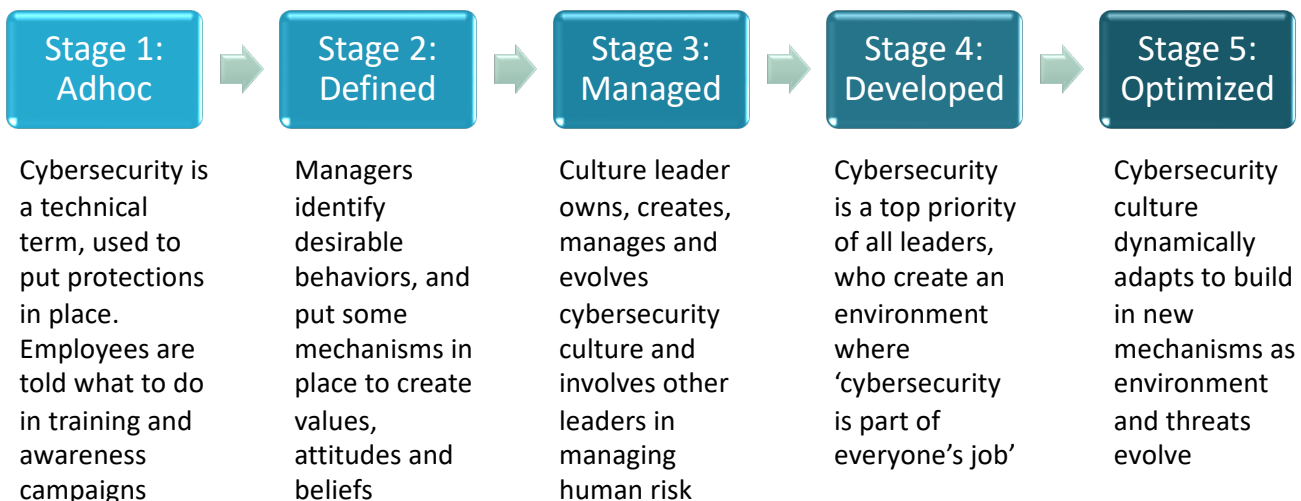**(we know of over 97 other studies citing this work)**

9
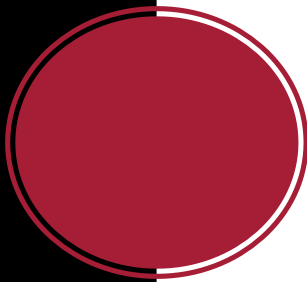
**Our latest research on cybersecurity culture creates a way to assess culture and determine "maturity"**

Cybersecurity at MIT Sloan

10

---

# Cybersecurity Culture: A Maturity Model

Cybersecurity at MIT Sloan

| Stage 1: Adhoc | Stage 2: Defined | Stage 3: Managed | Stage 4: Developed | Stage 5: Optimized |
|---|---|---|---|---|
| Cybersecurity is a technical term, used to put protections in place. Employees are told what to do in training and awareness campaigns | Managers identify desirable behaviors, and put some mechanisms in place to create values, attitudes and beliefs | Culture leader owns, creates, manages and evolves cybersecurity culture and involves other leaders in managing human risk | Cybersecurity is a top priority of all leaders, who create an environment where 'cybersecurity is part of everyone's job' | Cybersecurity culture dynamically adapts to build in new mechanisms as environment and threats evolve |

11

# The MAPS Tool to Measure Cybersecurity Culture Maturity

Hypothesis: We can assess constructs from our cybersecurity culture model and evaluate how mature a culture is:

## Management/Leadership
## Attitudes/Values/Beliefs
## Policies
## Strategy

12

---

# The MAPS Tool to Measure Cybersecurity Culture Maturity

We can measure these constructs and evaluate how mature a culture is:

## Man
## Attitu
## Polici
## Strategy

Management/Leadership:
Ownership and motivator for culture
-Culture leader
-Resilience plans
-Supervisor/Executive involvement

13

## The MAPS Tool to Measure Cybersecurity Culture Maturity

We can measure these constructs and evaluate how mature a culture is:

**M**ana

**A**ttitu

**P**olicie

**S**trategy

Attitudes/Values/Beliefs
The unwritten rules
-Individual empowerment
-Individual responsibility
-Team support

14

---

## The MAPS Tool to Measure Cybersecurity Culture Maturity

We can measure these constructs and evaluate how mature a culture is:

**M**anag

**A**ttitu

**P**olic

**S**trateg

Policies
Rules and procedures
-Training
-Compliance
-Rewards/Consequences

15

## The MAPS Tool to Measure Cybersecurity Culture Maturity

We can measure these constructs and evaluate how mature a culture is:

Mana
Attitu
Polic
Strategy

Strategy
Goals and plans
-Group Collaboration
-Just in time learning
-Funding of culture

16

---

# Measuring Culture: the Process

- Given to 30+ individuals (leaders and employees) in the organization
- Used to gauge their perceptions about how cybersecurity works in their organization, and their role in keeping the organization cybersecure

Cybersecurity Culture Assessment

- Given to one individual who is either the cyber culture lead or someone 'in the know' about cybersecurity in the organization.
- Used to assess the presence or absence of some of the components from the cybersecurity culture framework

Cybersecurity Culture Inventory

17

# Outcomes the Process

Analysis of the responses from both the assessment and the inventory will provide insight into the status of the the cybersecurity culture and how to improve it.

Collection from multiple organizations will enable comparisons and a rich data set for understanding how culture evolves and matures in enterprises.

- Summary of the inventory
- Summary of attitudes of respondent from MAPS
- Gaps between inventory and attitudes
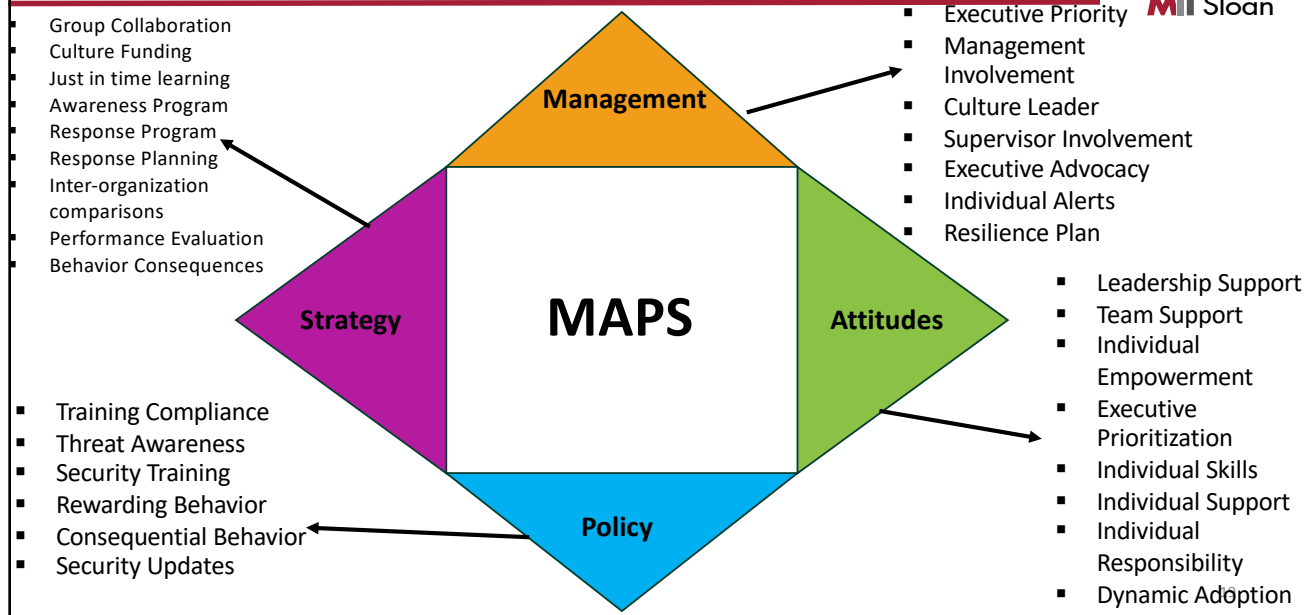- Actionable insights for organization to increase its maturity
- Comparisons between sites to understand culture maturity

18

18

---

# Measure each competency on a scale of 1-5

- Group Collaboration
- Culture Funding
- Just in time learning
- Awareness Program
- Response Program
- Response Planning
- Inter-organization comparisons
- Performance Evaluation
- Behavior Consequences

**Management**

**Strategy**

**MAPS**

**Attitudes**

**Policy**

- Training Compliance
- Threat Awareness
- Security Training
- Rewarding Behavior
- Consequential Behavior
- Security Updates

- Executive Priority
- Management Involvement
- Culture Leader
- Supervisor Involvement
- Executive Advocacy
- Individual Alerts
- Resilience Plan

- Leadership Support
- Team Support
- Individual Empowerment
- Executive Prioritization
- Individual Skills
- Individual Support
- Individual Responsibility
- Dynamic Adoption

19

# Culture Assessment Outcome
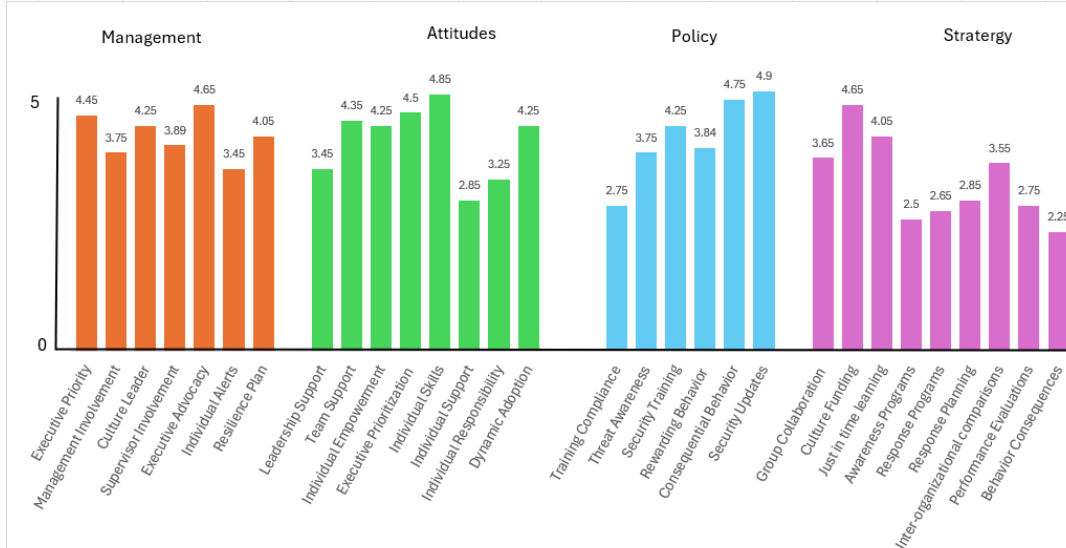
20

---

## SAMPLE: Recommendations Based on Assessment and Inventory Data (under development)

Sample analysis might include:

MAPS Assessment Report:
- Management: 3.8
- Attitudes: 3.2
- Policy: 4.0
- Strategy: 2.8

Gaps comparing Assessment with Inventory:
- Executives are not seen as prioritizing cybersecurity behaviors
- Non-cyber managers do not show interest or get involved in cybersecurity

Overall, the assessment of your organization shows a culture level between *managed* and *developed*.  Based on your MAPS report, here are actionable insights for increasing *management* competencies:

1. Ask executives to demonstrate commitment to cybersecurity talking about it with peers.
2. Give supervisors a cybersecurity topic to talk about it in their next team meeting.
3. Challenge employees do a short presentation on what they would do if the organization had a cyber incident.

21

# Pilot Testing with a Municipality

Opportunity:

Apply the Cybersecurity Culture Assessment to a local municipality.  Make this available to the MIT Cybersecurity Clinic program.

Pilot Test:

Working with the cyber-leader of a local municipality, we have administered the inventory and the assessment.

Status:

We are in the data collection phase.  We expect to do the analysis, create the sample report, and write up our experience by the end of June.

22

# Audience Participation: Help us refine our measurement tool

Here is our tool for assessing cybersecurity culture maturity.  Please take this survey so we can test it out:
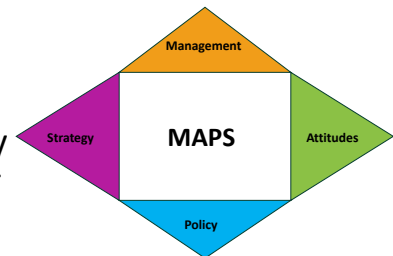
https://bit.ly/MITOrgCultureAssessment25

23

## Next Steps

➔ Review the results of the data collected at the municipality, create report summarizing the data and offering actionable insights.

➔ Modify/edit the survey and inventory if necessary (grammar, clarity, etc.) and package it for the MIT Cybersecurity Clinic.

➔ Pilot test with an organization

  ➔ Follow same process: assessment taken by multiple individuals and inventory completed by cybersecurity culture manager/leader.

  ➔ Anyone interested in being our pilot test? (If so, please contact Keri)

**MAPS**
Management
Strategy
Attitudes
Policy

24

---

# Discussion

25

Wrap Up

26

---

**CAMS Culture Club/Human Risk Management SIG Archives**

## Please visit:

## https://cams.mit.edu/cultureclub/

## To download meeting summaries from all Culture Club SIG meetings.

27

Cybersecurity at

**MIT** Sloan

# THANK YOU!

**We could not do the work we do without our CAMS members!  Thank you for supporting our work.**

**More info available at: https://cams.mit.edu  or
Contact Keri: kerip@mit.edu**

28