Implementing a Cybersecurity Culture

Culture is an important topic that has been studied by anthropologists and sociologists for years.

However, culture currently has the attention of senior management and many IT and auditing enterprises across the world, due to increasing online business (e.g., cloud-based services and e-commerce), market globalization and constantly evolving Internet technologies.

Enterprises are facing culture challenges every day. For example, consider a fictional enterprise that recently promoted its New York City (New York, USA) director of IT auditing to chief information security officer (CISO) for the Indian subcontinent. She needs to relocate from the enterprise's New York City office to the enterprise's Bangalore, India, office to implement and manage cybersecurity technology and processes, cybersecurity culture, IT privacy, IT risk management, digital forensic methods, and many other responsibilities associated with her role. Although she is an experienced, top-performing professional with expertise in information security standards, she has never lived outside of New York City, and she has never visited the Indian subcontinent.

Nevertheless, to address cybersecurity culture, the terms culture and organizational culture need to first be defined.

Defining Culture and Organizational Culture

Culture is a set of social system rules, which is patterned and may be conceived as a mechanism for providing a distinction of correct vs. incorrect behavior. It denotes a factor that shapes human behavior by transmitting content and patterns of ideas, values and other symbolic-meaningful schemes.[1] In this sense, culture represents a form

Luis Emilio Alvarez-Dionisi, Ph.D.
Is a professor of artificial intelligence (AI), machine learning and deep learning. He is an international management consultant with extensive experience working with chief executive officers, boards of directors and senior management in Fortune 500 companies. He has advised numerous organizations worldwide, including Intel, IBM, Merck, Chevron, Isuzu, Smiths Detection, the Beijing 2008 Olympic Games and the Government of Singapore Investment Corporation (GIC) on project, program and portfolio management. Alvarez-Dionisi's research work focuses on global project management trends, agile project management, AI, cybersecurity culture, chatbots for business, engineering robotics, big data applications, IT governance and medical information systems. He can be reached at dr.luis.alvarez@outlook.com.

Nelly Urrego-Baquero
Is an electronic engineer and IT researcher with broad management experience in operation and project management. She is a former director of a satellite communication system. Similarly, Urrego-Baquero was in charge of a mobile systems' division for tracking vehicles for the South American region. She was also in charge of setting up the infrastructure framework for a military mobile data center in South America. Her research focus is on the Internet of things (IoT), project management, cybersecurity, IT risk management and digital business. She can be reached at n.urregobaquero@audencia.com and nurrego@gmail.com.

or a set of reactions revealed, created or conceived during societies' history of handling problems. Such problems usually arise from the interactions of societies' members and their environment.[2]

On the other hand, organizational culture is defined as "the values and behaviors that contribute to the unique social and psychological environment of an organization."[3]

While organizational culture embraces the sociological and psychological atmosphere of an organization, knowledge sharing deals with interchanging facts and information with people, groups, systems and organizations as well. Correspondingly, organizational culture and knowledge sharing make the perfect binomial of a social ecosystem.

Therefore, this social ecosystem is composed of critical success factors (CSFs), which are:

> *The limited number of areas in which satisfactory results will ensure successful competitive performance for the individual, department or organization. CSFs are the few key areas where "things must go right" for the business to flourish and for the manager's goals to be attained.*[4]

The basic CSFs of organizational culture and knowledge sharing are:[5]

- **Trust**—Belief or interpersonal trust between coworkers
- **Information systems**—Systems required to convert data into information
- **Communication between staff**—Human interactions necessary for knowledge transfer
- **Organization structure**—Structures in the organization that are used to facilitate knowledge sharing
- **Reward systems**—Motivating and incentive mechanisms that are used to facilitate knowledge transfer

In addition to the basic CSFs, organizational culture can also include the following CSFs:

- **Change management**—Managing the resistance of organizational change
- **Motivational methods**—Ways to encourage people behaviors to reach a goal
- **Knowledge management**—Capturing, storing, processing and disseminating knowledge
- **Standard operating procedures**—Defining and documenting the level of accountability and responsibility of a role

Cybersecurity Culture

The main objective of cybersecurity is to protect "information assets by addressing threats to information processed, stored, and transported by internetworked information systems."[6]

"IN REALITY, THE MAIN OBJECTIVE OF CYBERSECURITY CULTURE IS TO DEVELOP AND IMPLEMENT A CYBERSECURITY CULTURE ECOSYSTEM TO SUPPORT CYBERSECURITY."

Cybersecurity culture is "the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behavior with information technologies."[7] In reality, the main objective of cybersecurity culture is to develop and implement a cybersecurity culture ecosystem to support cybersecurity. Sharing the experience of establishing an advanced social and psychological groundwork may help support cybersecurity.

The Internet has facilitated new ways of doing business for organizations, reaching many places never dreamed of in a matter of seconds. That is the magic of the Internet and cyberspace. However, such magical scenery vanishes every time organizations have to face cyberattacks. This is true because their assets (e.g., information and communications technology resources and strategic content) are at risk. As a result, a tangible

outcome of a successful cyberattack could be translated into a loss of the organization's reputation, a decrease in its stock value and even bankruptcy.

Consequently, cybersecurity becomes a significant factor of an organization's specific financial risk.[8] That is why cybersecurity is one of the most relevant technological and financial concerns of this century.

> "HAVING A CYBERSECURITY CULTURE IS A DYNAMIC PROCESS THAT DEMANDS CONTINUOUS ATTENTION."

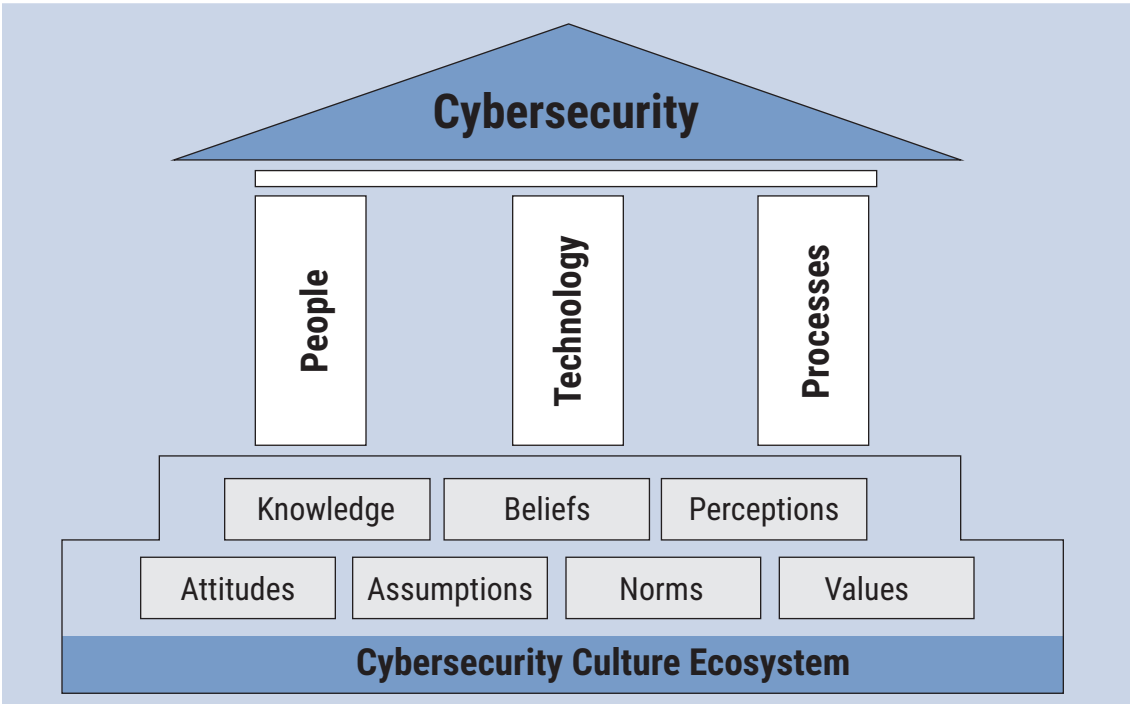
The need to address cybersecurity technology and processes requires having previously developed a cybersecurity culture. Having a cybersecurity culture is a dynamic process that demands continuous attention. Initially, organizations can use project management to implement a cybersecurity culture. Once the groundwork for a cybersecurity culture has been established, the organization can convert cybersecurity culture into an ongoing operation for the enterprise.

Figure 1 shows the seven blocks of a cybersecurity culture ecosystem supporting the people, technology and processes of cybersecurity.[9, 10]

The cybersecurity people, technology and processes domain includes the infrastructure that is required to run the cybersecurity solution. The seven blocks of knowledge, beliefs, perceptions, attitudes, assumptions, norms and values provide the appropriate social and psychological environment to support cybersecurity.

However, it appears that deep research work on defining and measuring cybersecurity culture is missing.[11] As a result, this gap is an opportunity for scholars and practitioners to embark on a study of cybersecurity culture.

Figure 1—Supporting Cybersecurity



A Strategic Decision About Cybersecurity Culture

Deploying cybersecurity culture requires the board of directors and senior management to decide to support and enable a cybersecurity shield to mitigate the risk associated with cyberattacks. As a result, enterprises should answer the following question: "Should we develop and implement a cybersecurity culture to reinforce cyberprotection of our organization?"

Perhaps such a question needs to be evaluated by senior executives who manage cybersecurity projects. These executives must also assess whether the development and implementation of a cybersecurity culture should be done before establishing cybersecurity technology and processes.

Scoping the Implementation of a Cybersecurity Solution

To implement a cybersecurity solution, it is necessary to clearly define the boundaries of the work that needs to be performed ahead of time. This is needed because the cybersecurity solution demands knowing the landscape of projects and programs and their interdependencies, investment mechanisms, recommended resources, time frames, key performance indicators (KPIs), quality yardsticks and benefit realization methods.

The earlier example of the newly appointed CISO for the Indian subcontinent is used to illustrate the scope of the implementation of a cybersecurity solution in **figure 2**. The programs and projects for which the CISO is responsible in the Indian subcontinent are managed as the Indian subcontinent cybersecurity portfolio. The portfolio is divided into seven programs, which correspond to the seven countries of the Indian subcontinent—Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan and Sri Lanka. The new CISO organized each program into two projects: a cybersecurity culture project in addition to technology and processes project.

Propelling Cybersecurity With a Cybersecurity Culture Ecosystem

Because people are considered the weakest link in the cybersecurity chain, they must be encouraged to increase their cybersecurity awareness and attend appropriate cybersecurity education[12] and training programs.

Figure 2—Cybersecurity Solution

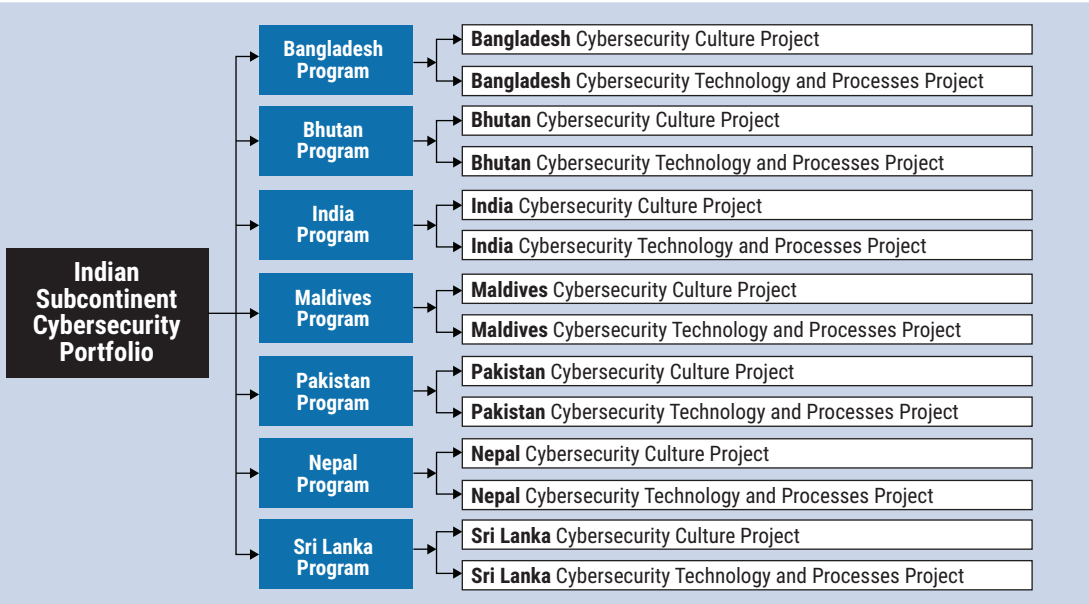


Figure 3 shows the awareness and education and training drivers as the force behind a cybersecurity culture ecosystem, which is required to propel the people, technology and processes of cybersecurity.[13, 14]

Importance of Cybersecurity Culture

Implementing a cybersecurity culture enables:

- **Empowering people**—Cybersecurity culture empowers people with the sociological and psychological skills that are required to work with cybersecurity technology and processes.
- **Projecting cybersecurity meaning**—Within the enterprise, the importance of the people, technology and processes of cybersecurity is understood. The consequences of ignoring cybersecurity's technological and financial risk are addressed.
- **Establishing stakeholder partnership and collaboration of key players**—A network of cybersecurity stakeholders is defined and managed. Stakeholders include employees, managers, government agencies, senior executives, boards of directors, technology providers, consulting providers, and education and training providers.
- **Providing an education and training road map**—An appropriate education and training program that encompasses the people, technology and processes of cybersecurity is integrated and delivered.

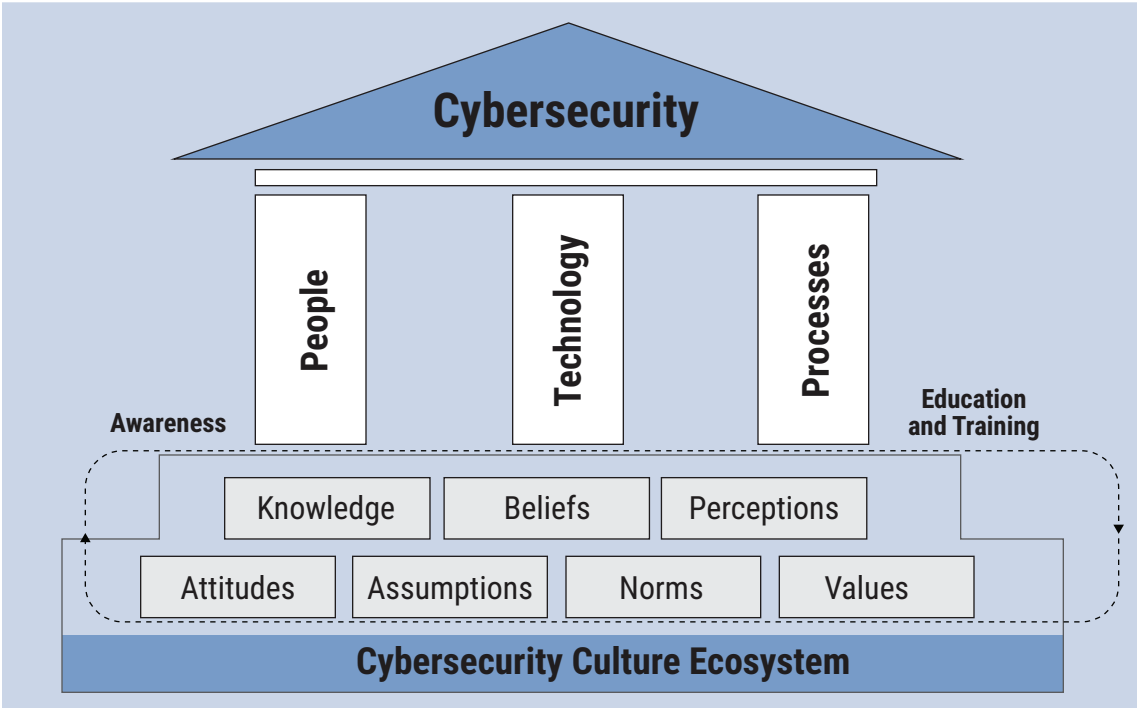
Conclusion and Recommendations

As a result, the cybersecurity culture ecosystem should be developed and implemented before cybersecurity technology and processes.

Additionally, a later phase of this study suggests addressing the following areas:

- The development of a cybersecurity culture body of knowledge (CCBOK)
- The possibility of creating a new cybersecurity culture certification
- The definition of a cybersecurity culture ecosystem methodology

Figure 3—Centrifugal Culture Ecosystems Drivers



Endnotes

1 Baecker, D.; "The Meaning of Culture," *Thesis Eleven*, vol. 51, 1997, p. 37-51
2 Business Dictionary, "Culture," *www.businessdictionary.com/definition/culture.html*
3 Business Dictionary, "Organizational Culture," *www.businessdictionary.com/definition/organizational-culture.html*
4 Bullen, C.; J. Rockart; "A Primer on Critical Success Factors," *Center for Information Systems Research,* USA, Massachusetts Institute of Technology, Sloan WP 1220 – 81, CISR no. 69, 1981
5 Al-Alawi, A. I.; N. Y. Al-Marzooqi; Y. F. Mohammed; "Organizational Culture and Knowledge Sharing: Critical Success Factors," *Journal of Knowledge Management*, vol. 11, no. 2, 2007, p. 22-42, *https://pdfs.semanticscholar.org/e9b9/4df7574d7b679dc18af5cc500811a8703c87.pdf*
6 ISACA®, Cybersecurity Fundamentals Glossary, USA, 2016
7 European Union Agency for Network and Information Security (ENISA), *Cyber Security Culture in Organizations*, Greece, 2017, *www.enisa.europa.eu/publications/cyber-security-culture-in-organisations*
8 Srinidhi, B.; J. Yan; G. K. Tayi; "Allocation of Resources to Cyber-Security: The Effect of Misalignment of Interest Between Managers and Investors," *Decision Support Systems*, vol. 75, 2015, p. 49–62
9 *Op cit* ENISA
10 Trim, P.R.J.; Lee, Yang-im; Ko, E; Kim, K.H.; "Cyber Trim, P.R.J; *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership,* British Embassy Seoul, Republic of Korea,2014, pg. 21-26, *https://westminsterresearch.westminster.ac.uk/item/q0731/cyber-security-culture-and-ways-to-improve-security-management*
11 Gcaza, N.; R. von Solms; "Cybersecurity Culture: An Ill-Defined Problem," Nelson Mandela Metropolitan University, 2017, p. 1-12
12 *Ibid*.
13 *Op cit* ENISA
14 *Op cit* Trim *et al*.