Profiling the Organizational Cybersecurity Culture: Toward a Cybersecurity Culture Framework

(Model Summary)

Dr. Keman Huang, Dr. Keri Pearlson

January 24, 2018

All the technology solutions available won't protect an organization from a cyber breach if the people in the organization are not equally careful and protective. People are the weakest link in information security; it only takes one person in an organization to click on a phishing email to potentially get past the technological security and bring down all the systems running a business. Worse, in some cases, a cyber breach can lock up critical information, as was seen in the WannaCry virus of 2017 or bring down critical infrastructure as was experienced in the Ukraine in 2017, when the Petra attack took the radiation monitoring system at the Chernobyl Nuclear Power Plant offline.

Building a culture of cybersecurity within an organization can guide employee's behaviors and increase cyber resilience. A culture of cybersecurity underlies the practices, policies and 'unwritten rules' that employees use when they carry out their daily activities. However, since an organization's culture is intangible, it's not easily studied. In this paper, we outline a model of cybersecurity culture that managers can use to identify decisions they can make and resources they can invest to build a more cyber-resilient culture.

The Concept of Organizational Cybersecurity Culture

To define organizational cybersecurity culture, we first need to understand three related concepts: organizational culture, national culture and information security culture.

A common definition of organizational culture comes from Ed Schein's model[1]. He suggests three components of a 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 culture based on the orientation of the values and beliefs:[2]

1. the *support* orientation emphasizes employee's spirit of sharing, cooperation, trust individual growth and the decisions can be made through informal contacts.;
2. the *innovation* orientation emphasizes that the organization is open to change and willing to search for new information, and creative in problem solving. ;
3. the *rules* orientation emphasizes the respect for authority, formal procedures, and the importance to follow the written rules, normally resulting into a top-down hierarchical

[1] Please refer to the following book for more information: Edgar H. Schein. 2010. Organizational culture and leadership, John Wiley & Sons.

[2] Please refer to this paper for more detail about the Quinn' s model: Jaap J. van Muijen and Et. Al. 1999. Organizational Culture: The Focus Questionnaire. Eur. J. Work Organ. Psychol. 8, 4 (1999), 551–568.

structure;

4. the *goal* orientation emphasizes the clear specification of the targets, the criteria for performance measurement and the reward based on the attainment of goals, reflecting the understanding of organizational goals, individual responsibility and accountability. .

National culture focuses on a cross-cultural perspective at the national level, and can impact how employees comply with authority and follow organizational rules and policies. The most accepted taxonomy of national culture, by Hofstede, consists of the six dimensions:[3]

1. "power distance index" refers to the extent to which people accept that power in institutions and organizations is distributed unequally
2. "individualism vs collectivism" refers to people's self-concept: "I" or "we"
3. "uncertainty avoidance index" refers to the degree to which people will feel uncomfortable with uncertainty and ambiguity
4. "masculinity vs femininity" stands for people's preference for achievement and material success or relationships, and quality of life
5. "long-term orientation vs short-term orientation" refers to the connection of the past with the current and future challenges
6. "indulgence vs restraint" refers to whether people believe themselves or other factors dictate their life and emotions

Information security culture, a subculture of an organization's culture, has been defined by Da Veiga and Eloff (2010) 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 the way things are done in the organization to protect its information assets. This information security culture changes over time,*" [4] which is to say, the "attitudes, assumptions, beliefs, values and knowledge" drive the employee's 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 NIST definition[5], Information security was 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 result from the compliance of the information security policy, but a cybersecurity culture not only includes this compliance, but adds an additional aspect of the employee's personal involvement in insuring organizational cyber safety. In this paper, we define organizational cybersecurity culture as "*the beliefs,*

[3] Please refer to this paper for more details: G. Hofstede. 1984. Cultural dimensions in management and planning. Asia Pacific J. Manag. 1, January (1984), 81–99.

[4] Please refer to this paper for more details: a. Da Veiga and J.H.P. Eloff. 2010. A framework and assessment instrument for information security culture. Comput. Secur. 29, 2 (2010), 196–207.

[5] Please check this document for more details: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf. In addition, this paper discusses the differences between the information security and cyber security: Rossouw Von Solms and Johan Van Niekerk. 2013. From information security to cyber security. Comput. Secur. 38 (2013), 97–102.

values, and attitudes that drive employee's behaviors to protect and defend the organization from cyber attacks."

Framework to Measure and Improve Organizational Cybersecurity Culture

To cultivate an effective organizational cybersecurity culture, we need to understand both the components that comprise the culture and the factors that influence the culture. As shown in Figure 1, organizational cybersecurity culture is *the beliefs, values and attitudes in the organization that drive cyber-secure behaviors*. These beliefs, values and attitudes are influenced by both external factors outside of the organization and by mechanisms and actions managers can take inside the organization. As depicted in Figure 1, the culture is influenced by organizational mechanisms, but since culture shapes the way things are done it can also have an impact on organizational mechanisms, hence the two-way arrows. Likewise, the behaviors are shaped by the culture, and in return, shape the culture. Again, this is depicted by the two-way arrows. External influences such as national culture, industrial sector regulations, and activities of peer organizations will impact the values, beliefs and attitudes of an organization, hence will influence the culture.

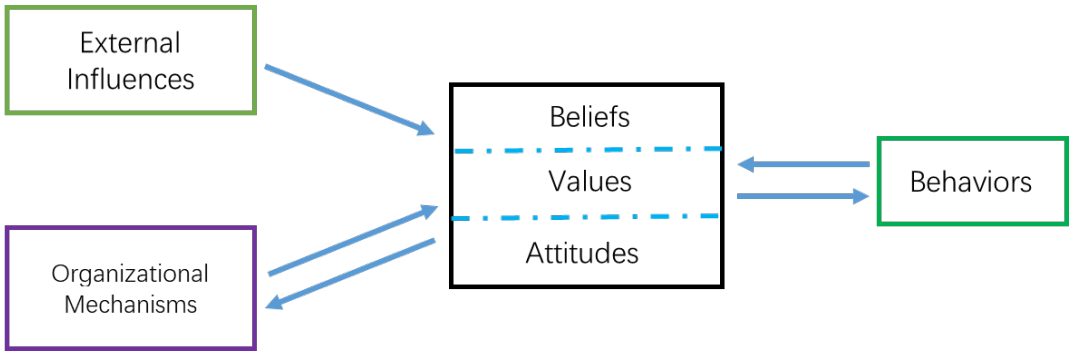

Figure 1. The conceptual framework for Cybersecurity Culture Evaluation and Improvement

Cybersecurity Beliefs, Values, and Attitudes

As shown in Figure 2, to understand, measure and promote cybersecurity culture, we consider the cybersecurity beliefs, values and attitudes for three levels of the organization: the leadership, the group and the individual.

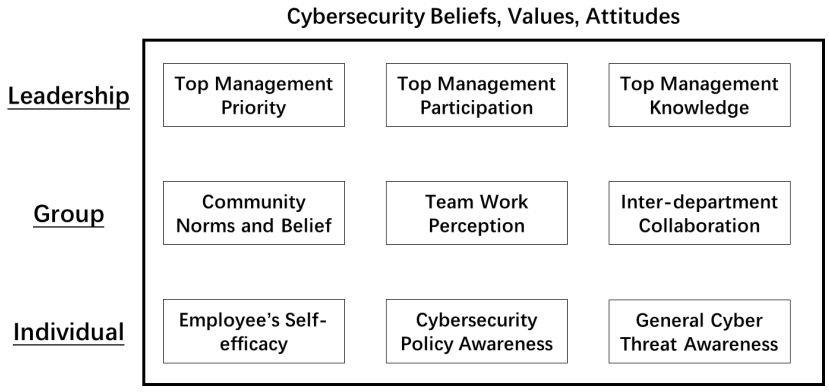

Figure 2: the three organizational levels of cybersecurity belief, values, and attitudes that create a cybersecurity culture

Leadership Level

Leadership in the form of top management, have a significant role to play in the culture of an organization. Leaders make decisions on how to invest the organizations resources, set examples for others in the organization by their own actions, and bring perspectives, skills and information to the organization. Employees build their beliefs, values and attitudes from watching what their senior leaders say and do. To understand this aspect of a cybersecurity culture, we include three constructs:

1. ***Top Management's Priorities***: this refers to the top management's psychological state regarding the importance of cybersecurity. When top managers believe that cybersecurity is important, they will make cybersecurity a priority for themselves and subsequently influence the beliefs of others in the organization about the importance of cybersecurity. "
2. ***Top Management's Participation*** refers to the top management's involvement in the organization's cybersecurity-related activities, which are observable artifacts of the values, beliefs and attitudes of the leader. Participation could be in the form of communicating cybersecurity policies and attitudes, or it could be in actions that specifically secure the organization (for example, funding training, creating games, investing in other cybersecurity solutions). Further, when employees see leaders participating in cyber-security activities, it motivates and reassures employees of the need for their own involvement.
3. ***Top Management's Knowledge*** refers to the cybersecurity-related knowledge, skills and competencies leaders have. When leaders have information about keeping their organization cyber secure, they act in ways that increase cybersecurity. Further they are more likely to share that information with others in the organization, creating stronger values, beliefs and attitudes towards cybersecurity. .

Proposition 1: The top management's prioritization of cybersecurity has a positive impact on the rest of the organizations values, beliefs and attitudes of cybersecurity.

Proposition 2: The top management's participation in cybersecurity activities indicates their values, beliefs and attitudes of the importance of cybersecurity which creates cybersecurity culture.

Proposition 3: The top management's knowledge of cybersecurity influences their values, beliefs and attitudes of cybersecurity.

Group Level

Organizations are made up of groups of people who work together to execute business processes that make up the activities of the business. Groups of individuals collaborate, create, and communicate and by doing so, they build shared values, beliefs and attitudes that comprise the culture. Three constructs summarize the group level culture.

1. ***Community Norms and Beliefs*** refers to the collective set of ideas the group has about cybersecurity. Groups form collective ideas when they work together. Individuals share thoughts and communicate values, influencing what each other believes and ultimately what the group believes. Newcomers to a group either absorb and begin to share the group norms or they are ultimately rejected by the group, making group

norms a strong component in shaping values, beliefs and attitudes. When a group norm includes a commitment to cybersecurity, this influences the culture of the organization.

2. ***Teamwork Perception*** refers to the perception of a group of individuals within the same part of an organization who work together to increase cybersecurity. Cybersecurity is a team activity and the acknowledgement of the need for teamwork to assist in creating a cyber resilience is an indicator of a strong cybersecurity culture.
3. ***Inter-department Collaboration*** refers to the work done between groups of individuals from different parts of the organization. Involvement by the information technology organization and the information security organization is expected in most organization, but collaboration beyond the cybersecurity professionals, around issues and activities of cybersecurity, is an indicator of cyber resilience in the organization.

Proposition 4: The normative social belief, the *community norm* about the importance of behaving in a cyber secure way, contributes to organizational cybersecurity culture.

Proposition 5: The teamwork perception, the collaboration on cybersecurity issues among employees on the same team contributes to organizational cybersecurity culture.

Proposition 6: The collaboration on cybersecurity issues among different groups in the organization, including business and IT groups, contributes to organizational cybersecurity culture.

Individual Level

The employees' individual understanding of cyber threats, awareness of organizational cybersecurity policies, and knowledge of their personal capabilities to impact security contribute to securing organizations. When individuals understand and know how to act, it is more likely that they will act in a manner consistent with increasing cyber resilience. We suggest that these three constructs comprise the individual level culture of cybersecurity:

1. ***Employee's Self-Efficacy*** refers to a person's knowledge about how well he or she can personally execute actions to increase cybersecurity. In an environment where individuals know what to do, feel empowered to do it, and have confidence in the actions they can take to protect the organization, they are more likely to do so.
2. ***Cybersecurity Policy Awareness*** refers to the employee's knowledge and understanding of what the organization want's done. It is not just "knowing what to do" about cybersecurity but "knowing what is wrong or right and why is important". Understanding the policies as well as what the policy means to the employee, personally, is part of policy awareness. Organizations that set up clear policies and clearly communicate them give employees a set of values and attitudes that help make the organization more cyber resilient. After all, if the employee is not aware of the policy or doesn't know what to do, then the organization is potentially less secure.
3. ***General Cyber Threat Awareness*** refers to the individual's knowledge and understanding of threats. Knowing what to look for that might be suspicious in emails, texts, attachments, and other communications employees receive is critical to keep individuals from infecting corporate systems. Employees cannot be expected to be aware of every threat and potential breach, but a general awareness is necessary to create values, beliefs and attitudes that drive cyber security behaviors.

Proposition 7: The individual's belief that they can personally impact cybersecurity contributes to the cybersecurity culture in the organization.

Proposition 8: The employees' awareness of and perceptions to learning about the general cyber threat influences their values, beliefs and attitudes about organizational cybersecurity.

Proposition 9: The employees' awareness and understanding of the organization's cybersecurity policy, influences organizational cybersecurity culture.

Creating Cybersecurity Behaviors: In-Role and Extra-Role 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. It's the behavior of the people in the system that creates or reduces vulnerability. For the purposes of this paper, employees are both permanent and temporary workers, full and part time, who have access to organizationally relevant information and systems while fulfilling their duties. There are two types of behaviors that are the outcomes of a cybersecurity culture: in-role and extra-role behaviors.

1. ***In-Role Cybersecurity Behaviors*** refers to the actions and activities an employee takes as part of their official role in the organization. For example, a help-desk engineer has certain responsibilities that come with the job such as answering emails from others who may need assistance, helping employees set up accounts and recover access, etc. Along with these specific job activities are cybersecurity behaviors that are necessary to keep the organization protected, such as reporting suspicious emails or inappropriate requests for access.
2. ***Extra-Role Cybersecurity Behaviors*** refers to actions and activities an employee does that are not part of their job description. Some examples are *helping,* referring to the cooperative behavior to aid others who might ask a cybersecurity question, and *voicing,* referring to speaking up to offer comments and knowledge to improve cybersecurity.

Proposition 10: The cybersecurity culture of the organization will impact the employees' in-role behaviors and their in-role behaviors will in turn have an impact on the culture.

Proposition 11: The cybersecurity culture of the organization will impact the employees' extra-role behaviors and these behaviors will in turn have an impact on the culture.

Organizational Mechanism for Cybersecurity

Managers have many options for influencing the culture of an organization. There are a number of decisions a manager can make and mechanisms a manager can invest in to influence the cybersecurity culture. All managers in the organization have opportunities to make decisions that can impact the cybersecurity culture. This model identifies six mechanisms managers can use to influence the cybersecurity culture, and in turn, the culture will influence these mechanisms.

1. ***Cybersecurity Culture Leadership*** refers to a formal acknowledgement of an individual or team responsible for building a cybersecurity culture. This leader might be part of the information systems organization or the information security team, or it might be outside of the technology-organization all together. The cybersecurity culture leader has responsibility to cultivate the cybersecurity culture of the organization and

has the direct power to impact the cultivation process. The leadership style and the background of the leader or leadership team, including the professional education, knowledge of cybersecurity, and work experience, will impact the effectiveness of the team in generating a cybersecurity culture.

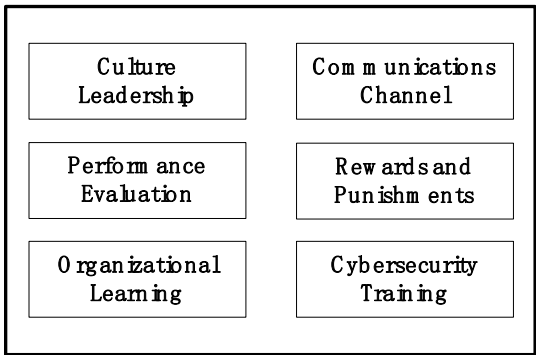

Figure 3: the organizational mechanisms for the cybersecurity culture

Proposition 12: Having specifically appointed cybersecurity culture leadership will significantly impact the organizational cybersecurity culture.

2. ***Performance Evaluations*** refers to the inclusion of measures of cybersecurity compliance and behaviors in the employee's formal evaluation processes. When an employee knows that specific behaviors are part of their annual review process they are more likely to do those behaviors. For example, when completing a required annual training program is recorded in the annual performance evaluation, employees are more likely to insure they take the training. Further, the performance evaluation mechanism can be used to define the expected cybersecurity behaviors for employees and evaluate their execution. Managers can use the performance evaluation process to clarify what behaviors are required, nice to have, and not acceptable. For example, it might be unacceptable for employees to hand out system passwords to vendors without specific approval from upper management. In this way, the performance evaluation mechanism will clarify for employees what the organization expects and how to make individual decisions about what to do.

Proposition 13: The performance evaluation process in an organization will significantly impact the cybersecurity culture.

3. ***Rewards and Punishments*** refers to the managerial-generated impacts of cybersecurity behaviors. Managers have the opportunity to set rewards and punishments for the organization. Rewards are thing that delight and excite employees, such as social events, proclamations and certificates acknowledging exemplary behaviors, etc. They are motivators encouraging cybersecurity behaviors. Punishments are things that managers might impose for inappropriate behaviors. Employees would be motivated to not do certain behaviors because of the punishment they might receive. Examples are things like remedial training programs, reprimands, letters put into the employee's personnel files, or at an extreme, firing of the offending employee. To be most effective, both rewards and punishments must somehow be in parity with the severity of the behavior. For example, firing someone who fails a

phishing test seems like an extreme punishment for the offense. However, if the opened email resulted in a successful ransomware attack, the severe punishment might be warranted.

Proposition 14: Rewards and punishments for cybersecurity behaviors influence the values, beliefs and attitudes towards cybersecurity, which in turn drive actual employee behaviors.

Managers can influence values, beliefs and attitudes by investing in mechanisms that bring in new knowledge as it is available, retain that knowledge in organizational databases, employees, experts and systems, and access that knowledge when it's needed. Three mechanisms do this: organizational learning, training and communications, encouraging the organization to learn and adapt, communicating campaigns to increase awareness, building just in time learning opportunities, creating collaborative opportunities between employees, etc.

4. ***Organizational Learning*** refers to the ways the organization builds and retains cybersecurity knowledge. Organizational learning activities encourage the individuals in the organization to learn and adapt. Some examples include things like mentors who work with individuals to help them build skills, processes that encourage information sharing, consultants that bring new knowledge to the team and subscriptions to information sharing services that provide curated and relevant information.

Proposition 15: Organizational learning mechanisms influence values, beliefs and attitudes about cybersecurity, and those values, beliefs and attitudes have an impact on investments in organizational learning.

5. ***Cybersecurity Training refers*** to specific investments in courses and exercises to develop cybersecurity skills and experiences. Managers build training programs designed to cover the basic policies and procedures that the organization wants employees to know. Training fosters information security awareness, educates users on the importance of information security, and trains insiders to take on information security roles. Many organizations make new hires complete a cybersecurity training module as part of the onboarding process. Some organizations make employees take an annual update course or online training program to 'refresh' their knowledge of cybersecurity practices. Still other organization have come up with additional training offerings such as just-in-time learning pop-up windows to teach a point in the moment. As managers invest in creative and memorable training programs, employees become more proficient in their ability to be cyber resilient.

Proposition 16: Cybersecurity training programs help shape values, beliefs and attitudes about cybersecurity, and those values, beliefs and attitudes have an impact on the type and quantity of cybersecurity training offered by an organization.

6. ***Communications Channel*** refers to coherent, well designed programs to communicate messages about cybersecurity to the organization and collect cybersecurity information from the organization. Communications is at the heart of the manager's role in the organization. Insuring that the right information is heard by the right person at the right time underlies all successful business decisions and cybersecurity is no different.

Some managers use marketing techniques, such as campaigns, flashy posters, catchy videos, all hands meetings, etc. to communicate important messages to employees. These techniques can promote awareness and retention of cybersecurity message. But listening is also part of the communication channel that helps the organization collect information from employees. Formal and informal channels can be created for reporting cyber incidents, sharing dynamic cyber information, and even identifying potential vulnerabilities give individuals a clear message that this information is important, which drives beliefs and attitudes about cybersecurity.

Proposition 17: Well-designed communications mechanisms impact the cybersecurity values, beliefs and attitudes, and those values, beliefs and attitudes have an impact on the communications plans designed by an organization.

External Influences

The attitudes, beliefs and values an individual or an organization has about cybersecurity do not occur in a vacuum. Factors external to the organization shape how people think about cybersecurity. As the press highlights devastating breaches and attacks around the world, managers, leaders and Board members become increasingly anxious about the safety of their organizations and their personal information. For example, when the Equifax Breach of 2017 occurred, many individuals were forced to face the fact that their personal financial information may have been compromised. Further, in some industries, the government or other regulating body dictates how companies must prepare and defend against cybersecurity issues. For example, the impending GDPR regulations in Europe require organizations to assign a data protection officer. Three external influencers have significant impact on the culture of an organization:

1. ***Societal Cybersecurity Culture*** refers to the societal norms, beliefs, attitudes and values in which an organization lives. For example, some countries have a strong societal value of protecting data, and we'd expect to see that reflected in the beliefs of the organizations operating in that country. Some organizations operate in a country with a more lasses-faire attitude, and we'd expect their cybersecurity culture to be influenced by this attitude.

Proposition 18: The culture of the society in which an organization resides will impact the organization's cybersecurity values, beliefs and attitudes.

2. ***External Rules and Regulations*** refers to the laws, guidelines, and imposed regulations from the government and other industry organizations under which an organization must operate. All organizations fall under multiple jurisdictions including local, regional/state and national governments. Many also are accredited or validated by industry organizations that impose rules and guidelines required to maintain the accreditation. Cybersecurity is increasingly on the agenda of regulators and public officials as they search for ways to keep their constituencies safe and protected. We would expect the values, beliefs and attitudes towards cybersecurity inside an organization to be influenced by the external rules and regulations they face.

Proposition 19: The external rules and regulations from agencies and industry regulators in

which an organization resides will impact the organization's cybersecurity values, beliefs and attitudes.

3. ***Peer Influence*** refers to the pressure felt by managers in an organization from actions their peer organizations have taken. Since cybersecurity is a relatively new threat for many organizations, the response managers consider to this threat is often influenced by what their peers in other organizations have done. Trade associations, conferences, and simple social situations are all opportunities for managers to chat with peers about cybersecurity issues and to learn what options others have adopted. Further, as cybersecurity becomes a strategic differentiator for companies (meaning that customers seek out vendors with strong cybersecurity operations and proven security processes), organization are pressured to 'up their cybersecurity game' in order to compete.

Proposition 20: Peer companies to an organization, and the managerial cybersecurity culture, cybersecurity activities, and cybersecurity investment will impact the organization's cybersecurity values, beliefs and attitudes.

Organizational Cybersecurity Culture Framework

Evaluating and cultivating the cybersecurity culture in the organization is a complex but critical task. Pulling together all the concepts we've discussed above, we develop our Organizational Cybersecurity Culture Framework (Figure 4). This Framework depicts the external influences and managerial mechanisms that impact the cybersecurity culture, the values, beliefs and attitudes, of leaders, teams and employees within an organization. The ultimate goal, of course is to encourage behaviors that increase the cyber resilience of the organization, and the cybersecurity culture is a major way those behaviors are influenced.

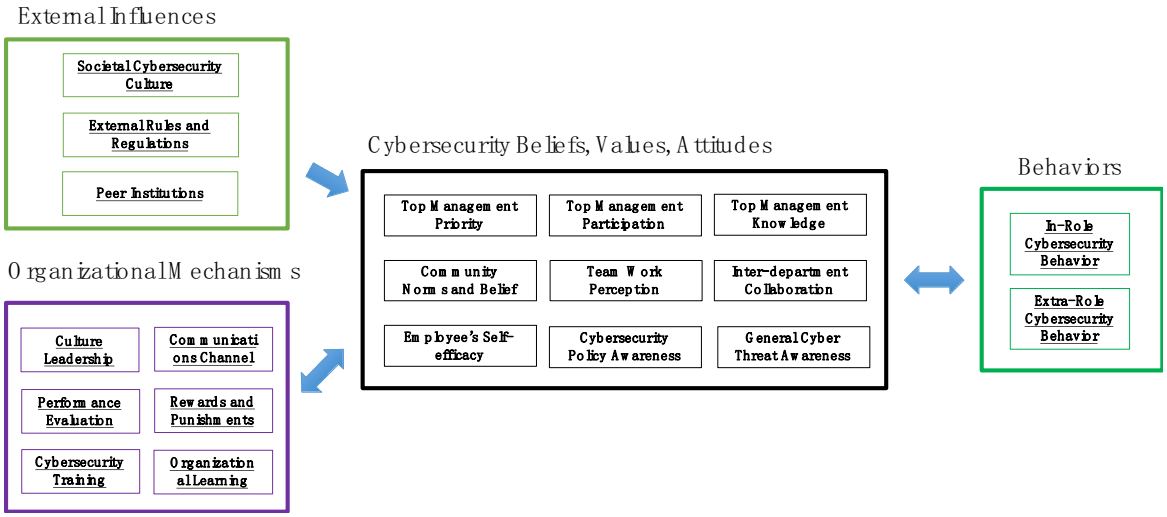

Figure 4: Organizational Cybersecurity Culture Framework

Our objective with this model is to assist managers and researchers in understanding how cybersecurity behaviors can be encouraged. The framework pulls together a number of mechanisms that managers can use to build a cybersecurity culture. Stated another way, the absence of these mechanisms is potentially an indicator of a sub-optimal cybersecurity environment which opens up the organization to unnecessary risk. We envision managers using this Framework to inform their cybersecurity planning activities and investments.

Our next step is to validate this model with empirical data by developing measures and metrics for the constructs. This will enable researchers and managers to dig deeper into details about an organization's cybersecurity culture to identify areas in need of future attention and areas of strength to potentially leverage further. After all, raising the cyber resilience of all organizations is good for the individuals, the managers, the teams, the leaders, and the society in which the organization lives.