Acta Scientific COMPUTER SCIENCES

Volume 3 Issue 8 August 2021

Review Article

Establishing a Cybersecurity Culture Organization

William Triplett*

Capitol Technology University, USA

***Corresponding Author:** William Triplett, Capitol Technology University, USA.

Received: June 07, 2021

Published: July 19, 2021

Abstract

Currently, organizations are addressing persistent complicated cyber threats, which has dramatically increased since the onset of the COVID-19 pandemic. Cybersecurity should be included in the culture of an organization and be a priority of management. Establishing culture in a cybersecurity organization depends predominantly on individuals, technology, organizational behavior, and several facets of information security. The most vulnerable aspect of cybersecurity is the human that needs to be trained to be more cybersecurity aware. Diversity in the work place is also increasing a person's individual cultural background needs to be considered to communicate effectively cross-culturally. A combination of cybersecurity culture and employee ethnic culture consideration is needed to successfully maintain consistent effective practices of cybersecurity. Creating cybersecurity culture needs to be communicated along with the recognition that human aspects of cybersecurity is an on-going learning experience that expands cybersecurity awareness.

Keywords: Communication; Culture; Cross-cultural; Cybersecurity Leadership; Organization; Technology

Introduction

Cyber attacks have risen exponentially since the onset of the COVID-19 pandemic particularly during lockdown [1]. Cyber attacks were targeting the healthcare industry, a critical infrastructure needed to address the pandemic [2]. United Kingdom's National Cyber Security Centre (NCSC) [3] together with The United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) responded by publishing an advisory about how cyber-criminals were exploiting the pandemic on April 8, 2020. Many governments and industries rapidly implemented employees working at home to continue their businesses during lockdowns leaving cyber security gaps open (Lallie., *et al*. 2020). The World Health Organization (WHO), government bodies, airlines, and supermarkets were impersonated by cyber criminals through emails and texts seeking cash to help with the pandemic [4]. Cyber crime is no doubt here to stay and must be counteracted with all hast and efficiency (Lallie., *et al*. 2020).

Deutschman (2005) defined culture as "a set of values, beliefs, norms, customs, rules, and codes that lead people to define themselves as a distinct group with a sense of commonality." The standards and practices of a business are not distorted by the cultural diversity of its representatives. Rather, variations in reasoning and possible creative solutions are an advantage and should be recognized as such. The art of communication in a high-diversity context rests on the attentive monitoring of spoken and transcribed communication. In a cross-cultural setting, linguistic hurdles can sometimes be difficult to overcome. Managing cultural change and forming a strong cybersecurity culture are not simple tasks. They involve points in time, assets, instruments, and, above all, effective assistance from management. As cultural and cybersecurity hurdles increase, so does the need for effective leadership to help conquer the communication challenges presented to leaders. Shahzad and Shahbaz [5] suggested further research regarding the workplace innovative and flexible culture which are key factors influencing innovative performance and collaboration in organizational culture.

Both Pollini., *et al*. [6] and Vanderhaegen (2017, 2021) called for further research about the learning of socio-technical systems cybersecurity along with the human components.

Theory of organizational culture

The theory of organizational culture can access the factors contributing to an organization's effectiveness. Denison and Mishra [7] determined that a theory of organizational culture and effectiveness require that factors of the wider cultural context in which organizations exist be considered and incorporated. As stated by Denison and Mishra [7], the "general cultural context influences organizations and their effectiveness." This cultural context is composed of a wide range of factors such as history, occupations, societies, regulatory environments, and many more. However, four particular cultural traits were found to be positively linked to perceptions on performance, sales growth, and return on assets: involvement, consistency, adaptability, and mission. In addition, contrary to prior research, organizational culture was found to be measurable as well as being related to important organization outcomes [7].

Rather than considering individuals to be part of the problem, the latest cybersecurity methods used by organizations should see individuals as part of the solution, as humans are indispensable to the implementation of sociotechnical systems. Yet, the 2018-2019 Global Information Security Survey revealed that 34% of organizations find unaware workers to be the biggest vulnerability [8]. Ingham (2018) reported that 88% of the data breaches in the United Kingdom were not caused by cyber attacks but by human errors such as sending sensitive data to the wrong person, forgetting to redact data, storing data in an insecure location many times on a public cloud server, or loss or theft of paperwork. Cybersecurity has become a high priority for organizations [9]. A supportive organizational culture can lead to a collaborative and innovative work environment [10]. In contrast a high correlation was found between destructive organizational leadership and counterproductive work behavior [11]. Pollini., *et al*. (2021) showed that when a person-centered cyber-security method was combined with traditional technological solutions were adopted, countermeasures of a non-technical type lead to a holistic ways of managing cybersecurity, such as user awareness. Currently, organizational culture has to determine the structure by which an organization forms its strategies. "The structure of [an] organization determines the placement of the power and authority in the organization" (Galbraith 2002). Management, unaware of organizational challenges, may not realize a solution since the organizational culture needs to be established in order to provide security. Organizational culture governs the management of the corporation's composition and its positions of influence. This includes defining organizational responsibility. The manager's obligation is to inspire employees to construct an environment that strengthens workers in all aspects of employment including cyber-security.

According to Martins and Terblanche [12], "in an attempt to increase the level of creativity and innovation, it has been found that one of the best approaches to describe organizational culture is based on the open systems approach." This suggests cybersecurity and culture will only occur in appropriate environments within organizations. In means-ends analysis planning, cybersecurity awareness is primarily restricted to problem-solving. Without strategic planning, there is less creativity. Culture is a crucial factor in organizational competence, as is having the moment to build and propel strategies to modernize. Realizing what the culture currently wants and need can help with promoting group behaviors and enhancing performance. A leader's most valuable task is the production and maintenance of organizational individuality and diversity to counteract effort. Organizations have long remained major strategic drivers for cybersecurity leaders. Before debating the basic factors of understanding cybersecurity culture, leaders must appreciate the correlation between cybersecurity and organizational culture, a subject that has been extensively researched.

A phased approach is required to meet an organization's strategic goals and plans. This approach should address the various technological tools that pose a security risk to the organization culture. Cybersecurity is a government-wide obligation, and the employment of additional workers is essential to the performance of corporate plans, company functions, and organizational security [13]. Representatives of organizations recognize that philosophy remains at the core of any organization. At the same time, individual life-paths have evolved through developments in technology and human behaviors. When an organization promotes a work culture in which the majority believe that managers can bring about change, the entire team thinks in terms of success. According to

Tanner [14], "a creative workplace is consistent with an emphasis on improving service to customers, employees, society, and stockholders". Such a workplace encourages the timely dissemination of cultural norms and best practices.

Furthermore, as origination progresses modernization emerges as the single most critical distinctive business component, closely linked to originality and culture. Organizational workforces are growing increasingly diverse. In the most valuable and effective U.S. organizations, leaders recognize that their distinctive organizational cultures make them exclusive and identifiable. This inspires improvement and an array of resolutions and revitalizes innovations that can be hindered in less effective culturally rich contexts. In an inadequately structured organization, meeting goals is often difficult, owing to the lack of structure in place to assign roles and tasks to workers effectively.

Hogan [15] stated, "leadership is not an inherited thing but comes from the personality attributes which are the essential elements of effective leadership." In ethnically diverse organizations, cultural thoughtfulness is an essential personality characteristic. Information technology advisers are adaptable, receptive to change over time, and open to feedback. In most organizations, culture arises from the coexistence of culturally distinctive views, thoughts, principles, and viewpoints on best practices. Kraft [16] suggested that culture involves two primary stages: the outer stage and the worldview stage. The core of a culture originates from the worldview of the character who establishes the beliefs, ideas, and reliability that underpin the functioning mode. Many people are assured that their way of life is the correct way to live. As a result, their worldviews and perspectives merge in the background of the decision-making processes. Therefore, a facet of cross-cultural leadership communication is that two individuals do not promote the same worldview or formulate an equivalent approach. Communication, cultural advancement, and intricate systems management play key roles in any organization. For this reason, cybersecurity should not be the sole responsibility of IT professionals; it must involve everyone. Workers need to be able to recognize when they might be compromising cybersecurity by using personal devices, sharing their password for instance, downloading software without considering possible cybersecurity issues [17]. Regardless of their role, every individual wants to know how to function with self-confidence in a digital environment and this desire can be utilized to improve cybersecurity through training. Communication that involves culture is the key to good communication with a cultural diverse workforce.

The significance of cultural diversity in organizations is more important than ever. In this modern technological era, culture is considered a substantial component of an organization's success. When focusing on organizational culture and its relationship to cybersecurity, managers cannot overlook the impact of domestic cultures on national standards and attitudes, and, ultimately, individual attitudes toward security. As Tanner [18] wrote, "creativity is critically important for organizations seeking to survive and thrive in today's highly turbulent business environments." Cultivating inventiveness is a vital skill for modern managers. Leaders can develop insight into an environment of resourcefulness by promoting a culture of transformation, permitting individuals to review assumptions and express corporate values when they encounter or foresee difficulties. In this way, innovation can become spontaneous and instinctive.

Resourcefulness and modernization are key to maintaining a company's organizational culture. To begin with, culture must be studied as a fundamental role of the organization, not just a subtopic. Technologies and systems are intimately linked in today's organizations. Supervisors regularly fail to remember that organizations consist of individuals who should be prepared to identify cybersecurity threats and respond to them adequately. Those individuals, however, must be placed in appropriate roles in order to function competently. Effective cybersecurity requires a responsive and satisfying workplace. Therefore, motivating individuals involves leaders paying attention to human behavior.

Each organization has its own cybersecurity culture that cannot be duplicated elsewhere. Cybersecurity culture is based on the particular attributes, tools, practices, and community values of a given organization. Connerley and Pedersen [19] wrote that "cross-cultural communication expertise and interpersonal conciliation proficiency are pre-requisites of efficient labor-force personnel management". Leadership has acquired new value among today's distinctive labor force. The organization's originator must introduce cybersecurity culture, even though the culture may shift over time as it is updated and reviewed. However, one fundamental model of success that remains constant is respect for different cul-

tures in meaningful communication that inspire the individual to be more cyber security aware. Helping organizations understand cybersecurity entails adjusting the mindsets of the various stakeholders toward cybersecurity. This is the true test for managers unaccustomed to dealing with such issues, as security is repeatedly deemed an important asset of organizational leaders. Arasaratnam and Doerfel [20] explained that, "communication of respect has been established as a significant dimension of cross-cultural competence." Culture has a strong influence on leadership and the organization environment. As an organization becomes more diverse and expands beyond the boundaries of its home country, management must provide appropriate training in order for the corporation to remain relevant in the constantly shifting business environment. According to Matveev and Nelson [21], "cross-cultural communication competence is a vital component of a manager's ability to address common challenges faced by a multicultural team." In culturally diverse groups, global leaders must have the social knowledge and skills to interact positively with people of different cultural backgrounds.

Proposed approach

The proposed approach is qualitative and the aim is to combine the awareness of organizational cybersecurity culture into the overall culture of the organization so the human factor is included. In addition, the personal culture of the workers requires managers to be sensitive to their differences in order to communicate well and respond directly to the individual so the message is understood. To establish a cybersecurity culture, training is needed so all workers become more efficient at recognizing violations that put the organization at risk of cybersecurity vulnerabilities, thus addressing the human factor. That training should be geared to fit the individual by developing demographic profiles of workers' information security policy awareness and their intention to comply with cybersecurity strategies. The human factor is critical for the cyber defense of organizations, which determine either the success or failure of cybersecurity [22,23].

Organizations should foster cultures that link cybersecurity and other culture components with an emphasis on performing critical roles. Executives and managers are responsible for establishing the organizational culture in which cybersecurity operates. The advancement of cybersecurity culture must not be independent from the operating environment. Improving workers' performance by inspiring them is critical to the successful management and promotion of a collaborative workspace that includes cybersecurity.

In the work environment, social proficiency defines the human capacity to efficiently accomplish a task or assignment. Culturally well-informed employees can establish a personal relationship with a global business through ongoing communication, which is often with a different culture other than their own personal culture in today's global businesses requiring cross-cultural communication. In cross-cultural communication, collecting information from a partner, or from management, requires in-depth communication. Success or dissatisfaction in the management of a diverse labor force is dependent on leadership. An organization with a consistent technical structure has a greater chance of success. A security culture must encompass both an organization's philosophy and the behavior of the workers; it should not be exterior to the organization and it should not be delegated.

The proposed approach will benefit from reflexive thematic analysis following the six steps of Braun and Clarke [24]. The six steps the researcher will take are to: become familiar with the data, coding, generating initial themes, reviewing themes, defining and naming themes, and last, writing up the report of the themes supported with prior literature. Reflexive thematic analysis allows the commonalities of meaningful themes and patterns to be identified, sorted, and emphasized. The articulations and the expressions of participants will be collected through interviews of those familiar with the topic while the researcher listens carefully and continually practices reflexivity to counteract possible biases.

Implications

This proposed study could help identify human factors within the organization that can be used to develop methods for enhancing workers cybersecurity awareness programs. Furthermore, an effective cybersecurity program increases knowledge and awareness in addition to changing employees' behavior and attitude to ensure compliance [25]. Both private and public organizational stakeholders can use this information to develop more effective cybersecurity policies by addressing the human factor along with traditional technical solutions. Since workers would most likely be more satisfied with their jobs, their performance might also increase and in turn increase the overall performance of the organization.

Conclusion

Cyber attacks have risen exponentially since the onset of the COVID-19 pandemic particularly during lockdown (ENISA 2020). Deutschman (2005) defined culture as "a set of values, beliefs, norms, customs, rules, and codes that lead people to define themselves as a distinct group with a sense of commonality." The standards and practices of a business are not distorted by the cultural diversity of its representatives. The theory of organizational culture can access the factors contributing to an organization's effectiveness. Denison and Mishra determined that a theory of organizational culture and effectiveness require that factors of the wider cultural context in which organizations exist be considered and incorporated. Currently, organizational culture has to determine the structure by which an organization forms its strategies. Culture is a crucial factor in organizational competence, as is having the moment to build and propel strategies to modernize. A leader's most valuable task is the production and maintenance of organizational individuality and diversity to counteract effort. Cybersecurity is a government-wide obligation, and the employment of additional workers is essential to the performance of corporate plans, company functions, and organizational security. Cybersecurity culture is based on the particular attributes, tools, practices, and community values of a given organization. Improving workers' performance by inspiring them is critical to the successful management and promotion of a collaborative workspace that includes cybersecurity. A security culture must encompass both an organization's philosophy and the behavior of the workers; it should not be exterior to the organization and it should not be delegated.

Acknowledgements

I would like to express my deep appreciation to Dr. Ian, my research colleague, for his patient guidance, inspiration, and helpful assessments of this cybersecurity work. I would also like to thank Dr. Nobles and Dr. Burrell, for their advice and support in keeping me on schedule. My grateful thanks are also extended to Mr. Rocha for his help in doing the data analysis. His willingness to give his time so generously has been very much appreciated. I would also like to thank Dr. Dark from Cyber.Org for enabling me to visit her office to observe the daily operation. Finally, I wish to thank my parents for their support and encouragement.

Funding Support

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Bibliography

1. ENISA. ENISA threat landscape 2020: Cyber attacks becoming more sophisticated, targeted, widespread and undetected. European Union Agency for Network and Information Security (2020).
2. Wired. "Hackers are targeting hospitals crippled by coronavirus" (2020).
3. UK's National Cyber Security Centre (NCSC) and the US' Department of Homeland Security (DHS) Cyber-security and Infrastructure Security Agency (CISA). "Advisory: COVID-19 exploited by malicious cyber actors" (2020).
4. MalwareBytes. "Cybercriminals impersonate World Health Organization to distribute fake coronavirus e-book" (2020).
5. Shahzad F., *et al*. "Organizational culture and innovation performance in Pakistan's software industry". *Technology in Society* 51 (2017): 66-73.
6. Pollini A., *et al*. "Leveraging human factors in cybersecurity: An integrated methodological approach". *Cognition, Technology and Work* (2021).
7. Denison D R and Mishra A K. "Toward a theory of organizational culture and effectiveness". *Organization Science* 6.2 (1995): 204-223.
8. Ernst Y. "Global Information Security Survey" (2018, 2019).
9. Vaidya R. "Cyber security breaches survey 2019". Department for Digital, Culture, Media and Sport (2019): 66.
10. Kahn KB. "Understanding innovation". *Business Horizons* 61.3 (2018): 453-460.
11. Schyns B and Schilling J. "How bad are the effects of bad leaders? A meta-analysis of destructive leadership and its outcomes". *The Leadership Quarterly* 24.1 (2013): 138-158.
12. Martins E C and Terblanche F. "Building organizational culture that stimulates creativity and innovation". *European Journal of Innovation Management* 6.1 (2003): 64-74.
13. Magid L. "Why cyber security matters to everyone". *Forbes* (2014).
14. Tanner D. "Applying creative thinking techniques to everyday problems". *Journal of Consumer Marketing* 9 (1992): 23-28.
15. Hogan R., *et al*. "What we know about leadership: Effectiveness and personality". *American Psychologist* 49.6 (1994): 493-504.

16 Kraft C H. "Anthropology for Christian Witness". Orbis Books (1997).

17 Chua HN., *et al*. "Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations". *Telematics and Informatics* 35.6 (2018): 1770-1780.

18 Tanner D. "Creativity management-roadmap to building a more innovative organization". *Strategic Direction-Bradford* 19.4 (2003): 2-3.

19 Connerley M and Pedersen P. "Leadership in a diverse and multicultural environment: Developing awareness, knowledge, and skills". *Sage* (2005).

20 Arasaratnam L and Doerfel M. "Cross-cultural communication competence: identifying key components from multicultural perspectives". *International Journal of Intercultural Relations* 29 (2005): 137-163.

21 Matveev A V and Nelson P E. "Cross Cultural Communication Competence and Multicultural Team Performance". *International Journal of Cross Cultural Management* 4.2 (2004): 253-270.

22 Glaspie H W and Karwowski W. "Human factors in information security culture: A literature review". *Advances in Intelligent Systems and Computing* (2018).

23 Zimmermann V and Renaud K. "Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset". *International Journal of Human-Computer Studies* 131 (2019): 169-187.

24 Braun V and Clarke V. "Using thematic analysis in psychology". *Qualitative Research in Psychology* 3 (2006): 77-101.

25 Khando K., *et al*. "nEnhancing employees information security awareness in private and public organizations: A systematic literature review". *Computers and Security* (2021).

Volume 3 Issue 8 August 2021