A Culture of Cybersecurity Can Be Your Competitive Advantage

By:[*]
Dr. Keri Pearlson and Dr. Keman Huang
Cybersecurity at MIT Sloan (CAMS) Research Consortium
December 20, 2020

Introduction

Companies do not want to do business with suppliers who might cause a cyber breach. Those who are able to show they are more secure than their competitors just might have a competitive advantage. Cybersecurity would be a non-issue if it could be completely solved by allocating more budget for the latest and greatest technology. Unfortunately, more technology does not reduce the risk of a team member clicking on the wrong link or downloading the wrong file and many of the most publicized breaches start with someone doing something wrong. Organizational cybersecurity requires more than just the latest technology. It requires creating a cyber-resilient culture within your organization. This means all members of your organization must not just know how but actually take action to reduce risk. They need to have the values, attitudes and beliefs that drive secure behaviors. Our research has shown that a culture of cybersecurity doesn't have to be difficult to build, but it has a profound impact on reducing risk.

Building a strong cybersecurity culture is more than just telling team members what they should do. Instead, leaders have a special responsibility to align the beliefs, values, and attitudes of the entire organization with overall security goals. After all, people do what they believe is important and what they value. That's the role of organizational culture- to shape values, attitudes and beliefs. Our research contributes to this goal by studying many organizations who have successfully, and unsuccessfully, dealt with the human side of cybersecurity. Managers need practical solutions, and our research has uncovered ways to build and reinforce a culture of cybersecurity.

Focus on Values, Attitudes and Beliefs, not just Rules and Training

Organizations are vulnerable to cyber-attacks partially because people in the organization are unaware of or unprepared for cyber risks. Managers want individuals to do the right thing, to make the right choices and to connect the right dots when it comes to security. "Doing the right thing" might mean shutting the laptop a coworker left open, reporting phishing emails, or simply saying something if they see something. It's easy enough to require training, or send out phishing exercises, but these measures alone won't change hearts and minds and they won't build a culture of cybersecurity.

[*] This research was done in part with the support of MIT Sloan School's CAMS research consortium. All authors contributed equally to this project. For information contact Dr. Pearlson at kerip@mit.edu.

Organizational culture has been well-researched[1], and we adopted the concept of an organizational culture as the *values, attitudes and beliefs that drive behaviors* for this work. Extending this idea to cybersecurity, we define a culture of cybersecurity as the values, attitudes and beliefs that drive cybersecure behaviors. The right culture that aligns with organizational goals of cyber resilience is a more powerful approach than rules, technology, or policies. In one company we studied, when leaders, groups and individuals believe that it's their job to help keep the organization secure, they do things to achieve this goal. When they value security, they want to make sure their organization is secure. It's these attitudes that drive behaviors. Training makes explicit what behaviors are desired, but that's just not enough to shape the culture. Leaders build a culture by taking specific actions to shape their team's attitudes.

This is similar to cultures we see in industrial settings, where safety is paramount. In environments involving heavy machinery, construction, lasers, and other physically risky settings, leaders have a relatively easy argument to convince team members to propagate safety and reduce accidents. After all, when lives are on the line, driving attitudes about the importance of physical security drives secure behaviors such as wearing goggles and hard hats. Building a culture of cybersecurity can work the same way.

Building a Culture of Cybersecurity

To begin to answer the question "*how can leaders drive cybersecure behaviors?"* we studied[2] organizations from many different industries, in different countries, and of different sizes. We noticed that there were some common factors that influenced the values, attitudes and beliefs that drive cybersecure behaviors. We created a practical framework to illustrate our findings (see FIGURE 1).

SIDEBAR: Our framework was developed from extending organizational culture research to drive cybersecure behaviors. We conducted focus group sessions with companies who attended one of our CAMS research consortia conferences to identify constructs for the model. We initially validated our model with deep case studies from 3 companies. We then validated the construct relationships in our model with a survey of 187 individuals from 11 industries in 18 countries[3]. END SIDEBAR

To best understand the framework, we start with the desired behaviors. Leaders want to drive cybersecure behaviors. Some behaviors, like recognizing a phishing email, are just part of the job. Other desired behaviors, like participating in group discussions about keeping the company from the latest breach, are behaviors done because someone is part of the organization. We want to drive both kinds of behaviors: those that are an individual's responsibility and those that are necessary for the organization. Leaders can start the process of building a culture of cybersecurity by identifying behaviors they want to drive in the organization.

Values, attitudes and beliefs drive behaviors. People do what they believe is important and valued. While it's difficult to 'see' or 'measure' values, attitudes and beliefs, we can see evidence of them at three levels:

Leadership Level- at the leadership level, we see evidence of the values when we see what leaders prioritize, what they spend their time on, and what they spend their time learning about. In one company we studied, the CEO took time at every all-hands meeting to bring up cybersecurity, communicating his belief of its importance. In that organization, everyone knew that executives wanted them to help keep the company secure and they displayed those kinds of behaviors.

Group Level- we see evidence of the values, attitudes and beliefs of an organization by looking at how groups work together. When we see group norms that support cybersecurity, we see behaviors resulting from those norms. We see group members working together to find ways to be more secure. For example, in one organization, we saw non-technical business groups seeking out their cybersecurity counterparts to ask them about how to be more secure. We also saw groups teaching themselves ways to keep the organization as a whole secure. Conversations around the water-cooler (or it's virtual equivalent such as Slack and Zoom meetings) naturally included security-related topics. These kinds of group-level activities show that cybersecurity is important to the team, and that in turn drives more secure behaviors.

Individual Level- at the individual level, we see employees seeking out ways to know how to be more secure. We see them feeling empowered to do something when they see something suspicious, and that drives them to actually take action. In one organization, we saw individuals reporting phishing emails because they knew *how* to report them. Self-efficacy, knowing the cybersecurity policies of the organization, and having a general awareness of the kind of threats that might occur all support values, attitudes and beliefs that cybersecurity in important enough for everyone in the company to take part. And they do.

Driving Values, Attitudes and Beliefs

What can a manager or leader to do drive values, attitudes, and beliefs around cybersecurity? From our research we observed many influences, and we divided them into two buckets: External influences are things that a manager cannot easily impact, and managerial mechanisms are things that a manager can do.

External influences impact the culture of an organization, and managers must understand what those are in order to drive the right culture for their team. For example, the industry of the organization has a big impact on attitudes about cybersecurity and keeping data secure. Financial service firms and hospitals have a different attitude about cybersecurity than organizations in other industries in part because of the strict regulations they must follow for their industry. In addition, no one wants to do business with a bank the feel is not cybersecure.

It's built into the value-proposition of the entire industry. Another influence are peer organizations. When one peer institution ups their game to be more secure, it drives everyone to follow. In some industries, cybersecurity is table stakes and that drives attitudes within the organization. Societal attitudes about security and privacy also impact culture. When a society values privacy, for example, we expect the organizations in that society to reflect those values, attitudes and belief. For example, we studied three different financial services firms. One was a well-established bank in Italy, and another was a start up in Brazil. We saw different attitudes around the individual's role in keeping the organization secure.

Managerial mechanisms are the actions that manager can take to influence the values, attitudes and beliefs of their organizations. In our research we saw many examples. Training is one such mechanism. Just about every organization we studied shared information about training programs to educate team members about cybersecurity. Cybersecurity training is usually done annually for compliance reasons or possibly during orientation when new team members are learning about their new role. It rarely occurs at the teaching moment when the knowledge is more useful. We noted that training is necessary to help drive attitudes about keeping the company cybersecure, but by itself training is not sufficient. When asked what they learned in their training program, many interviewees could not recall specifics. In our experience, training provides a baseline and sets expectations, but does not sufficiently change values, attitudes and beliefs. Additional managerial actions are needed.

Successful cybersecurity cultures have a leader who owns the actions necessary to drive the values, attitudes and beliefs. One company we studied had a culture-owner who was a former marketing manager. She was responsible for driving a cybersecurity culture. She reported to the chief-information-security-officer (CISO) but her activities were companywide. Using her marketing experiences, she was able to create campaigns to change hearts and minds in ways that connected with individuals in the organization. She built upon the company culture to further drive values, attitudes and beliefs that drove cybersecure behaviors. For example, she noticed early on that the term 'cybersecurity' was not really connecting with team members; they all agreed it was important, but it was not something they related to. So she changed the messaging to be 'protect our data and systems,' and that changed the values, attitudes and beliefs. Individuals did not really know what to do when told to be more cybersecure, but they definitely knew what to do, or they asked others to learn how to protect data and systems. The messaging made a significant difference. Likewise, additional communications programs that were easily understandable, used fun icons, current movie titles, famous memes, etc. made the messaging accessible, engaging and actionable. For example, she used famous movie titles, slightly edited to reflect cybersecurity messages and those became topics of discussion among employees. When she interjected this kind of marketing technique into their cyber- training programs, team members not only sought out the class to see what she did that time, but they became fodder for team discussions.

Formal performance evaluation processes are another useful managerial mechanism to change values, attitudes, and beliefs. With formal evaluation of cybersecure behaviors, individuals understand what is expected of them. For example, in one company we studied, managers kept track of failed phishing exercises. Individuals who failed these exercises multiple times were aware that records were being kept. Rewards and consequences are also important mechanisms to drive culture. In the phishing exercise example, when someone failed the first time, they had to take a reminder course to help them identify phishing emails. The second time, they had to discuss their performance with their manager. The third time, they met with HR. The fourth time, they lost internet privileges and if it happened again, they were fired. Relatively few people clicked on phishing emails more than one time in this organization. In a different organization, we asked about the impact of failing the phishing exercise, and were told that they would never consider firing or removing internet privileges, but at the same time, they told us that they had a hard time convincing team members to not click on these exercises. In another organization, the cyber-evangelist offered a reward for individuals who noticed anything out of the ordinary. Individuals went out of their way to contact him with potential cyber risks they noticed. What reward did he offer? A cookie. It was both low cost and effective. Team members wanted the reward and the company benefited from increased cybersecure behaviors.

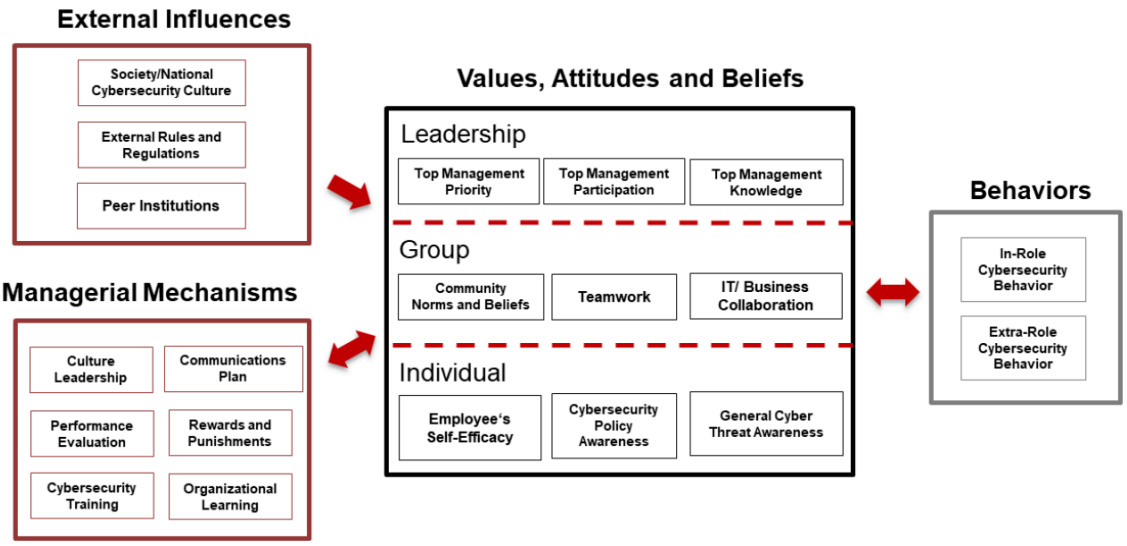
A Culture of Cybersecurity Could be your Competitive Advantage

Building and sustaining a culture of cybersecurity is no longer an option, it's a necessity. When your people are your front-line entrance to data, systems, and processes, they must be part of the security solution. Their cybersecure behaviors are critical to keeping the company secure, and potentially a competitive advantage that your customers value. Telling employees what to do is not enough; we have to change their values, attitudes and beliefs to truly drive the behaviors we seek. Our research highlighted a number of actions that every leader can take to create a culture of cybersecurity. To get started, here are a few first steps:

1. **Appoint a cybersecurity culture leader-** give this day-to-day responsibility to someone other than a very busy C-level executive, and make sure this person is a strong communicator, a well-respected team member, and a good representative of your current culture. After all, they will be building programs and actions to change hearts and minds of their colleagues and a strong foundation within the organization will help them.
2. **Make cybersecurity your priority and it will become the priority of those around you**- when someone knows it's important to you, they will seek out ways to show you it's important to them. Talk about cybersecurity often. Start your team meetings with a cybersecurity story- there are plenty in the news every day- and ask your team how your company can protect themselves from a similar incident.
3. **Find ways to reward the cybersecure behaviors you want to see**- Rewards don't have to be expensive, but they do have to be visible. Badges for emails, certificates, even a cookie were all very effective rewards we saw in our research. Team members value the things that bring them rewards, and they believe they should not do things that have

negative consequences. Your culture of cybersecurity needs both of these to be successful.

Most of all, start now. Cybersecurity incidents are not going away, and your customers are increasingly asking if your company is cybersecure enough to do business with. Until now, cybersecurity was not a key factor in choosing suppliers; it was either expected or just not important enough. But that has changed. The bad guys are getting better at a faster pace than ever, and technology cannot keep your team and your organization safe enough. You need everyone in the organization to help, and that means setting up the values, attitudes and beliefs that drive cybersecure behaviors. After all, a culture of cybersecurity could be your competitive advantage.



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

Figure 1: Framework for Building a Culture of Cybersecurity

[1] See for example Schein, E. H. (1990). Organizational culture. *American Psychologist, 45*(2), 109–119. https://doi.org/10.1037/0003-066X.45.2.109; Barley, S. (1983) Semiotics and the study of occupational and organizational cultures. *Administrative Science Quarterly*, 28, 393-413; and Chandler, A.P. (1977). *The visible hand.* Cambridge, MA: Harvard University Press.

[2] Huang and Pearlson, For What Technology Can't Fix: Building A Model of Organizational Cybersecurity Culture. *Proceedings of the 52nd Hawaii International Conference on System Sciences,* 2019, URI: https://hdl.handle.net/10125/60074 ISBN: 978-0-9981331-2-6

[3]Building a Model of Organizational Cybersecurity Culture: Identifying Factors Contributing to a Cyber-secure Workplace. https://cams.mit.edu/wp-content/uploads/Culture_Survey_Report_Findings_Dec2019.pdf