Cybersecurity Culture Maturity Model

Dr. Keri Pearlson, Mridula Prakash

Date 08/17/2023

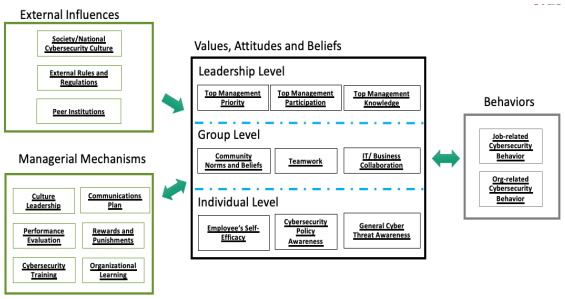
CAMS - (IC)³ • https://cams.mit.edu

Cybersecurity at MIT Sloan

1

Research Overview

- The CAMS Cybersecurity Culture Model setups a framework for building a cybersecurity culture.
- Since implementation happens over time, we have observed that the maturity level of an organization's culture changes as more investment is made.
- This research project suggests a 5-level maturity model that provides a road map to a highly effective cybersecurity culture.



CAMS Cybersecurity Culture Model

2

Research Assumptions

- People continue to introduce cyber vulnerabilities into organizations. Managing this vulnerability continues to be a challenge.
- As the threats change, the cybersecurity culture must also change. Culture is not static. It evolves and matures.
- Managers want a roadmap to make their culture better. It would be useful to articulate different levels of maturity of a cybersecurity culture so managers can assess where their organization is and have a clear set of action items to increase maturity.
- A more mature cybersecurity culture is more effective.

3

Discussion

How would you describe the best possible cybersecurity culture for your organization? What is your vision?

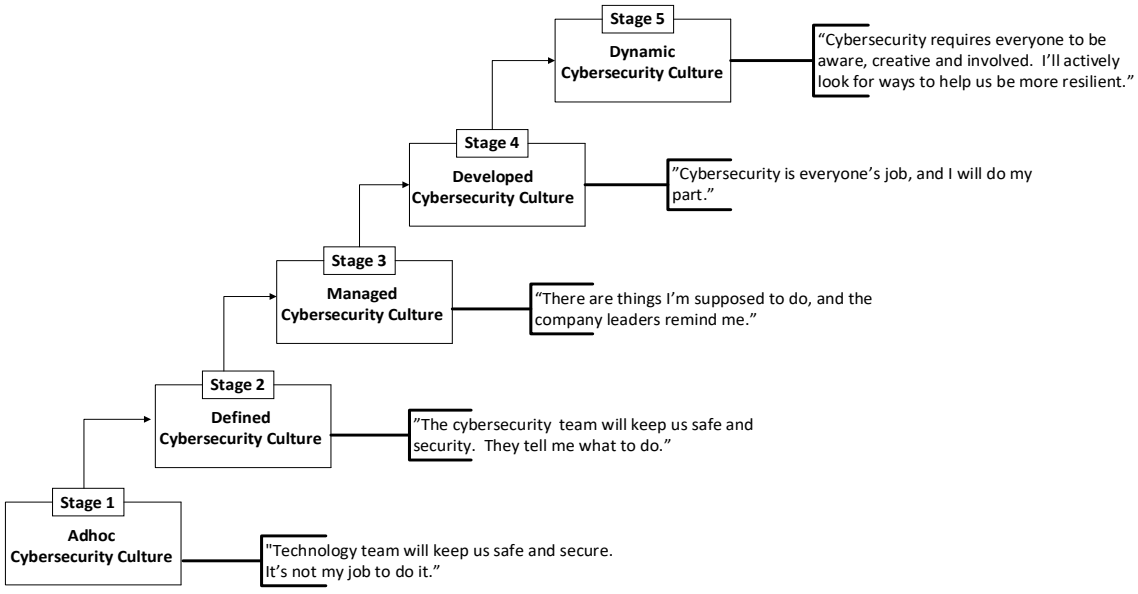
4

Research Objectives

- Articulate different levels of cybersecurity culture maturity.
- Suggest a roadmap of actionable insights for managers to use to increase cybersecurity culture maturity.
- Create an assessment model for understanding the current level of cybersecurity maturity

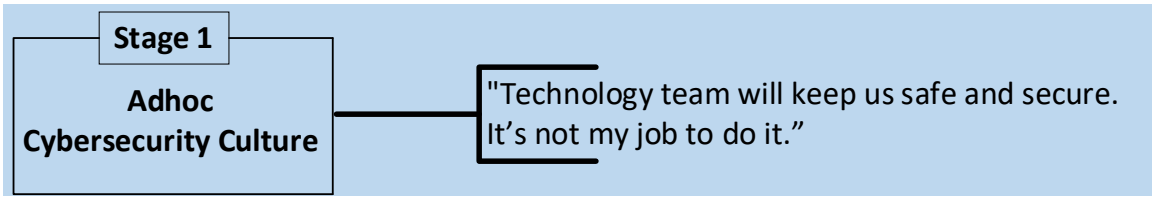
5

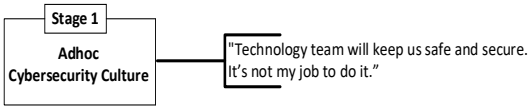
Cybersecurity Culture Maturity Stages



6

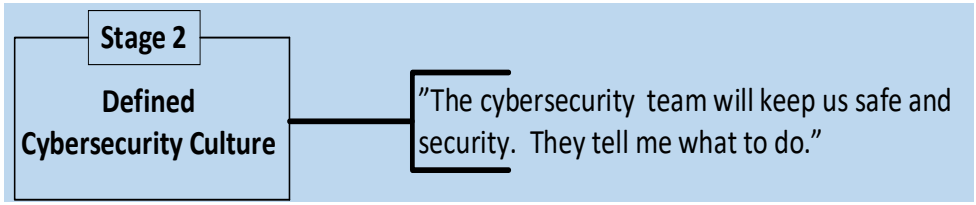
Stage 1: Adhoc Cybersecurity Culture

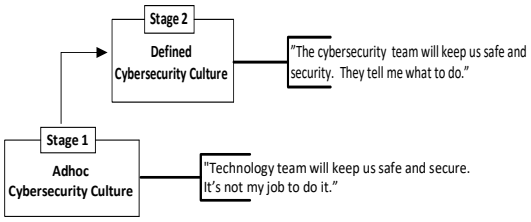




7

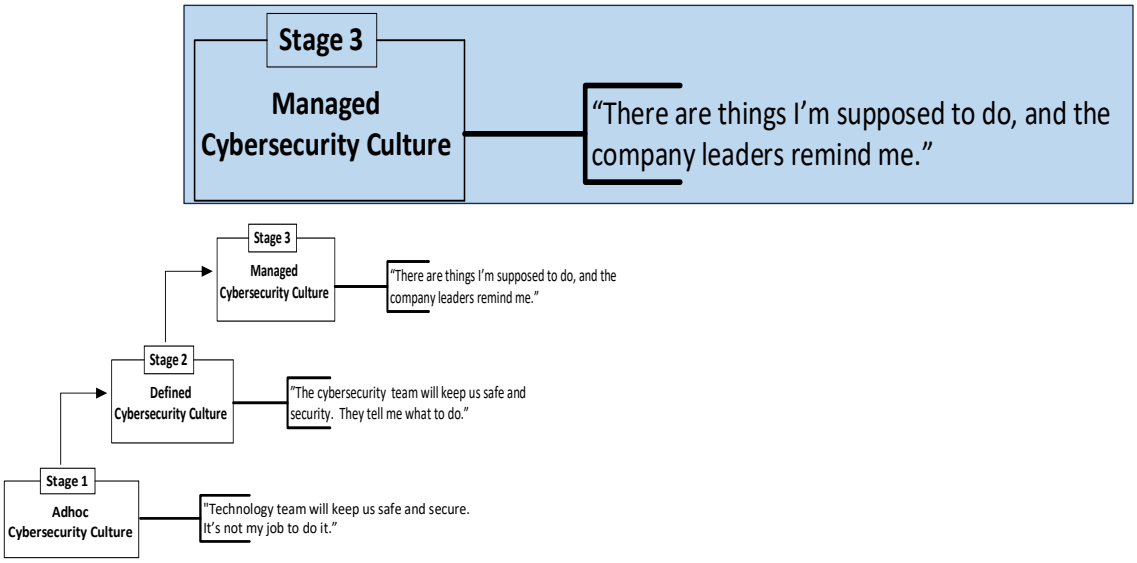
Stage 2: Defined Cybersecurity Culture





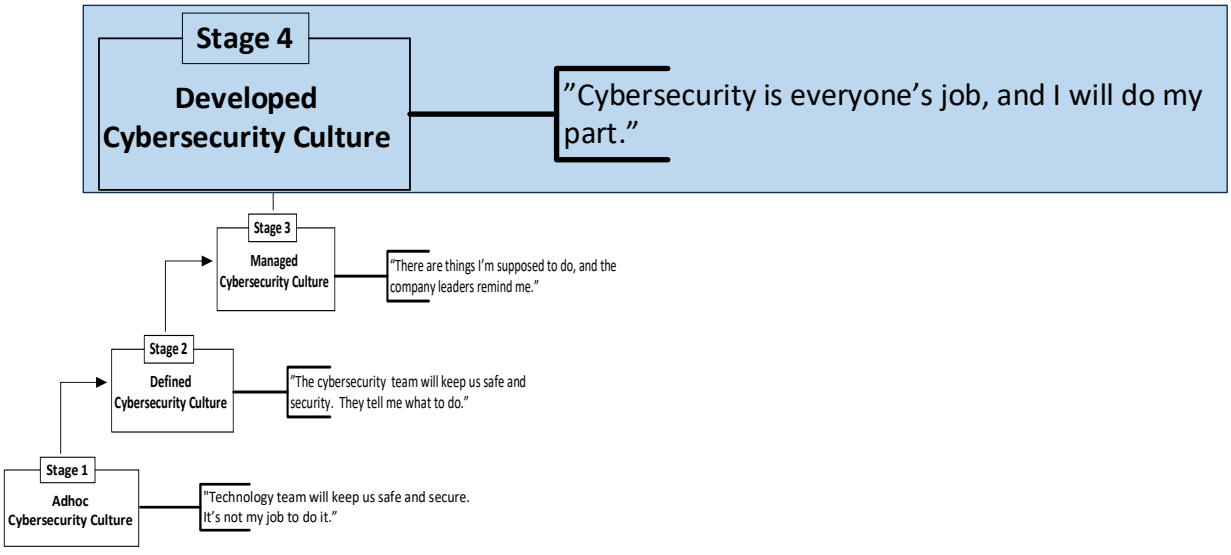
8

Stage 3: Managed Cybersecurity Culture



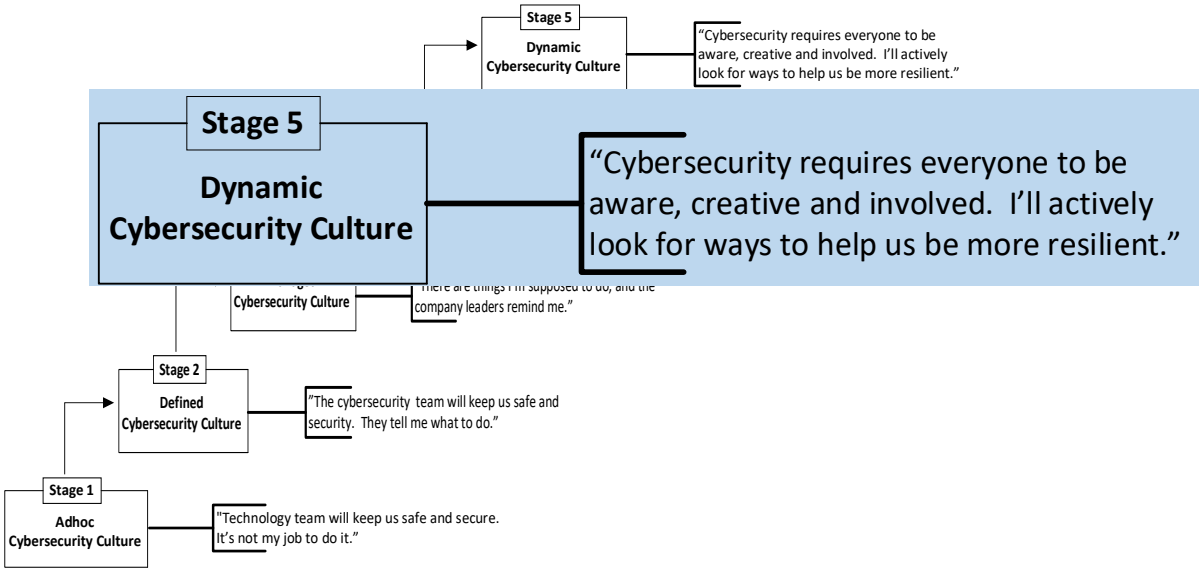
9

Stage 4: Developed Cybersecurity Culture



10

Stage 5: Dynamic Cybersecurity Culture



11

Cybersecurity Culture Maturity Model – Attitudes

Maturity Stages	Description	Values, Attitudes and Beliefs
Stage 5 Dynamic Cybersecurity Culture	The processes that drive cybersecurity culture incorporate the changing environment and threat landscape, and adapt naturally to build in new mechanisms for culture as needed.	Employees are regularly involved in and creating actions that keep the organization more resilient.
Stage 4 Developed Cybersecurity Culture	Cybersecurity is one of management's top priorities where the prevailing attitude is that "cybersecurity is part of everyone's job." There are programs and mechanisms designed to propagate this attitude.	Employees are empowered to do what is necessary to be secure, and everybody thinks cybersecurity is their job.
Stage 3 Managed Cybersecurity Culture	Management has a cybersecurity culture leader with ownership of creating, managing, and evolving the cybersecurity culture.	Employees shared values, attitudes and beliefs around the importance of cybersecurity and do what they are told to do to keep the organization secure.
Stage 2 Defined Cybersecurity Culture	Management has identified cybersecure behaviors they seek from employees. There are some mechanisms in place to create values, attitudes and beliefs that drive cybersecure behaviors.	A cyber culture leader/team drives the culture, using mechanisms to create values, attitudes and beliefs to drive cyber behaviors.
Stage 1 Adhoc Cybersecurity Culture	Cybersecurity is only a criterion for IT systems and management, and the culture is mostly to invest in technology solutions to build protection. There are activities like orientation, training and awareness programs to tell employees what to do and not do.	Employees believe that "Technology team will keep us safe" and they have little if any personal responsibility to do so.

13

Cybersecurity Culture Maturity Model

Maturity Stages	Training and Awareness	Leadership Involvement	Performance and Evaluation	Employee expectations	Response to new threats
Dynamic Cybersecurity Culture	As new threats emerge, employees make their own training and awareness programs.	All leaders are regularly involved with no additional prodding from their more senior leaders.	Self-motivated. No additional rewards needed to encourage behavior.	Employees are self motivated to help organization find ways to be more secure.	Everyone in the organization empowered to respond to new threats in role–appropriate way.
Developed Cybersecurity Culture	Ongoing on-demand training available at any time. Constant, engaging awareness programming.	Executives regularly demonstrate their commitment to cybersecurity by prioritizing it, talking about it, and investing in it.	Cybersecurity behavior is part of your annual performance evaluation.	Employee expected to take actions without being told or reminded.	All Leaders look for new threats and feed them to cyber team to build new responses.
Managed Cybersecurity Culture	Regular training and awareness programs pushed out to employees.	Business leaders demonstrate ownership of cybersecurity and drive culture in their teams.	Consequences for repeated offences.	Employees are expected to follow supervisors guidance.	Business Leaders guided by cybersecurity team respond to new threats
Defined Cybersecurity Culture	Annual and just-in-time training programs and periodic, regular awareness campaigns.	Technology leaders drive cybersecurity activities and try to engage business partners.	Rewards or incentives for good cybersecurity behaviors.	Employee are expected to follow policies and procedures setup by the security group	Cybersecurity team builds in new responses as needed.
Adhoc Cybersecurity Culture	Little (maybe during orientation only) or no cyber training.	Cybersecurity leaders drive cybersecurity programs, processes and activities.	No connection between cybersecurity behavior and performance	No specific employee expectations set up since technology	Technology responsible for handling new threats

14

Discussion Questions

1. How do you identify your cybersecurity culture today? How do you know what the culture is? What do you measure or observe?
2. How would you use a cybersecurity culture maturity model? Do you see different levels of culture maturity in your organization? How are the levels different?
3. What does the 'optimum level' of cybersecurity look like? What is your vision for the best possible cybersecurity culture?
4. Any other feedback on the cybersecurity culture maturity model? Anything you suggest we consider adding?

15

Thank You

For further questions reach out to:

mridula@mit.edu
kerip@mit.edu

16