Building a Model of Organizational Cybersecurity Culture

Identifying Factors Contributing to a Cyber-secure Workplace

2019 Survey Results

Dr. Keman Huang, CISSP
Cybersecurity at MIT Sloan
keman@mit.edu

Dr. Keri Pearlson
Cybersecurity at MIT Sloan
kerip@mit.edu

Contents

Executive Summary

I. Organizational Cybersecurity Model

II. Survey Results

i. Survey Methodology

ii. Demographics Profile

iii. Panoramic View

iv. Cybersecurity Culture Level Analysis

v. Suggested "Best" Practices

III. Conclusion

IV. Acknowledgement

V. Appendix

Appendix A: Model Definitions

Appendix B: Heat Maps for Three Layers

Appendix C: Suggested "Best" Practice List

Executive Summary

Organizations are vulnerable to cyber-attacks partially because people in the organization are unaware of or unprepared for cyber risks. Building a culture of cybersecurity where the values, attitudes, and beliefs align with organizational goals of cyber resilience is of significant interest to managers and leaders in charge of cybersecurity in organizations today.

This research aims to provide practical tools for cybersecurity leaders to evaluate and improve the maturity of their organizational cybersecurity culture. This organizational cybersecurity culture model, named OCCM, is based on a systematic literature review, case studies, and workshop discussions. More specifically, to go beyond a literature review to identify the related components of organizational cybersecurity culture, we collected information through surveying individuals with knowledge of cyber practices in their companies, semi-structured interviews with willing participants, and voluntary workshop to discuss practices.

This survey was developed by Cybersecurity at MIT Sloan (CAMS) at MIT's Sloan School of Management to verify the developed model and explore cybersecurity culture across organizations within different industries.

From June to December 2018, this project surveyed 187 individuals from 11 industries and 18 countries.

KEY TAKEAWAYS

- The Organizational Cybersecurity Culture Model (OCCM) can be used as a roadmap for advancing cybersecurity culture and driving more cyber-secure behaviors.
- The survey results show that ***Managerial mechanisms*** for building a cybersecurity culture are present but underdeveloped. The leader responsible for building a cybersecurity culture (***Culture Leadership***) had the critical influence on the perception of strong organizational cybersecurity culture. While ***Cybersecurity Training*** is the most popular practice, ***Performance evaluations and rewards and punishments*** are untapped mechanisms that managers can use to influence values, attitudes, and beliefs.
- The ***Behaviors*** of employees in organizations were the most reflective of the cybersecurity culture in place; specifically, looking at the ***In-role*** and ***Extra-role cybersecurity behavior***. A great indication of a high-level cybersecurity culture would be an increase in ***Extra-Role Cybersecurity Behavior***, as it indicated an increase in employees' personal cybersecurity responsibility.
- There is value in driving the attitude that cybersecurity is something everyone needs to care about; it is not just something an IT group or technology does for you.

I. Organizational Cybersecurity Culture

We define organizational cybersecurity culture as "the *beliefs*, *values*, *and attitudes* that drive employee behaviors to protect and defend the organization from cyber-attacks."

To build a model of cybersecurity culture, we examined three concepts: **organizational culture, national culture, and information security culture**.

A common definition of organizational culture comes from Ed Schein's model. He suggests three components of culture: 1) the belief systems forming the basis for collective action; 2) the values representing what people think is important; and 3) artifacts and creations which are the "art, technology, and visible and audible behavior patterns as well as myths, heroes, language, rituals and ceremony."

Using a different lens, Quinn's competing values-model distinguishes between four types of organizational cultures based on the orientation of the values and beliefs: 1) The support orientation emphasizes employees' spirit of sharing, cooperation, trust, individual growth, and the decisions made through informal contacts. 2) The innovation orientation emphasizes that the organization is open to change, willing to search for new information, and willing to be creative in problem solving. 3) The rules orientation emphasizes respect for authority, formal procedures, and the importance of following written rules, normally resulting in a top-down hierarchical structure. 4) The goal orientation emphasizes specification of targets, the criteria for performance measurement and the reward based on the attainment of goals, reflecting the understanding of organizational goals, and individual responsibility and accountability.

National culture focuses on a cross-cultural perspective and impacts how employees comply with authority and follow organizational rules and policies. The most accepted taxonomy of national culture, by Hofstede, includes concepts such as "individualism vs. collectivism," "long-term vs. short-term orientation" and "indulgence vs. restraint".

Information security culture, a subculture of an organization's culture, has been defined by Da Veiga and Eloff as: "attitudes, assumptions, beliefs, values and knowledge that employees / stakeholders use to interact with the organization's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior (i.e. incidents) evident in artifacts and creations that become part of processes in the organization to protect its information assets. This information security culture changes over time". Essentially this says that attitudes, assumptions, beliefs, values, and knowledge drive employee behaviors related to the organization's information and information systems.

While focused on the security of an organization's data, networks, and systems, the concept of cybersecurity culture differs in a fundamental way from an information security culture. According to the National Institute of Standards and Technology's (NIST) 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," while cybersecurity is the "ability to protect or defend the organization from cyber-attacks". Information security culture emphasizes behaviors that comply with information security policy, while a cybersecurity culture includes not only compliance with policy, but also personal involvement in organizational cybersecurity culture.

Therefore, in this research, we define organizational cybersecurity culture as "the beliefs, values, and attitudes that drive employee behaviors to protect and defend the organization from cyber attacks", including both in-role and extra-role behaviors.

A goal for cybersecurity managers is to drive cyber-secure behaviors. This can be achieved, in part, by creating an organizational cybersecurity culture (the beliefs, values and attitudes). The culture, in turn, is influenced by both external factors outside the control of managers, and internal managerial mechanisms that managers can use.

➔ Behaviors

Since cybersecurity is more than a technical issue, organizations need to rely on the employees' behaviors to prevent and protect the organization from potential cyber-attacks. Behaviors include those done as part of their job (in-role) and those done as part of the community (extra-role). Ultimately, employee behavior can create or reduce cyber-based vulnerability.

➔ Values, Attitudes and Beliefs

Values, attitudes and beliefs are unwritten rules that many know but few can articulate. However, they can be observed in actions taken by leaders, groups, and individuals in an organization.

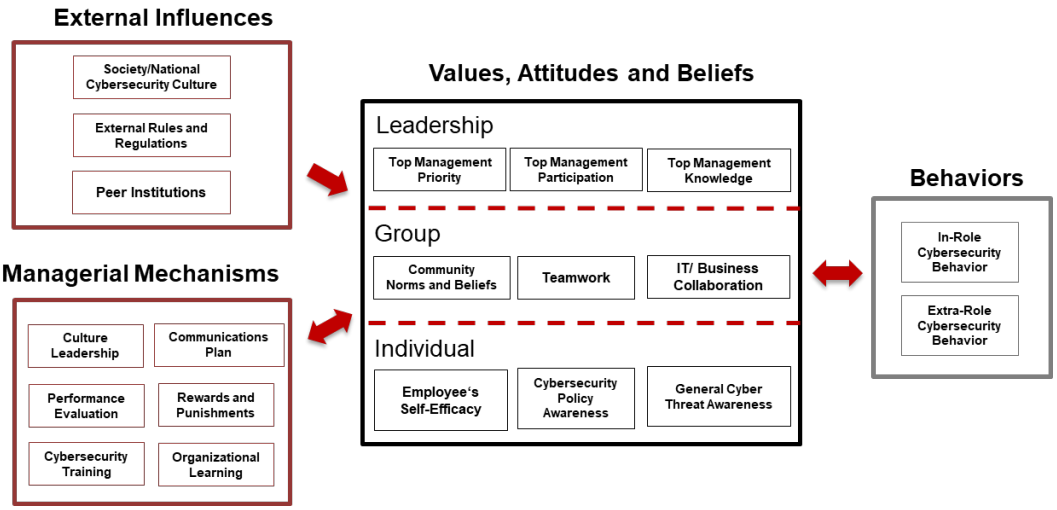
➔ Managerial Mechanisms

Beliefs, values, and attitudes are created by the actions of managers and leaders which we have labeled managerial mechanisms. Managers can use these managerial mechanisms to influence values, attitudes, and beliefs, and these mechanisms in turn are driven by culture.

➔ External Influences

The attitudes, beliefs, and values about cybersecurity are also shaped by external factors beyond the organizational boundary, including society/national cybersecurity culture, external rules and regulations, and peer institutions.

Figure i.1. Cybersecurity Culture Model *(please refer to Appendix A for definitions of all factors)*



Source: K. Huang and K. Pearlson, "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture", MIT CAMS 2019 / HICSS 2019. https://scholarspace.manoa.hawaii.edu/bitstream/10125/60074/0634.pdf

II. Survey Summary

i. Survey Methodology

Survey Structure Breakdown

Section 1: Values, Beliefs, Actions and Behaviors

Section 2: Internal / External Managerial Mechanisms

Section 3: Background Information

- The study population consisted of managers and leaders in companies that are research consortium members, cyber security professional conference attendees, or MIT-affiliated alumni interested in this research.
- There was no compensation or payment for participation. For this survey, 187 subjects participated. 110 surveys were completed.
- The method of recruitment was through emails to consortium members, interested MIT alumni, and requests at conference presentations made by MIT researchers.
- The survey was conducted online. There was no personal identifying information on this survey and answers were completely anonymous.

The survey consisted of 25 cybersecurity culture questions and 10 background questions.

- The cybersecurity culture questions were answered on a Likert Scale, from Strongly Disagree to Strongly Agree (1-5).
- The length of respondent involvement ranged from about 5 minutes to 15 minutes.
- All participants provided informed consent upon taking the survey.

ii. Demographics Profile

Overview:

- The study received **110 completed surveys** and only these completed records are used for analysis.
- Respondents came from **11 industries** (*Figure ii.1*)
  - The top 5 industries in terms of respondents contributed 84 (76.36%) records, including the government & military, financial and insurance services, information technology and technology services, educational institutions, and health care.
- Respondents ranged over **8 company positions** in their organization (*Figure ii.2*)
  - Of the 110 respondents, 69 of them work within the Cybersecurity/Security division in their organizations, including C-level cybersecurity executives, cybersecurity department managers and cybersecurity staff; while only 22 (20%) were from non-IT or non-cybersecurity related positions.
- Respondents came from **18 countries** around the globe (*Figure ii.3*)
  - Respondents came from 18 countries around the globe, but **68.1% were from the United States**, and 12 of the 18 countries only had one representing respondent.
  - This study primarily looked at each respondent's own perception of cyber-resiliency in his/her workplace to identify and categorize the responses, while the comparison cross different national culture is out-of-scope for this report.

Figure ii.1: Respondent Industries

Industry	# Count (out of 110)
Government & Military	27
Financial and Insurance Services	19
Information Technology and Technology Services	19
Educational Institutions	11
Healthcare, Medical Providers & Medical Insurance Services	8
Nonprofits	5
Manufacturing	5
Consulting Services	5
Retail/Merchant-Including Online Retail	4
Other	4
Science and Engineering	3

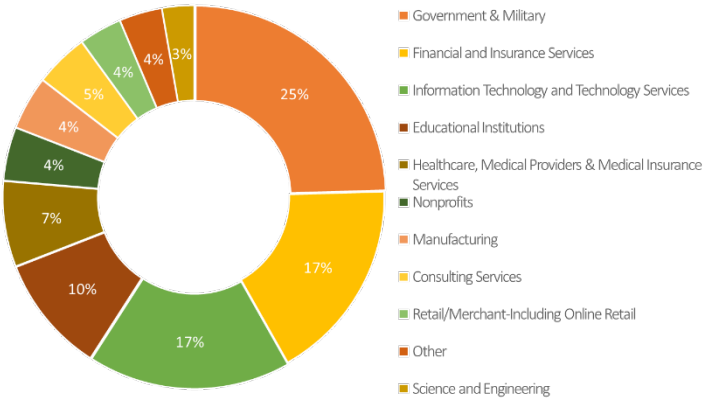


Figure ii.2: Respondent Positions in Organization

Position in Organization	# Count (out of 110)
C-level Cybersecurity Executive (CISO, CSO, CIO, CTO, etc)	24
Cybersecurity Department Manager	23
Cybersecurity Staff	22
IT Staff	10
Business Department Manager	8
Business Unit Staff	8
IT Department Manager	8
C-level Business Executive (CEO, COO, CFO, CHrO etc)	6
Other	1

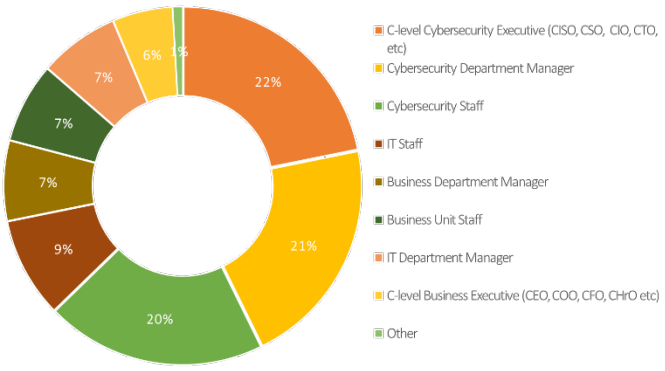


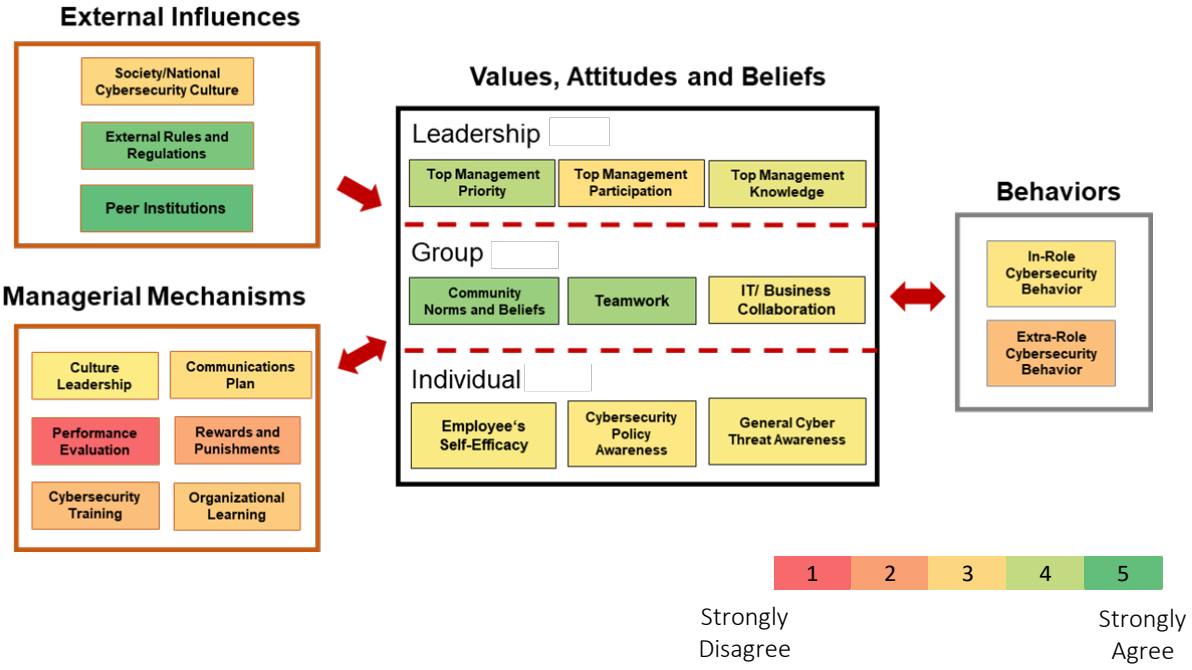
Figure ii.3: Respondent Countries c

Country	# Count (out of 110)
United States of America	75
Sweden	10
Canada	6
Argentina	2
Netherlands	2
United Kingdom of Great Britain and Northern Ireland	2
Brazil	1
Chile	1
Colombia	1
France	1
Hong Kong (S.A.R.)	1
Iraq	1
Italy	1
Jamaica	1
Japan	1
Malaysia	1
None	1
Pakistan	1
Saudi Arabia	1

iii. Panoramic View

To analyze the survey, we coded the Likert Scale responses of strongly disagree to strongly agree with the numbers 1-5. For each component within our organizational cybersecurity culture model (OCCM), we calculated the average score of the related questions from the 110 completed records, representing the overall view from the survey participants. The survey design allows for an analysis of different levels for each construct. In the figure below, green indicates higher levels than yellow. Red is the weakest, or lowest, levels.

Figure iii.1: Survey Results (ALL) Heat Map



Here are some key findings from the heat map shown in Figure iii.1

- Most responses consistently agree that the external rules and regulations and the peer institutions serve as the most common influences of cybersecurity culture performance. However, there is a lack of societal or natural cybersecurity influences.
- All the managerial mechanisms scored relatively low, with the average around 2.5. This indicates a lack of mature managerial mechanisms in fostering a more cyber-resilient workplace. More specially, the performance evaluation, and the rewards and punishments are scored lowest, indicating a lack of consequences for cyber positive or negative behaviors.
- Of the three organizational layers of values, attitudes, and beliefs, responses indicate the lowest level at the individual layer. Though this may be impacted by the position bias, these results suggest the need for cybersecurity managers to focus on improving employees' cyber capability and awareness to the cybersecurity policy and general cyber threat.
- There is a significant gap between in-role cybersecurity behavior and extra-role cybersecurity behavior. There is value in driving the attitude that cybersecurity is something everyone needs to do.

iv. Cybersecurity Culture Level Analysis

All respondents were asked to select a statement (below) that most closely describes their sentiment about cybersecurity in their organization.

Cybersecurity Participate Level

(a) Cybersecurity is not discussed in our organization. When we procure technology and/or systems, cybersecurity features are not high on our priority list.

(b) Cybersecurity is primarily handled by the technology and systems we use. The security features built into our systems (such as firewalls, password encryption, etc.) provide the majority of our cybersecurity defense and that is sufficient for us right now.

(c) Our cybersecurity leaders, such as our CIO or Chief Information Security Officer (CISO), or Chief Security Officer (CSO), own the mission of keeping our company cybersecure. They lead most cybersecurity initiatives around here.

(d) Our business managers understand cybersecurity risks and are often involved in designing and promoting cybersecurity activities in their teams.

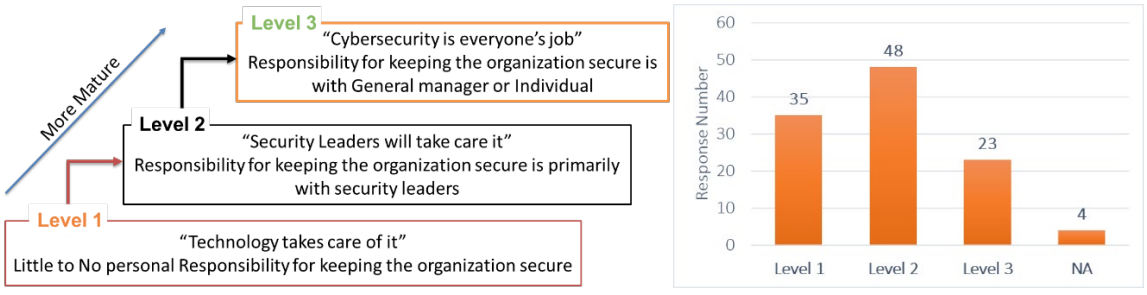
(e) Everyone in our organization feels personal responsibility for cybersecurity in our company. Often my colleagues and I take additional measures (voluntary and as part of our jobs) to make sure our data and systems are protected.

(NA) Does not apply or do not know what cybersecurity sentiment is most accurate for my organization.

Each statement represents one of three levels of sentiment towards cybersecurity in the organization. The results of these questions are shown in fig. 1.

- **Level 1: Little to no personal/managerial responsibility of keeping the organization secure (a+b)**
- **Level 2: Responsibility of keeping the organization secure is primarily with IT, CIO, CISO (c)**
- **Level 3: Responsibility of keeping the organization secure is with general organization managers/leaders or with individual employees (d)**

Figure iv.1: Cybersecurity Culture Level based on Responsibility Perception



The following sections will analyze each construct of the model in detail, and how the answers changed with the three levels of this maturity model to determine significant factors and insights for increasing the maturity of an organization's cybersecurity culture.

Please refer to Appendix B for the complete heat maps for three levels.

External Influences

The attitudes, beliefs, and values an individual or an organization has about cybersecurity are shaped by external factors, including the general society environment, the related regulations and industry rules, and the practices of peer institutions.

- Looking at the responses, there is a consensus that cybersecurity is important in all industries, and rules and regulations are factors influencing cybersecurity culture.

Figure iv.2: Responses for External Influences (Over view)

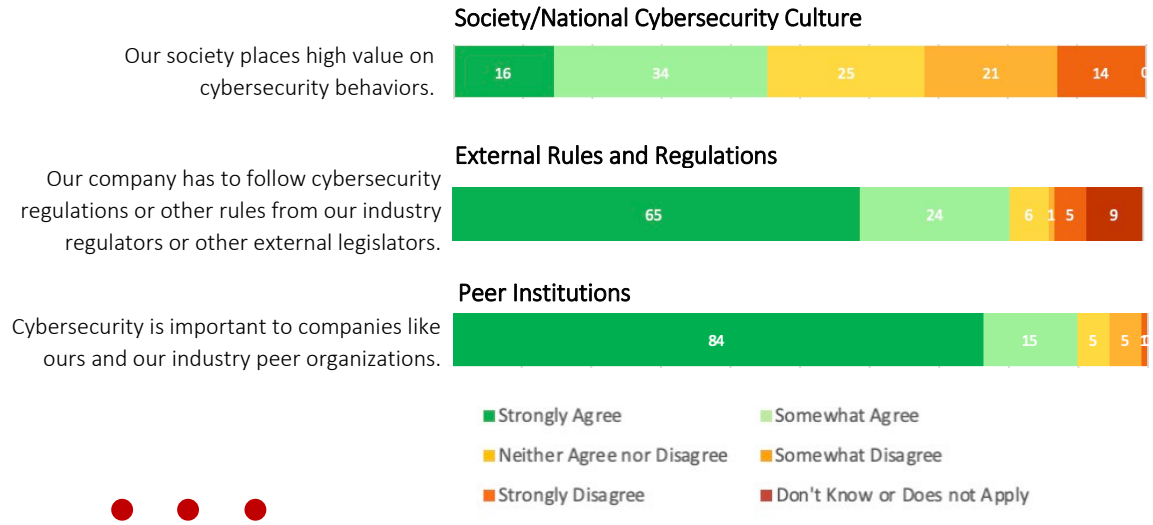
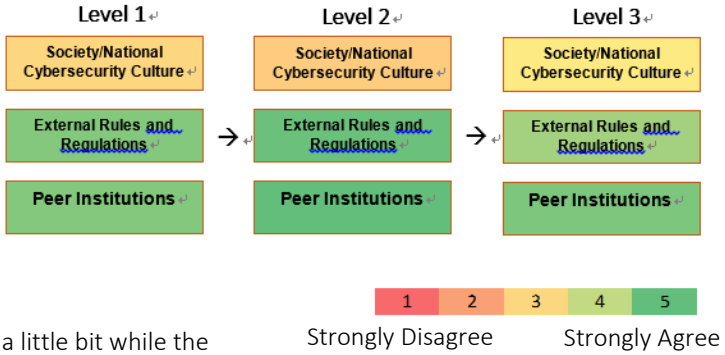


Figure iv.3: Responses for External Influences (BY LEVEL)



By dividing the responses into the three maturity levels, we can observe a slight increasing score for external rules and regulation, and peer institutions but a decrease in society /national cybersecurity culture from level 1 to level 2. However, from level 2 to level 3, the scores for both external rules and regulations, and peer institutions decrease a little bit while the score for society/national cybersecurity culture increases. These suggests that:

- Complying with the external industry rules and regulations, and learning from peer institutions plays a role in advancing cybersecurity culture by increasing the values, attitudes, and beliefs of cybersecurity leaders.
- However, for general managers and individual employees, the impact from regulations and peer institutions decreases. Instead, the society/national cybersecurity culture is more important to improve the general managers' and individual employees' values, attitudes, and beliefs regarding cybersecurity.

Managerial Mechanisms

Beliefs, values, and attitudes underlie the unwritten rules, but they are created by the actions of managers and leaders. Here are some observations from the data we collected.

- Within all managerial mechanisms, the score was highest for the cybersecurity culture leadership. The establishing of a leader to build a cybersecurity culture is impactful.
- Performance evaluation and rewards/punishments scored lower than the other managerial mechanisms. Performance evaluation was particularly low, indicating a lack of use of this mechanism to influence values, attitudes, and beliefs about cybersecurity.
- Though cyber training is recognized as the most common practice, which is reported in the practice section later in this summary, few responders believe that their cybersecurity training programs are relevant and effective.
- Cybersecurity incidents, internal or external, are always an opportunity for organizational learning and promoting a cybersecurity culture.
- The communication about cybersecurity within organizations is an opportunity, as only around 52.73% responses agree, or somewhat agree, that there is regular communication from the cybersecurity team happening today.

Figure iv.4: Responses for Managerial Mechanisms (Over view)

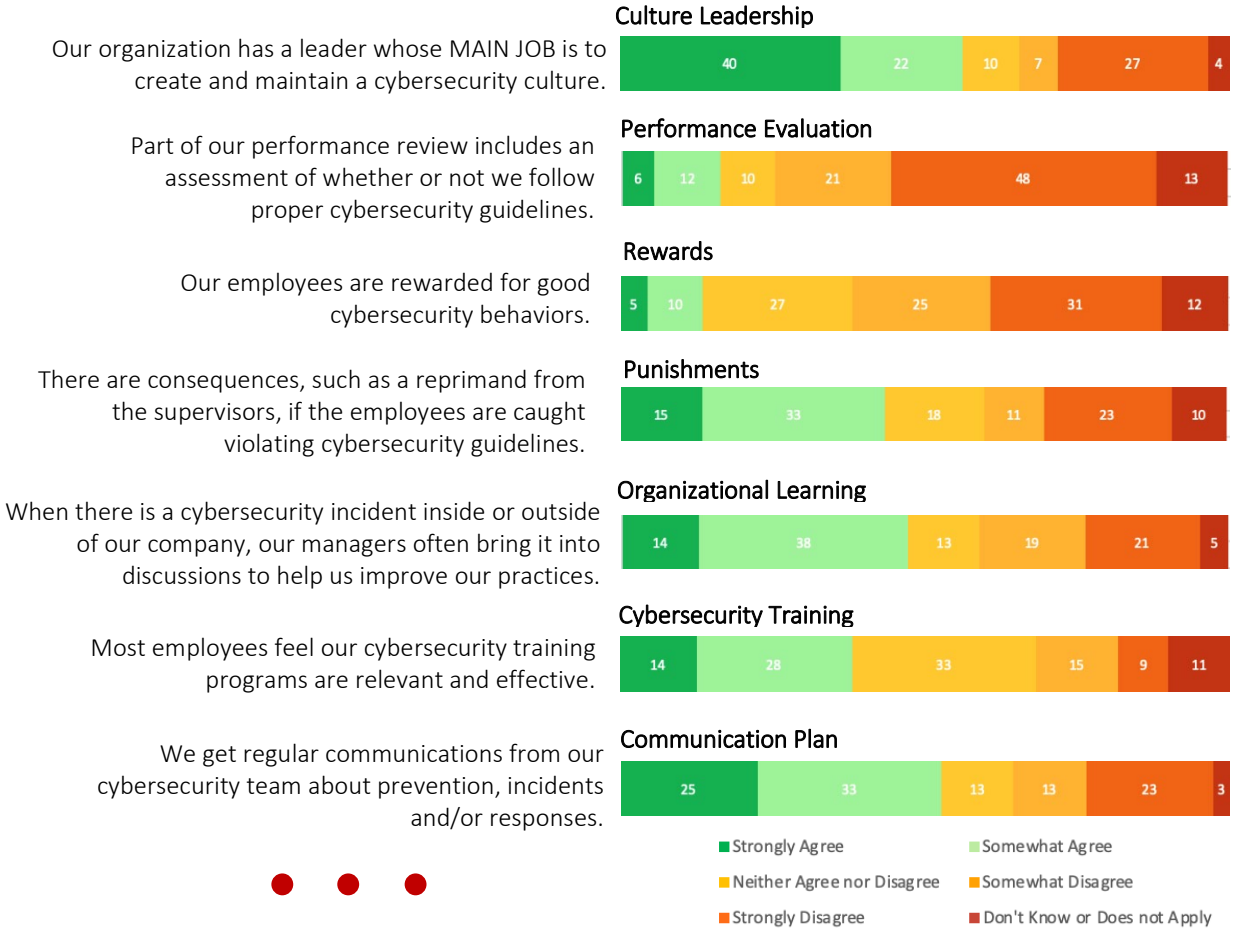
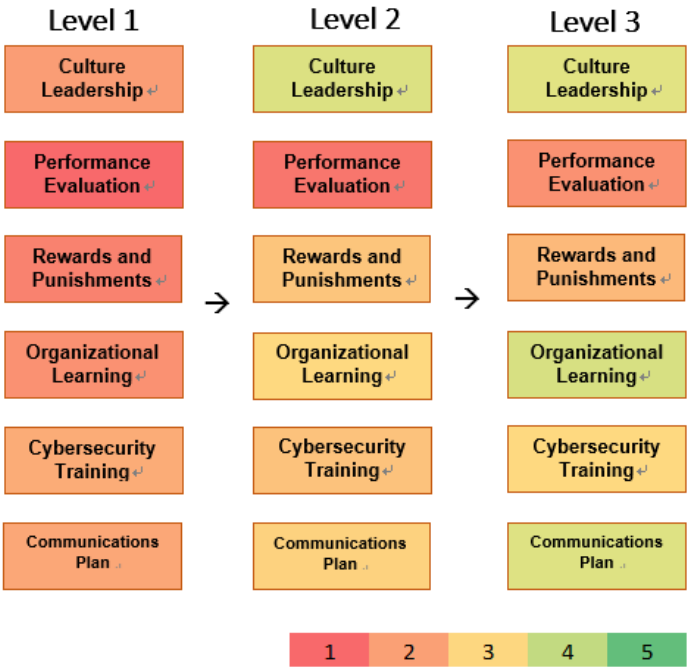


Figure iv.5: Responses for Managerial Mechanisms (BY LEVEL)



The responses show significant differences in managerial mechanisms for different cybersecurity culture maturity levels: the score for each managerial mechanism increases for higher maturity levels. More specially:

- From level 1 to level 2, we observe a significant increase in the existence of culture leadership. This indicates that the appointment of a cybersecurity culture plays an impactful role in creating a cybersecurity culture.
- To continually advance the cybersecurity culture maturity and engage the involvements from general managers and individual employees, the organizational learning and communications play an important role.
- Performance evaluation and rewards/punishments scored low for all the three levels with a slight increase. This may be because organizations lack a metric for measuring individual cybersecurity behavior was not fully developed so it is difficult to evaluate the rewards and punishments given in an organization. Our discussions with industrial leaders showed a debate about the efficiency and design challenge for the rewards and punishments mechanisms in different organizational environments.
- Cyber security training was rated relatively low for all levels of maturity, indicating an opportunity to improve the quality of these actions.

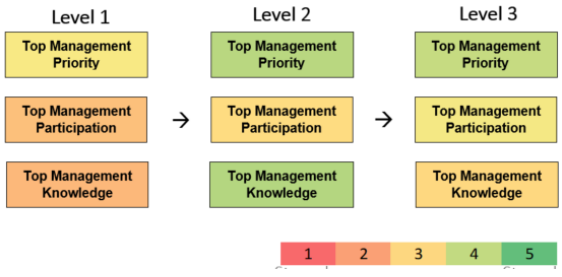
Values, Attitudes, and Beliefs (Leadership Layer)

Values, attitudes, and beliefs make up the culture, or are the unwritten rules that everyone knows but few can articulate, which can be observed in actions taken by leaders, groups, and individuals in the organization. The leadership in an organization plays a significant role in creating and propagating the organization's culture. Top management are the decision makers for investing limited resources, and examples which influence cognitive beliefs.

- 70.91% of responses strongly or somewhat agree that leaders make cybersecurity a high priority in the organization. However, the top management's participation and knowledge about cybersecurity scored lower. This indicates the necessity of promoting the "real" involvement from the top management team for cybersecurity culture building beyond just highlighting the priority of cybersecurity.

Figure iv.6: Responses for Value, Attitudes and Beliefs from Leadership Layer (Over view)

Figure iv.7: Responses for Leadership Layer (BY LEVEL)



When looking into the responses among the maturity levels, we observe a significant increase in scores for all three leadership components from level 1 to level 2; however, from level 2 to level 3, the scores decrease, especially for the top management knowledge and participation. This might indicate that the involvement from top leadership does cultivate a better cybersecurity culture when none exists. However, to move a step further and engage everyone in cybersecurity practices, top management must continue to indicate that cybersecurity is a priority and participate.

Values, Attitudes, and Beliefs (Group Layer)

Organizations are people who work together to execute business processes that make up the business activities. Groups of individuals collaborate, create, and communicate. By doing so, they build shared values and beliefs that are artifacts of cybersecurity culture.

- Most responders (84.55%) to this survey strongly or somewhat agree that community norms and beliefs are important and 79.09% believe that they share the responsibility among their team to support each other in creating a more cyber secure environment. However, the collaboration between IT and businesses to manage cybersecurity incidents is more challenging. 54.55% responses believe they have a regular and effective collaboration between the IT and business divisions. Note that this may be explained by any bias related to the positions of the responders.

Figure iv.8: Responses for Group Layer (Over view)

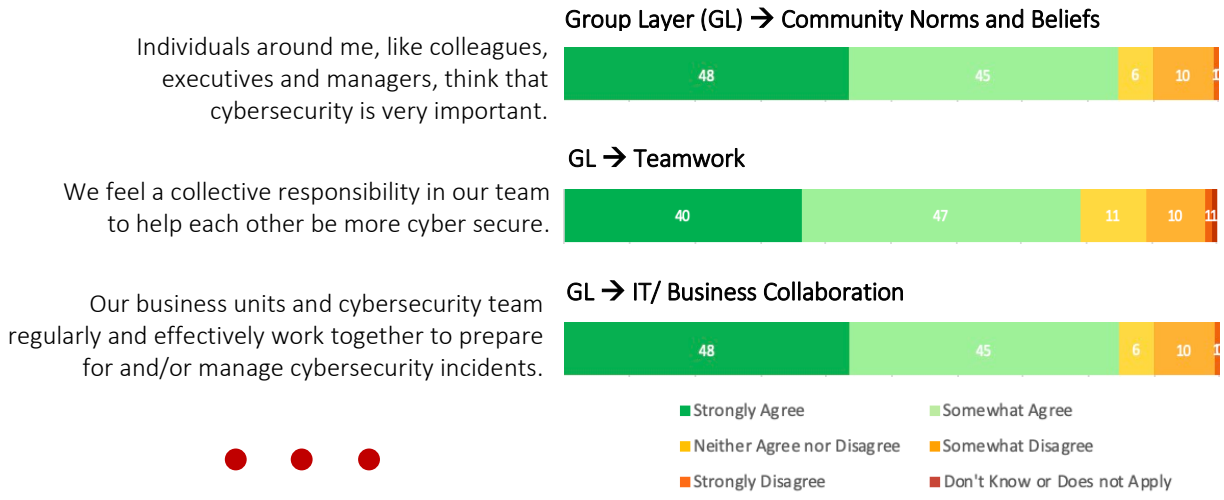
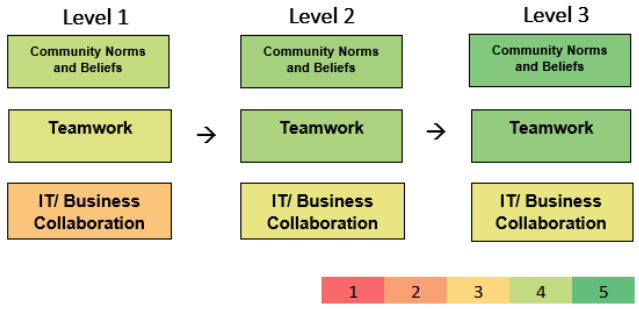


Figure iv.9: Responses for Group Layer (BY LEVEL)



The results showed a positive correlation between the cybersecurity culture maturity levels and group layer components. More mature cybersecurity cultures showed a higher value, especially community norms and beliefs and teamwork. The relatively lower score of IT/Business collaboration within all three maturity levels suggests a gap that cybersecurity culture leaders should focus on to improve their cyber-resiliency. Coordinating cross-departmental collaboration is a challenge, and figuring out how to strengthen this collaboration can be helpful in raising organizational cybersecurity.

Values, Attitudes, and Beliefs (Individual Layer)

The third set of constructs indicate individual employee beliefs. This includes an understanding of cyber threats, awareness of organizational cybersecurity policies, and knowledge of personal capabilities to impact security. When individuals understand and know how to act, it is more likely that they will behave in a manner consistent with increasing cyber resilience.

- Overall, comparing with the leadership, group, and individual layers, the components within individual layers have lower scores, indicating an opportunity to improve cybersecurity culture values, attitudes, and beliefs of individual employees. More specifically, only 56.36% responses strongly or somewhat agree that their employees are aware of the cybersecurity rules and procedures, and have the necessary skills and capability to follow them, while slightly fewer responders (53.64%) believe that employees understand the risk posed by poor cybersecurity practices in general.

Figure iv.10: Responses for Individual Layer (Over view)

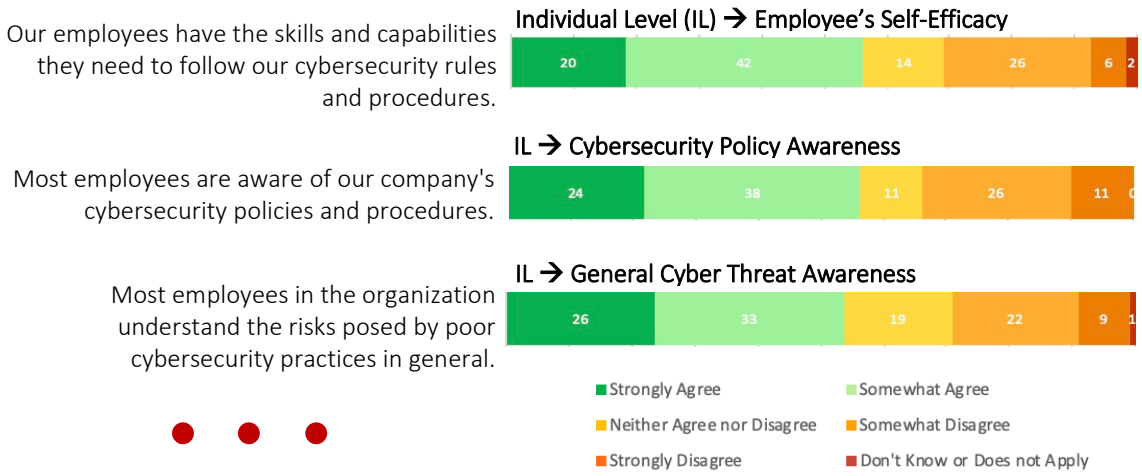
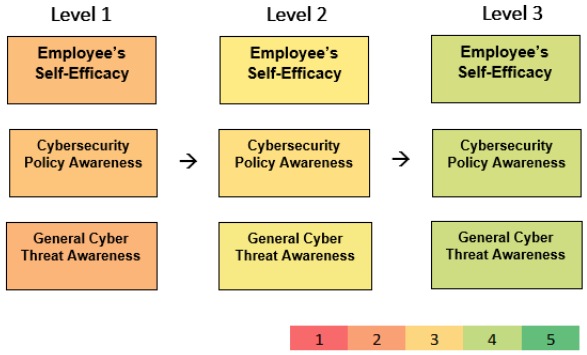


Figure iv.11: Responses for Individual Layer (BY LEVEL)



The results showed a positive correlation between the cybersecurity culture maturity levels and the constructs at the individual layer. This trend emphasized the importance of individual involvement in creating cybersecurity culture within an organization. Of the three organizational layers (leadership, group and individual), the individual layer was the greatest indicator of the cybersecurity culture maturity. As opposed to cybersecurity being just on the minds of employees (Level 2) or not in mind at all (Level 1), the data showed that an increase in employees' personal responsibility contributed to a generally higher cybersecurity culture maturity level.

Behaviors

Organizations need to be able to rely on the employees' behaviors to prevent and protect the organization from potential cyber-attacks. Ultimately, employee behavior can create or reduce cyber-based vulnerability. Many studies suggest that most cyber breaches occur because of human error. Reducing this error is a primary goal of creating a cybersecurity culture. In-Role Cybersecurity Behaviors are the behaviors that all employees do as part of their job role to increase resiliency in an organization. Extra-Role cybersecurity behaviors are activities outside of an employee's role that the employee does to help to increase organizational cyber-resiliency.

- The goal of creating a cybersecurity culture within the organization is to increase the number of secure behaviors by employees. However, the data indicates a gap between the desired and actual cybersecurity behaviors. More specifically, 23.64% strongly agree that most employees do what is required for their job role while only 11.82% strongly agree that many employees do more than what is expected.

Figure iv.12: Responses for Behavior (Over view)

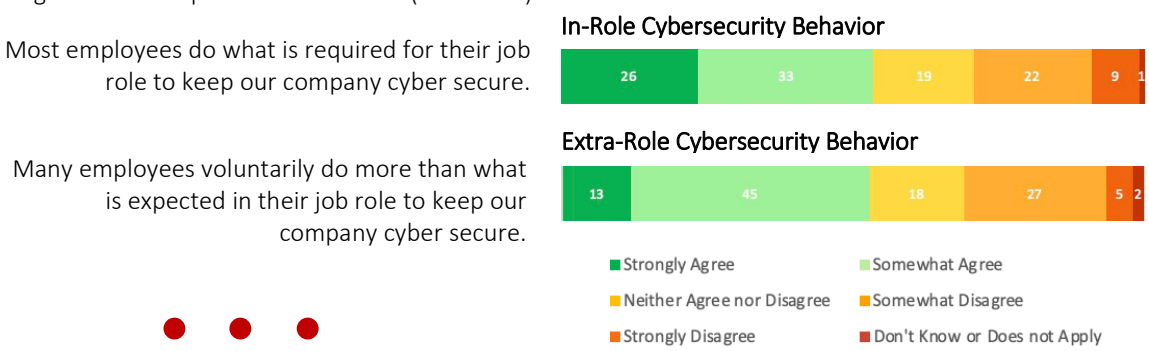
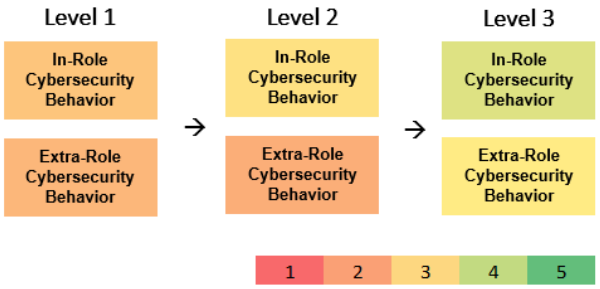


Figure iv.13: Responses for Behavior (BY LEVEL)



The responses indicated that as the levels of cybersecurity culture maturity increase, the perceptions of employees' cyber secure behavior, both in-role and extra-role behavior, increase. This confirms the importance of motivating the employees' behavior. More interestingly, comparing the in-role and extra-role behavior, we observed an increase in-role behavior between level 1 to level 2 and a significantly larger increase of extra-role behavior between level 2 to level 3. This suggests that leaders who motivate employees to be more cybersecure in their job are more successful in more mature cultures. However, to improve cybersecurity maturity, leaders should encourage the employees to contribute voluntarily to improving the workplace cyber-resiliency in all areas of their interaction within the community.

v. "Best" Practices to drive cybersecurity behaviors

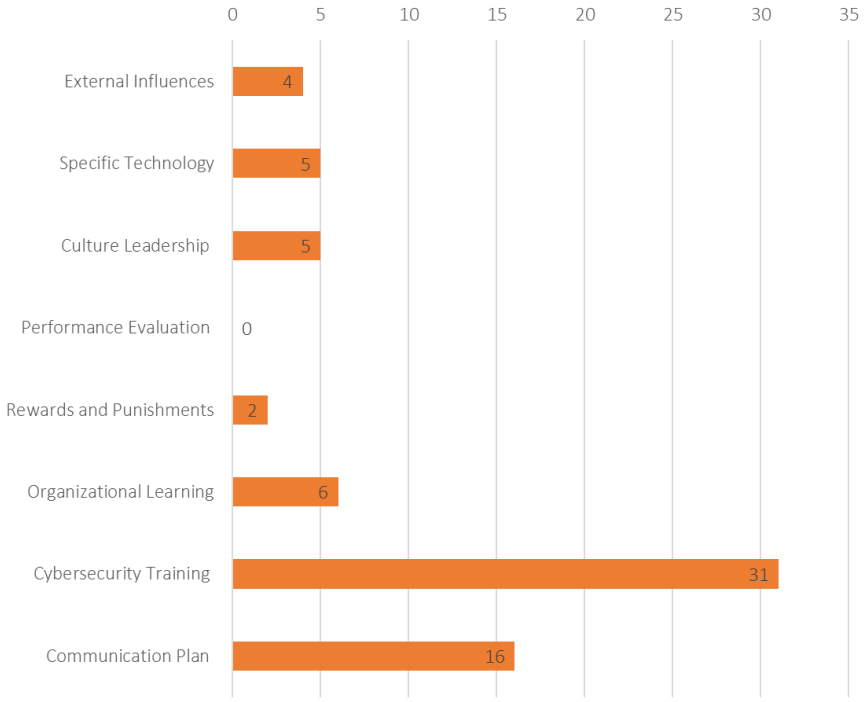
Participants were asked to share some examples of practices or activities they have seen implemented to drive cybersecurity behaviors in an organization. Common responses included: creating cybersecurity policies and awareness campaigns, mandatory employee training in cybersecurity, and internal phishing exercises. A word cloud was produced from this data to highlight the qualitivative answers to this question.

Figure v.1: Response Word Cloud

55 respondents gave suggestions on their cybersecurity culture best practices.

- The 55 suggestions were categorized into *External Influences*, Special Technology, and/or the six *Managerial Mechanisms. (Please refer to Appendix C for the full list of respondent suggestions)*
- The graphs below highlight the most common practices used in organizations for maintaining and growing Cybersecurity Culture. Note: suggestions can be sorted into more than one category.

Figure v.2: Categorizing Organizational Best Practices Suggestions (55 Responses)



Based on the survey results, **Cybersecurity Training** was the most popular suggestion shared by respondents. Some typical examples include:

"'Don't Feed the Phish'-Mandatory online training to educate the company about how to avoid phishing attacks."

"Periodic mandatory training on cybersecurity practices and insider threats"

"Mandatory training, active infosec dept, sysdev and sysops training"

"Randomly timed social engineering testing"

"Training and table top simulation exercises"

Having a robust **Communication Plan** was also a method suggested by many respondents. This indicates the awareness of the importance of good "information sharing" practices for the organizational cybersecurity culture building. For example:

"Internal talks, both on specific ways we can improve, but also on technologies and general problems in the space".

"Our managed desktops use screensavers with various cyber security best practices"

"Lunch & Learn including industry experts on data, privacy, law enforcement"

"Occasional emails warning about suspicious behavior"

The other mechanisms were relatively low in response to this question, including the **Culture Leadership** and **Organizational Learning**. One response with position "C-level Cybersecurity Executive" provided an interesting example highlighting the importance of **leadership**:

"Getting rid of an ineffective CISO and bringing in a new CISO"

We observed few practices for **organizational learning**, although responses received suggested learning practices are varied and possibly non-impactful.

"8-12 articles annually disusing recent incidents and best practices on company intranet"
"There was a cyber-threat briefing held by the CISO a few years ago that every employee had to attend, ordered by the board after a major cyber incident. But it was a one-off effort and nothing similar has been done since."
"Interest was brief after a breach of employee personal data. It quickly faded."

Another thing to note is the lack of mention of **Performance Evaluation** by the respondents. This suggests an opportunity for an employee cybersecurity evaluation metric, which can make it easier to formalize an evaluation process. We did receive some interesting examples of **Rewards and punishments** from our respondents:

"if you lost your laptop - you lose your job"
"Reward & Recognition of Cyber Practices"

Beyond these six managerial mechanisms, several **specific technologies** were mentioned by the respondents, including:

"MFA (Multi-factor authentication) "
"next generation firewall"
"LastPass and Yubikey "
"Biometric Authentication on the Blockchain"
"cybersecurity vulnerability scanning tools, configuration management and release mechanisms built with 100% free and open source (FOSS) software"

"ISO 27001 implementation and certification" is the standard most often mentioned by the respondents. Interestingly, one respondent commented that the implementation of ISO 27001 certification was "*at customers request*" and "*security was not a priority prior to this request*".

Please refer to Appendix C for the complete survey results of the suggested practices.

III. Conclusion

To grow an organization's cybersecurity culture, management must not only implement the latest technology but also invest in the organizational culture. Based on the Organizational Cybersecurity Culture Model (OCCM) developed by Cybersecurity at MIT Sloan (MIT CAMS), a survey of individuals from 11 different industries crossing 18 countries showed that the model can help describe factors that create a cybersecurity culture across different maturity levels and identify the gaps and challenges of building a cybersecurity culture. The OCCM can be used as a roadmap for advancing cybersecurity culture and driving more cybersecure behaviors.

The data from this survey demonstrated the importance of the managerial mechanisms for building a cybersecurity culture. These mechanisms are still immature for many organizations. The cybersecurity culture leader is recognized as a critical role to increase the cybersecurity culture maturity level. Although cybersecurity training is the most popular leading practice, the effectiveness of cybersecurity training is doubted by many respondents. There was also a lack of systematic mechanisms for communication plans and organizational learning. Performance evaluations and rewards and punishments are additional mechanisms that managers can use to influence values, attitudes, and beliefs.

The unwritten rules were evident at three organizational layers: leaders, groups, and individuals. Individuals are not sufficiently aware of cybersecurity policies and general cyber threats, highlighting an opportunity for leader attention. Further investing in increasing top managers participation, knowledge, and group collaboration between IT and business teams will increase culture maturity and drive more cybersecure values, attitudes, and beliefs.

Finally, both in-role behavior and extra-role behaviors are indicators of the level of organizational cybersecurity culture maturity. A higher-level maturity both encourages employees to follow organizational policy and voluntarily take on extra behaviors such as sharing knowledge, helping others to avoid risky behavior, and making daily efforts to improve cyber-resilience. Driving the attitude that cybersecurity is something everyone needs to do and that everyone can contribute to create more cyber-resiliency is at the core of cybersecurity culture.

IV. Acknowledgement

The research reported herein was supported by the Cybersecurity at MIT Sloan (MIT CAMS), which is funded by a consortium of organizations. MIT CAMS welcomes funding from sponsors for general support of the consortium research, and from organizations interested in specific research topics.

The authors would like to thank all the CAMS members and partners for making this research possible and to all the participants providing their responses to this survey. Thanks also to the $(ISC)^2$ annual conference participants and everyone who attended the MIT CAMS annual conference and seminars. Your input was insightful and valuable. The authors also would like to thank Suki Zhang and Lara Warren for their research assistance. All errors remain the responsibilities of the authors.

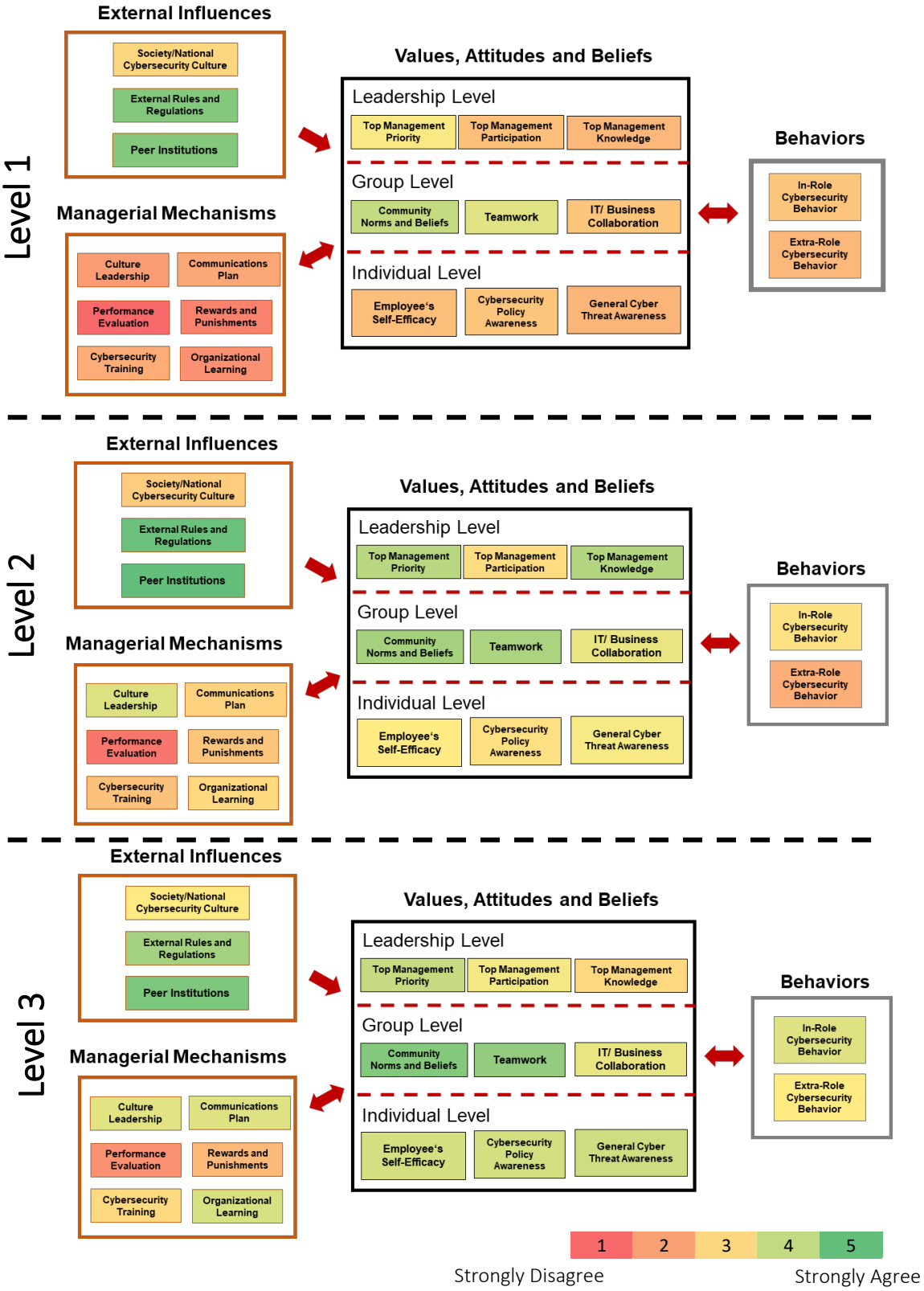
Please contact Dr. Keman Huang, keman@mit.edu, or Dr. Keri Pearlson kerip@mit.edu if you have any comments and further interests in this research. For more information about MIT CAMS, please visit: https://cams.mit.edu/.

V. Appendix

Appendix A: Cybersecurity Culture Model Definitions

	External Influences
Societal Cybersecurity Culture	the culture of the society in which an organization resides
External Rules and Regulations	the laws, guidelines, and regulations imposed by government and other industry organizations
Peer Institutions	the pressure felt by managers in an organization from actions their peer organizations have taken
	Managerial Mechanisms
Culture Leadership	the appointment of an individual or team with formal responsibility for building a cybersecurity culture
Performance Evaluation	the inclusion of measures of cybersecurity compliance and behaviors in the employee's formal evaluation processes
Rewards and Punishments	the managerial-generated impacts of cybersecurity behaviors
Organizational Learning	the ways the organization builds and retains cybersecurity knowledge
Cybersecurity Training	courses and exercises that develop cybersecurity skills and knowledge
Communications Plan	coherent, well-designed messages about cybersecurity communicated using multiple methods and networks
	Cultures, Values, and Beliefs
Top Management Priority	when top managers believe that cybersecurity is important, they will make cybersecurity a priority for the organization
Top Management Participation	the top management's personal involvement in the cybersecurity-related activities
Top Management Knowledge	the cybersecurity-related knowledge, skills and competencies leaders have
Community Norms and Beliefs	the collective set of ideas the group has about cybersecurity
Teamwork	the way teams within the organization work together to be more cyber secure
IT/Business Collaboration	the work done between groups of individuals from different parts of the organization
Employee's Self Efficacy	a person's knowledge about how well he or she can personally execute actions to increase cybersecurity
Cybersecurity Policy Awareness	the individual's knowledge of what behaviors the company seeks
General Cyber Threat Awareness	the individual's knowledge and understanding of threats
	Behaviors
In-Role Cybersecurity Behavior	the actions and activities an employee takes as part of their official role in the organization
Extra-Role Cybersecurity Behavior	actions and activities an employee does that are not part of their job description

Appendix B: Heat Maps for three Culture Levels



Appendix C: Suggested Best Practices

occasional emails warning about suspicious behavior
seminars; mandatory training; treasure hunts; games
Report if there is bug over SLA, Security policy violations
Regular explicit training, external red-teaming, all-hands presentations, ubiquitous discussion in culture, separate internal- and external-facing email systems.
online self test required yearly
Internal SpearPhishing Exercises
We treat employees as "sensors" who are encouraged to detect and report cyber events. We are responsible and held accountable for patching our own systems.
Training, fake phishing emails
E-Mails to test employees on accessing
I give lots of internal talks, both on specific ways we can improve, but also on technologies and general problems in the space.
Security Awareness Training monthly, Simulated phishing tests, posters, newsletters
Yearly training
Training and table top simulation exercises
Security awareness videos
Biometric Authentication on the Blockchain
Annual training requirement for all employees; quarterly "fake phishing" exercises to test employees; bi-annual discussion at Corporate Town Halls; 8-12 articles annually disusing recent incidents and best practices on company intranet; proprietary software looking for improper downloads and/or IP addresses that are not typically used/
mandatory cyber security awareness training, phishing simulaitons
Regular phishing exercises for training
Employee education. Tech solutions are good, but education is best
New it-strategy with principals for cyber security
Regular password changes, approved company-wide shared cloud platform, limited access to web services,
periodic mandatory training in cybersecurity practices and insider threat
Security (Cyber) Strategic Plan & Roadmap mapped to the Customer Experience Strategy; Reward & Recognition on Cyber Practices; Lunch & Learn including industry experts on data, privacy, law enforcement; Change Management Program on Best Practices to Security and Cyber.
Mandatory for new employees to sign a User Agreement including an Acceptable Use and Cyber Security Policy. It's never followed up on though. There was a cyber threat briefing held by the CISO a few years ago that every employee had to attend, ordered by the board after a major cyber incident. But it was an one-off effort and nothing similar has been done since. Top priority is focus on the core business and cyber security is not a main concern.
LastPass and Yubikey send-factor used by all employees both for work and personal use.All cybersecurity vulnerability scanning tools, configuration management and release mechanisms, etc. are built with 100% free and open source (FOSS) software. Bringing modern cybersecurity practices to US Federal agencies (DoD, HHS, DoED, etc.) is difficult as they want FISMA compliance with 3-year ATO schedule, which is far from appropriate to manage today's threat landscape. But getting an AO to look at (e.g.) GitHub or Graylog dashboards can be surprisingly difficult, as MS Word documents are more within their comfort zone.
Phishing testing, currently annual awareness training. Beginning stages of ISO 27001 certification at customers request, security was not a priority prior to this request.
Basic Security & Privacy Awareness eLearning Module; Phishing Awareness Exercises
"Don't Feed the Phish"-Mandatory on line training to educate company about how to avoid phishing attacks. Compliance was formally tracked throughout business. Also have annual mandatory online training on general security matters
third party contract, next generation firewall contract
Cybersecurity training for all new hires
Implemented IT Security Policy
ISO 27001:2013 implementation and certification
Annual training and frequent email notices.
RMF audit
if you lost your laptop - you lose your job
Beginning work on creating policies and procedures and incident reporting.
Getting rid of an ineffective CISO and bringing in a new CISO
KnowBe4 user training and simulated tests have been effective
Mandatory training, active infosec dept, sysdev and sysops training, publicizing incidents and MO of perpetrators, etc
Security discussed at weekly business meeting
randomly times social engineering testing
Our managed desktops use screensavers with various cyber security best practices
Interest was brief after a breach of employee personal data. It quickly faded.
annual awareness Training
Annual on-line training
Awareness training, and rewarding good behavior.
sec awareness, data protection policy
Awareness sessions
training, phishing campaigns
Phising simulations
KnowBe4 monthly training / quarterly phishing
MFA
Timely, and relevant security awareness training.
Training sessions, marking EXTERNAL on messages from outside the organization
security awareness training; phishing campaign; intranet bulletins;
limited training, phishing awareness campaigns, screen saver messages.