CYBERSECURITY CULTURE MATURITY MODEL

GOAL: To create a cybersecurity culture maturity model for evaluating, assessing, and increasing effectiveness of cybersecurity culture in managing human risk.

Mridula Prakash & Dr. Keri Pearlson

15th May 2024

1 Cybersecurity culture is not static. It evolves as it matures.

Assumptions for this research:

- Human risk from people in our organizations continue to introduce cyber vulnerabilities. Building a culture of cybersecurity is one way to manage this risk.
- As threats change, the cybersecurity culture must adapt.
- A more mature cybersecurity culture is more effective
- A roadmap can highlight different levels of maturity of a cybersecurity culture so managers can assess where their organization is and have a clear set of action items to increase maturity.

2 This research studies the levels of culture maturity

Our research focus is to create a cybersecurity culture maturity model:

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

3 Definition of cybersecurity culture

Cybersecurity culture is the values, attitudes and beliefs that drive cybersecure behaviors in an organization

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

4 Maturity means different values, attitudes and beliefs

Values, attitudes, and beliefs change as the organization evolves through the stages. Below is an example of how the corporate mindset changes:

Stage 1: "Technology team will keep us safe and secure. It's not my job to do it."

Stage 2: "The cybersecurity team will keep us safe and security. They tell me what to do."

Stage 3: "There are things I'm supposed to do, and the company leaders remind me."

Stage 4: "Cybersecurity is everyone's job, and I will do my part."

Stage 5: "Cybersecurity requires everyone to be aware, creative and involved. I'll proactively look for ways to help us be more resilient."

5 Culture maturity stages

Stage 1: Adhoc	Stage 2: Defined	Stage 3: Managed	Stage 4: Developed	Stage 5: Dynamic
Cybersecurity is a technical term, used to put protections in place. Employees are told what to do in training and awareness campaigns	Managers identify desirable behaviors, and put some mechanisms in place to create values, attitudes and beliefs	Culture leader who owns, creates, manages and evolves cybersecurity culture	Cybersecurity is a top priority of leaders, and creates environment where 'cybersecurity is part of everyone's job'	Cybersecurity culture adapts naturally to build in new mechanisms as environment and threats evolve

6 Call to action: Share your thoughts

We are interested in your thoughts on evolving the maturity of your cybersecurity culture. Please reach out to us in email if you are interested in participating in research and sharing your observations and opinions about cybersecurity culture maturity. Read our whitepaper on cybersecurity culture maturity by scanning the QR Code. For more details, please reach out to kerip@mit.edu