CYBERSECURITY AT MIT SLOAN

Working Paper Series
CAMS24.1109

Cybersecurity Culture Maturity Model

(March 1, 2024)

Authors:

Mridula Prakash, MIT CAMS, mridula@mit.edu

Dr. Keri Pearlson, MIT CAMS, kerip@mit.edu

These papers are written in partial support by CAMS memberships.

Cybersecurity Culture Maturity Model

Mridula Prakash and Dr. Keri Pearlson
Cybersecurity at MIT Sloan, MIT
March 1, 2024

Abstract

Cyber-attacks are on the rise, becoming increasingly sophisticated and severe. Businesses and government entities should implement strong governance, organizational cultures, and data management procedures to reduce susceptibility to these risks and ensure efficient counter measures. This paper presents a Cybersecurity Culture Maturity Framework (CCMF) for assessing and providing a roadmap to a highly effective cybersecurity culture. People are an important aspect of cybersecurity culture and continue to introduce cyber vulnerabilities into organizations. Managing these vulnerabilities continues to be a challenge. After conducting a thorough review of the most commonly used security frameworks, we identified core security human-related elements and classified them by constructing a domain agnostic security model. We then proceeded by presenting in detail each component of our model and attempted to add markers to each level to achieve a feasible assessment methodology. The paper thereafter presents a five-level maturity model to evaluate the current security readiness of an organization's workforce and provides a clear set of action items to help the organization to increase their culture maturity. The model has been designed with the assumptions that as threat change, the cybersecurity culture must also change i.e culture is not static and evolves and matures. With this model we are trying to articulate different levels of maturity of a cybersecurity culture so managers can assess the organization.

Keywords: Cybersecurity, culture, organization culture, people, maturity framework.

1. Introduction

Cybersecurity encompasses three dimensions- technical, managerial and culture. The technical address technologies, tools, and skills to detect and mitigate cyber-attacks. The managerial aspect focuses on defining data governance and establishing enterprise processes. The culture component brings values, attitudes and beliefs of an organization (Huang and Pearlson 2019). Even if an organization possesses the most sophisticated technological and managerial security measures, it remains susceptible to a cyber breach if the individuals within the organization do not exercise caution and prioritize protection. In recent years, the concept of security culture has gained significant attention in both practical and research settings. This is primarily due to organizations' efforts to counter the rising number of attacks that exploit human vulnerabilities. In the 2023 Data Breach Investigation Report, Verizon Corporate highlighted that "seventy-four of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering." Managers are having a hard time and are required to motivate employees to perform in secure ways. This means a culture of cybersecurity needs to be created.

However, it isn't easy to identify, measure and quantify cybersecurity culture. Most of the organizations consider cybersecurity culture to be static. As threats change, the cybersecurity culture must also change. This project presents a practical framework for articulating various levels of cybersecurity culture maturity focusing on research question '*How will leaders describe the best possible cybersecurity for their organizations.*' In this paper, we outline a five-level maturity model to a roadmap of actionable insights for managers to use to increase cybersecurity culture maturity. This will help organizations understand the current level of assessment of cybersecurity maturity.

This paper presents the initial findings captured by surveying cybersecurity managers and leaders for their input regarding their vision of an effective

cybersecurity culture. In essence, this is ongoing research, here we present a representative framework mapping all various stages of cybersecurity culture. This research will help incentivize organizations to measure their current cybersecurity culture and create a roadmap to lead towards a better efficient cybersecurity culture.

The remainder of the paper is structured as follows: Section 2 offers an overview of recent, eminent literature discussing current practices of cybersecurity culture framework or models. Section 4 presents the research methods used in this study. Section 5 presents the conceptual framework derived based on our study. Section 6 provides concluding remarks.

2. Literature Review

As the foundation for this research, two areas of literature are summarized. First, this work draws from literature about the maturity models developed across various aspects or domains. Next one, draws upon cybersecurity culture maturity models from previous studies done by cybersecurity companies.

The ultimate goal of a cybersecurity maturity model is to be able to articulate the different levels of cyber culture maturity and help organizations use the same. To build a cybersecurity culture maturity model, we examined how an organization leaders envision an optimum level of cybersecurity culture. According to the National Institute of Standards and Technology (NIST 2024) definition, information security is defined as "*the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability,"* and cybersecurity is the *"ability to protect or defend the organization from cyber-attacks*".

There are several well-established models that divide various other aspects of maturity from highest to lowest. For example, one such well known model for process maturity is the Capability Maturity Model (Paulk, et al. 1993). This model has five levels of maturity starting from initial in the lowest level to continuous improvement being the highest level. Level 1 is known as Initial where their inconsistencies in the management process across the organization. Level 2 is known as Managed where the process is documented. The next Level 3 is known as Standard where there is repeatability in process and apply throughout the organization. Level 4 is predictable where the organization process is benchmarked and tracked through key performance indicators (KPIs). The final level 5 is continuous improvement where the organization is continuously improving.

Other models very specific to security culture maturity is the Security Culture Maturity Model was developed by KnowBe4 (KnowBe4 2022). In the KnowBe4 model there are again five stages of maturity. Level 1 is the Basic Compliance where there is basic minimum training. Level 2 is Security Awareness Foundation where there is annual and onboarding training provided to employees. There is also occasional phishing simulation provided and focus is on content during training. The next Level 3 is Programmatic Security Awareness & Behavior there is intentional awareness program with integrated tools and focus on security-aware behaviors. The next Level 4 which is the Security Behavior Management where there is continuous training across varied delivery methods. The focus of programs is on real behavior change. The final level is Level 5 Sustainable Security Culture where the program intentionally measures, shapes and reinforces security culture. The entire security value is woven through the fabric of the entire organization.

4. Research Methods

The review of relevant literature demonstrated that cybersecurity culture maturity is incomplete due to two key reasons – (1) It does not consider culture is not static and evolving (2) It does not provide a roadmap to achieve effective cybersecurity culture.

To provide a deep and meaningful understanding of cybersecurity culture, a short survey with CIOs across diverse industries were conducted. This survey requested participants two main questions: (1) What would a "mature cybersecurity culture" look like? (2) What does an effective cybersecurity culture include? Is it different than a mature culture in your mind?

Around six responses were recorded, and the analysis of the responses showed qualitative dataset that formed the baseline for the cybersecurity culture maturity model.

4.1 Qualitative Data and Findings

The insights derived from the qualitative findings provided guidance for the design of the cybersecurity culture maturity model. All respondents had strong opinions about mature cybersecurity culture. Generally, participants agreed that stronger engaged employee base with all levels within the organization fully understanding the cybersecurity principles. For example, one respondent commented,

"*Cybersecurity is fully embedded within the organization and is part of the company DNA*"

Most of the respondents agreed that there was a difference between defining an effective and mature cybersecurity culture. One of the respondent, who is a CISO remarked as follows,

"While the terms "effective" and "mature" are often used interchangeably, an effective culture may signify a strong foundation, whereas a mature culture implies a more evolved and continuously improving state, adapting to emerging cybersecurity challenges"

All the participants expressed the need for a cybersecurity culture to reduce cybersecurity risk to the organization. A respondent a current CISO at a reputed firm compared cybersecurity culture to that of a relationship between a parent and child remarked below:

"*A mature cybersecurity culture has each individual making the appropriate cybersecurity actions and decisions to effectively reduce cybersecurity risk to the organization and they do so without having to think too much about it. For example, a parent holds a child's hand as they learn to safely cross the street. The parent holds the child back at the curb and teaches them to look right, left, and right again, to make sure all traffic is clear, before proceeding. After many lessons and the passage of time, the child can be trusted to safely cross the street. At that point even the child doesn't think too much about it. It's now just what they do 'naturally'. They can be lost in thought, chasing a ball. Whatever...but when they come to a street to cross the make sure it's safe to cross before crossing."*

5. Cybersecurity Culture Maturity Model

The model was created to address three clear research objectives: (1) able to articulate different levels of cybersecurity culture maturity. (2) have a roadmap with actionable insights for managers. (3) provide a model for assessing the current level of cybersecurity culture maturity. Figure 1 illustrates the five stages of cybersecurity culture maturity model.

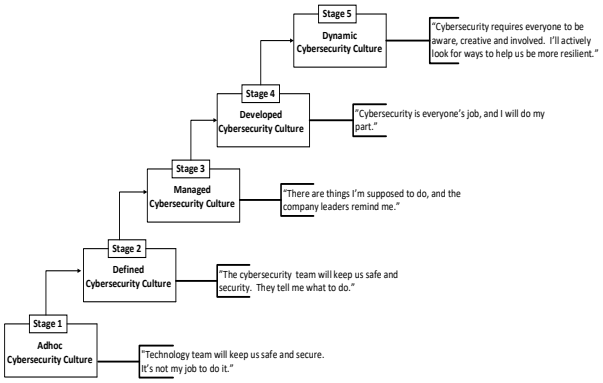

Figure 1: Cybersecurity Culture Maturity Stage

5.1 Stage 1: Adhoc Cybersecurity Culture

We are calling stage 1: Adhoc cybersecurity culture. In this stage the organization has grown organically, and the culture is more about investing in technology to keep the organization secure. There is no organization 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. The mindset of the people is technology team will keep us safe and secure and it's the IT team's responsibility.

5.2 Stage 2: Defined Cybersecurity Culture

We are calling stage 2: Defined cybersecurity culture. In this stage there is a plan within the organization about culture. There is a cybersecurity team within the organization and the mindset of the employees is that cybersecurity team will keep them safe and secure. The employees do what they are told to do. 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.

5.3 Stage 3: Managed Cybersecurity Culture

We are calling stage 3: Managed cybersecurity culture. Organizations at this level have a plan and there is an owner for the cybersecurity culture across the organization other than a CISO. Management has a cybersecurity culture leader with ownership of creating, managing, and evolving the cybersecurity culture. The mindset of the employees are they know that they have certain responsibility towards

cybersecurity but need constant reminders from company leaders.

5.4 Stage 4: Developed Cybersecurity Culture

We are calling stage 4: Developed cybersecurity culture. The mindset of the employees is cybersecurity is everyone's job. For example, if an employee sees a phishing email, they will report it to the cybersecurity team. 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.

5.5 Stage 5: Dynamic Cybersecurity Culture

We are calling stage 5: Dynamic cybersecurity culture. In this stage the culture is able to adapt based on the changing threat vectors. The values, attitudes and beliefs are easily updated by the changing dynamics. The employees mindset is cybersecurity is everyone's job but they are involved and looking at ways to help organizations become more resilient. Employees are actively involved and bring new ideas on cybersecurity and hold discussion for wider audience within the organization.

6.0 Cybersecurity Culture Maturity Model – Mindset and Attitudes.

Mindsets and attitudes are important to create a culture across the organization. It is these that determine the maturity of the organization. Table 1 summarizes the mindset of employees across each stage of the cybersecurity maturity model. Table 2 summarizes the attitudes of the employees across each stage of cybersecurity maturity model.

Table 1: Cybersecurity Maturity Model - Mindset of Employees

Maturity Stages	Mindset
Stage 5: Dynamic Cybersecurity Culture	"Cybersecurity requires everyone to be aware, creative and involved. I'll actively look for ways to help us be more resilient"
Stage 4: Developed Cybersecurity Culture	"Cybersecurity is everyone's job, and I will do my part."
Stage 3: Managed Cybersecurity Culture	"There are things I'm supposed to do, and the company leaders remind me."
Stage 2: Defined Cybersecurity Culture	"The cybersecurity team will keep us safe and secure. They tell me what to do."
Stage 1: Adhoc Cybersecurity Culture	"Technology team will keep us safe and secure. It's not my job to do it."

It can be seen that the mindset of the employees changes as the organization matures. From shifting responsibility employees become more open to take up ownership and responsibility. In the Stage 5, dynamic cybersecurity culture the employees are involved and are proactively involved to suggest additional cybersecurity measures to help their organizations.

Table 2: Values Attitudes and Beliefs of a Cybersecurity Culture Model

Maturity Stages	Values, Attitudes and Beliefs
Stage 5: Dynamic Cybersecurity Culture	Employees are regularly involved in and creating actions that keep the organization more resilient
Stage 4: Developed Cybersecurity Culture	Employees are empowered to do what is necessary to be secure, and everybody thinks cybersecurity is their job
Stage 3: Managed 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	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	Employees believe that "Technology team will keep us safe" and they have little if any personal responsibility to do so.

In Table 2, we can see the change in values, attitudes and beliefs across various stages.

7.0 Cybersecurity Culture Maturity Model Framework

To identify the maturity of an organization it's important to look at some key parameters. The key

parameters identified are: (1) Training and Awareness. (2) Leadership involvement (3) Performance and Evaluation (4) Employee expectations. (5) Response to new threats. Table 3 shows the parameters and the markers across each level.

Table 3: Cybersecurity Culture Maturity Framework

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 evaluation	No specific employee expectations set up since technology manages security.	Technology responsible for handling new threats

If consider parameter training and awareness, at adhoc stage then there is little, or no training is provided to the employees. At stage 2, defined cybersecurity culture annual or just-in-time training programs and periodic, regular awareness campaigns are provided. In the next managed stage, regular training and awareness programs pushed out to employees. In the developed stage, ongoing on-demand training is available at any time with constant engagement and awareness programs. In the final and dynamic stage as new threats emerge employees make their own training and awareness programs.

Similarly in another parameter like employee expectations in the adhoc stage no specific employee expectations as the technology is expected to manage security. In the defined cybersecurity stage, employees are expected to follow policies and procedures set up by the security group. In stage 3, managed cybersecurity level, employees are expected to follow supervisors guidance. In stage 4, developed cybersecurity level employees are expected to take actions without being told or reminded. In the final stage 5, dynamic cybersecurity culture employees are self-motivated to help organizations find ways to be more secure.

7. Conclusion

Cybersecurity culture is people dependent, and organizations are embracing the importance and organizations are taking actions to improve their cybersecurity culture. However, there are not many tools to measure cybersecurity culture and even less tools to provide the maturity level of the organization's cybersecurity culture.

By creating a cybersecurity culture framework, it will help provide a roadmap with actionable insights for managers. Organizations will be able to assess the current level of cybersecurity culture maturity. In this paper a cybersecurity culture maturity framework is presented with five stage levels of maturity. Culture is not static but evolves and matures over time. Hence, having a framework will help identify the current gaps and provide a roadmap for assessing the cybersecurity culture maturity of an organization.

12. References

Huang, Keman, and Keri Pearlson. 2019. "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture." *52nd Hawaii International Conference on System Science.*

KnowBe4. 2022. "Introducing the Security Culture Maturity Model." https://www.knowbe4.com/security-culture-maturity-model.

NIST. 2024. https://www.nist.gov/cyberframework.

Paulk, Mark, Bill Curtis, Mary Chrissis, and Charles Weber. 1993. "Capability Maturity Model." *IEEE.* 18-27.