EasyChair Preprint

№ 10810

Conceptualizing and Learning to Foster Cybersecurity Culture: a Literature Review

Meseret Assefa Adamu

August 31, 2023

CONCEPTUALIZING AND LEARNING TO FOSTER CYBERSECURITY CULTURE: A LITERATURE REVIEW

Research full-length paper

Meseret Assefa Adamu, University of Agder (UiA), Kristiansand, Norway,
meseret.a.adamu@uia.no

Abstract

This study aims to conceptualize cybersecurity culture and discuss lessons that organizations can learn from the research findings to foster an appropriate cybersecurity culture. The PRISMA method and scoping literature review were used in the study. An intensive literature search was conducted in well-known publishers and online databases. Literature was selected that dealt exclusively with cybersecurity culture. Cybersecurity culture was conceptualized based on Schein's organizational culture model and Van Niekerk & Von Solm's information security culture model. The results show that cybersecurity culture could be defined and conceptualized based on four important elements, namely cybersecurity competencies, behaviors, policy compliance, and practices of employees at all levels of an organization toward the cybersecurity goal of protecting digital assets from intentional cyberattacks or unintentional employee mistakes. In addition to the lessons learned from the literature, organizations could also consider the four important elements proposed in this study to foster their cybersecurity culture and improve their security posture. The main contribution of this study is to provide researchers with an understanding of the current concepts and scope of cybersecurity culture and to simplify the approaches for organizations to foster an appropriate cybersecurity culture.

Keywords*: Cybersecurity culture, cybersecurity culture concept, cybersecurity culture scope, fostering cybersecurity culture*

1. Introduction

In recent years, it has become apparent that maintaining and ensuring an organization's cybersecurity (cs) through technical approaches alone is less effective (Kortjan & Solms, 2012; Alshaikh, 2020; Malmedal & Røislien, 2014). Cybersecurity can only be effective if the human component gets equal attention and employees know, understand, accept and foster the necessary organizational and cybersecurity culture (csc) (Zimmermann & Renaud, 2019). Cybersecurity culture provides an attractive complement to the existing technical defense approach (Reegård, Blackett, & Katta, 2019; NIST, 2018; ENISA, 2017), increases attention toward protecting information assets in an organization (Corradini, 2020; Reegård, Blackett, & Katta, 2019) and combating increasing cyberattacks (Uchendu, Nurse, Bada, & Furnell, 2021). Therefore, it is strongly recommended that contextualizing and fostering an appropriate cybersecurity culture become mandatory in every organization (ENISA, 2017).

Organizational culture plays a substantial role in contextualizing and fostering appropriate cybersecurity culture (Uchendu, Nurse, Bada, & Furnell, 2021). As Schein (1999) explains, organizational culture is a combination of belief systems, values, and behavioral elements. Cybersecurity culture is a subculture of organizational culture (Corradini, 2020; Reegård, Blackett, & Katta, 2019). One of the most known models researchers used to contextualize cybersecurity culture at an organizational level is Schein's (1999) organizational culture model, which comprises three levels, artifacts (the visible and measurable day-to-day behavior in the organization), espoused values (the written documents, such as a vision or policy statements, that espouse the organization's formal values), and shared assumptions and beliefs (the underlying beliefs and values of the employees) (Schein, 1999). Van Niekerk & Von Solms (2006), adopted an Information Security Culture model based on Schein's levels of organizational culture by adding one additional level, Security Knowledge, to be seen as the fourth level of Schein's organizational culture model (Tsoeu & Da Veiga, 2022; Ubowska & Królikowski, 2022; Reid & Niekerk, 2014). Hence in this study, the context of cybersecurity culture is derived based on the above models i.e. (Schein, 1999) corporate culture model and (Van Niekerk & Von Solms, 2006) Information security culture model.

Further, researchers have suggested that significant security gains can be achieved by fostering an appropriate cybersecurity culture among an organization's employees (Alshaikh, 2020). An appropriate cybersecurity culture is one where organizational information assets and the system can be protected throughout its life cycle in cyberspace (Da Veiga, 2018; Astakhova, 2014; Tsoeu & Da Veiga, 2022). Even though fostering a desirable cybersecurity culture is not easy and may take many years (Corradini, 2020), it is to minimize risks in cyberspace and achieve organizational cybersecurity goals (Da Veiga, 2016) and helps to encourage employees to follow security policies, which lowers the potential risk of harmful information interaction by employees as they properly develop their knowledge and skills and behave safely in their work environment and helps organizations to mitigate the number of security breaches caused by human error (Tolah, Furnell, & Papadaki, 2021; Dojkovski, Lichtenstein, & Warren, 2010).

As a result, organizations should clearly understand the context of cybersecurity culture and use understandable concepts and dimensions/scope to foster a culture of security that uses a variety of approaches to improve the competency, practice, and behavior of employees to protect them from cyber risk (National Cyber Security Center, 2017; AlHogail, 2015). The effective fostering of a cybersecurity culture can lead an employee to act as a first-line of solution (Jennings, 2013; Gundu & Maronga, 2019) that can better safeguard organizational digital assets (Zakaria, Gani, Nor, & Anuar, 2007; AlHogail, 2015; Corradini & Nardelli, 2018).

This paper reviewed the literature to conceptualize cybersecurity culture in an organizational context based on Schain's (1999) model of organizational culture and Van Niekerk & Von Solm's (2006) Information Security Culture model and discusses the lessons that organizations can learn to foster an appropriate cybersecurity culture through a literature review.

2. Prior literature reviews

Prior literature review studies on the definition and concepts of cybersecurity culture (Reid & Niekerk, 2014), cybersecurity culture factors (Reegård, Blackett, & Katta, 2019; Gcaza & Solms, 2017; Mwim & Mtsweni, 2022), practices, frameworks, and metrics (Uchendu, Nurse, Bada, & Furnell, 2021) has been conducted. Gzaca and Solms (2017) also conducted a literature review of cybersecurity culture and indicated that there is a lack of widely accepted key concepts that delimit the culture, due to the fact that the cybersecurity concept is subjected to different researchers' perspectives and contexts of applications (Gcaza & Solms, 2017). Similarly, Reegård, Blackett, & Katta (2019) conducted a narrative review of the literature and concluded with how organizations realized cybersecurity culture and highlighted key practices. Uchendu, Nurse, Bada, & Furnell (2021) also conducted a more comprehensive systematic review of the literature and assessed issues like the definition of cybersecurity culture, essential factors, frameworks, and metrics.

Among the previous works of literature review, Reegård, Blackett & Katta (2019) and Uchendu, Nurse, Bada & Furnell (2021) specifically focused on reviewing the concept, definition, and factors of cybersecurity culture in general. Based on their research, they present definitions suggested by researchers, key practices for developing a cybersecurity culture, and factors such as management support, policy, awareness and training, involvement and communication, and learning from experience.

This study argues that prior literature reviews on cybersecurity culture tend to be descriptive summaries of the research conducted in specific years. They lack to explicitly focus on conceptualizing cybersecurity culture based on organizational constructs or context reflecting an organization's artifacts, shared tacit assumptions, and espoused values related to cybersecurity competencies to conceptualize cybersecurity culture at the organizational level. Moreover, they lack exclusive discussion of lessons organizations can learn from the literature to foster an appropriate cybersecurity culture. For this reason, in most organizations, the same attention is not given to fostering cybersecurity culture as the technical aspects, even though it is equally important for defending against ever-increasing cyberattacks.

Therefore, this study aims to conceptualize cybersecurity culture in an organizational context based on Schain's (1999) model of organizational culture and Van Niekerk & Von Solm's (2006) Information Security Culture model, map the concept to propose a simplified and holistic definition and discuss lessons that organizations can learn to foster an appropriate cybersecurity culture in an organization.

The study answers the following three questions:

- How cybersecurity culture is being conceptualized in an organization?
- What is the scope or dimension used to conceptualize cybersecurity culture in an organization?
- What lesson can organizations learn from research outputs to foster an appropriate cybersecurity culture?

3. Methodology

3.1. Scoping Literature Review

A scoping review is commonly undertaken to examine the extent, range, and nature of research activity in a topic area; determine the value and potential scope and cost of undertaking a full systematic review; summarize and disseminate research findings; and identify research gaps in the existing literature (Arksey & O'Malley, 2005; Levac, Colquhoun, & O'Brien, 2010). The main objectives of scoping reviews are to identify gaps in the current research and highlight areas that require further inquiry (Daudt, Mossel, & Scott, 2013). They aim to assess the potential size and scope of available research literature and the current level of synthesis available (Daudt, Mossel, & Scott, 2013). Scoping reviews can identify the conceptual boundaries of a field, the size of the pool of research, the types of available evidence, and any research gaps (Xiao & Watson, 2019).

This study applies the scoping literature review approach to understand the concept and scope of cybersecurity culture and to discuss the lesson that organizations should learn from literature to foster an appropriate cybersecurity culture.

3.2. Literature source and type

The main sources of literature were IEEE Xplore, Elsevier (Science Direct / Scopus), Springer, Web of Science (Clarivate), ProQuest, and AIS eLibrary. In addition, a general internet search for relevant published literature was conducted using the Google search engine and Google Scholar. The search included peer-reviewed academic publications and some other publications such as published conference papers, book sections or reviews, and published papers on cybersecurity culture were included.

3.3. Searching procedure and Keywords

Literature searches and selections were made using keywords from well-known online journal databases. Search strategies were used to gather information from a variety of databases from leading publishers, online libraries, and various accessible sources. The search was conducted using specific keywords that include "cybersecurity culture" or "cyber security culture" or “cyber-security culture” or “culture of cybersecurity” or “culture of cyber security” to retrieve all the research works from selected online databases. In some cases, references to selected literature were assessed to include additional relevant literature.

3.4. Selection Criteria

Because this study is concerned with conceptualizing cybersecurity culture based on organizational constructs, the focus of this literature review was solely on cybersecurity culture in an organizational context. To this end, once the search was completed, criteria for relevant literature selection were established, i.e., all duplicates were removed and the presence of the above search keywords in either the title, abstract, and/or keywords of the literature was checked. Subsequently, the abstracts and content of the selected literature were reviewed to ensure that the focus was exclusively on cybersecurity culture and answered the research question of this study. Cohort literature such as "information security culture" was not included during the selection. This is because both cybersecurity culture and information security culture have to do with creating a security-oriented environment in an organization, but there are some differences between them (von Solms & van Niekerk, 2013). According to von Solms & van Niekerk (2013), cybersecurity culture focuses specifically on digital and online interactions, while information security culture focuses on protecting all types of information, including physical and electronic data. The year of publication was not considered as a criterion, the study disregards the time limit to review broad evidence and resources in cybersecurity culture.

3.5. Selection Process

The PRISMA method was used in this study. The PRISMA flowchart visually summarises the screening process (Mengist, Soromessa, & Legese, 2020). It first records the number of articles found and then makes the selection process transparent by reporting the decisions made at the different stages of the literature review. The number of articles is recorded in the different phases. As shown in Figure 1, the initial search yielded a total of 114 works of literature, of which 51 were duplicates and 63 were screened in the first round. From the screened 63 pieces of literature, 22 literature were excluded by assessing the title. Further, abstract, keyword, and content assessments were done, and 22 papers were excluded. Literature that focused exclusively on cybersecurity cultures rather than cohort literature was included. As a result, a total of 19 relevant works of literature were selected for this study. Figure 1 illustrates a PRISMA flow diagram outlining the process used to achieve the final selected papers.

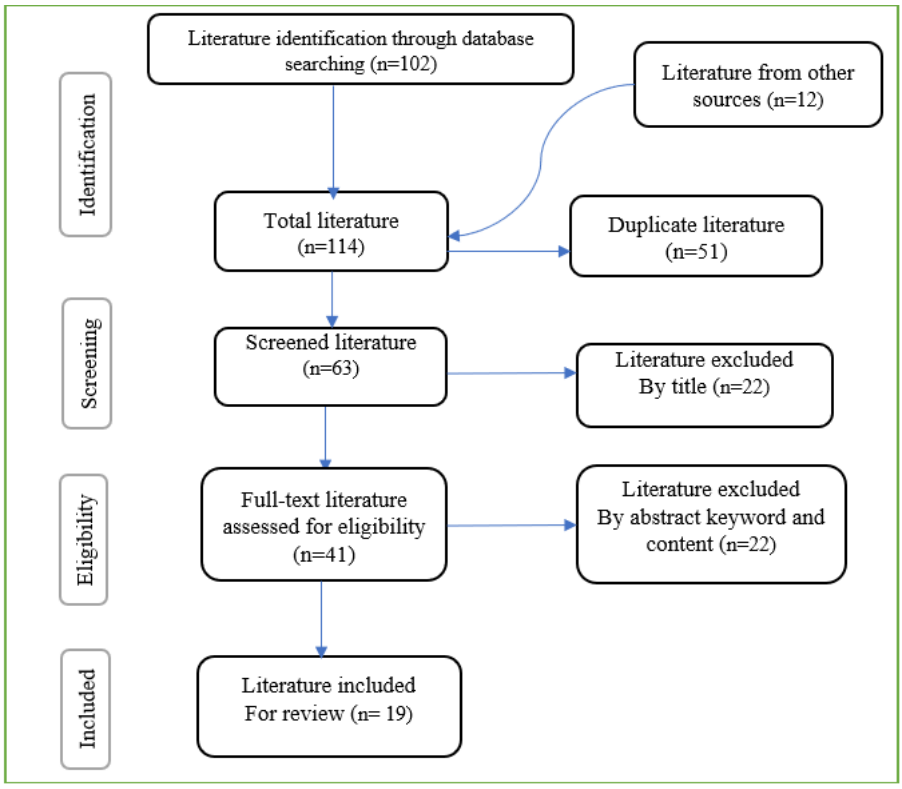

Figure 1: PRISMA flow diagram outlining the process of selecting relevant literature

4. Result

The purpose of this study was to conceptualize cybersecurity culture at the organization level and discuss lessons that organizations can learn from the literature. Most of the papers selected for this study focus exclusively on cybersecurity culture. The study identified the dimensions of the literature used to conceptualize cybersecurity culture in an organization. Table 1 summarizes the results of the focus areas of the selected papers in relation to the author(s) of the literature.

Focus area	Author/s
Day-to-day cybersecurity practice, actions, activities	(Corradini, 2020; Gcaza & Solms, 2017; Ubowska & Królikowski, 2022; Corradini & Nardelli, 2018; Gundu & Maronga, 2019; Hassandoust & Johnston, 2023)
Cybersecurity Policy, compliance, standards, strategies, and guidelines	(Alshaikh, 2020; Gioulekas, et al., 2022; Ioannou, Stavrou, & Bada, 2019; Reegård, Blackett, & Katta, 2019; Uchendu, Nurse, Bada, & Furnell, 2021; Georgiadou, Mouzakitis, Bounas, & Askounis, 2022; Solange Ghernaouti, 2010; Ubowska & Królikowski, 2022)
Beliefs, perceptions, attitudes, assumptions, norms, and values of employees regarding cybersecurity	(Tsoeu & Da Veiga, 2022; Reid & Niekerk, 2014; Georgiadou, Mouzakitis, & Askounis, 2022; Gcaza & Solms, 2017; Ubowska & Królikowski, 2022; Da Veiga, 2016) (Alshaikh, 2020; Georgiadou, Mouzakitis, & Askounis, 2021; Huang & Pearlson, 2019)
cybersecurity education, training and awareness (SETA), knowledge, skill	(Van Niekerk & Von Solms, 2006; Alshaikh, 2020; Tsoeu & Da Veiga, 2022; Corradini & Nardelli, 2018; Huang & Pearlson, 2019; Uchendu, Nurse, Bada, & Furnell, 2021; Dojkovski, Lichtenstein, & Warren, 2010; Georgiadou, Mouzakitis, & Askounis, 2022)

Table 1: Summary of selected literature and concept mapping

The gap identified in the literature was that cybersecurity culture has been defined and conceptualized from different perspectives based on their research foci, such as behavior, compliance, practice, awareness, or knowledge and training. Therefore, this study proposes a holistic conceptualization of cybersecurity culture based on the concepts from the literature and Schain's (1999) model of organizational culture and Van Niekerk & Von Solm's (2006) Information Security Culture model. Further, the study discusses the lesson that organizations can learn from literature to foster an appropriate cybersecurity culture. In the following section, we present the concepts of cybersecurity culture, the scope used to conceptualize it, and the lesson that organizations can learn to foster cybersecurity culture.

The scope of cybersecurity culture in this context refers to the attributes, elements, or factors (Reegård, Blackett, & Katta, 2019) used to conceptualize, define and foster an appropriate organizational cybersecurity culture (Uchendu, Nurse, Bada, & Furnell, 2021).

5. Discussion

5.1. Concepts and definitions

Research on the cybersecurity culture has emerged recently and has attracted much attention, and numerous definitions have been established. One of the general and frequently cited definitions is proposed by the European Agency for Network and Information Security (ENISA), which reads as the knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values of people regarding cybersecurity and how they manifest in people's behavior with information technologies (ENISA, 2017).

Further, researchers conceptualize cybersecurity culture in many different contexts based on the aim and focus of their study. Such as, some literature contextualizes it from the organizational cultural perspective (Corradini, 2020; Tsoeu & Da Veiga, 2022; Reid & Niekerk, 2014), while others took an organizational behavior perspective (Georgiadou, Mouzakitis, Bounas, & Askounis, 2022; Da Veiga, 2016; Gioulekas, et al., 2022) to define it. Some works of literature also use cybersecurity culture interchangeably with information security culture (Corradini, 2020; Tsoeu & Da Veiga, 2022; Ubowska & Królikowski, 2022; Reid & Niekerk, 2014) others see it as a subculture of organizational or corporate culture (Georgiadou, Mouzakitis, & Askounis, 2021; Reid & Niekerk, 2014; Huang & Pearlson, 2019), and one described as the intersection of information technology and industrial psychology at the workplace (Da Veiga, 2016). A significant number of researchers also understand and define cybersecurity culture from the human behavior perspective which is about the employee's attitude, perception, values, and (Georgiadou, Mouzakitis, Bounas, & Askounis, 2022; Gioulekas, et al., 2022; Tsoeu & Da Veiga, 2022) normative beliefs, and habits (Georgiadou, Mouzakitis, Bounas, & Askounis, 2022). There are also studies that define cybersecurity culture from the point of view of training, education, awareness and compliance with policy and procedures at the workplace (Alshaikh, 2020; Ioannou, Stavrou, & Bada, 2019; Georgiadou, Mouzakitis, Bounas, & Askounis, 2022).

It is notable that only few papers (Alshaikh, 2020; Da Veiga, 2016; Gundu, Maronga, & Boucher, 2019) specifically conceptualize cybersecurity culture in a comprehensive manner. Da Veiga (2016), conceptualizes it as something that "…promotes or impedes the security, safety, privacy, and civil liberties of individuals, organizations, or governments," which covers a broader spectrum than just the security of data, but also the security of people and organizations as a whole (Uchendu, Nurse, Bada, & Furnell, 2021). Alshaikh (2020) also conceptualizes cybersecurity culture in a more comprehensive manner as "…contextualized behavior of people in an organizational context to protect information processed by the organization through adherence to information security policy and an understanding of how to implement requirements in a prudent and attentive manner." They focus on improving security policies, employee behaviors, and training, especially with regard to protecting data and information. Although cybersecurity culture is a subculture of organizational culture, it's not conceptualized in the literature based on organizational constructs. The following sections present concept mapping from literature to Schein's 1999 organizational model to conceptualize cybersecurity culture in an organizational context.

5.2. Mapping concepts from literature to the model

As indicated in the previous section of this study, the literature defines, conceptualizes, and describes cybersecurity culture in different ways and from different perspectives including human factors, organizational behavior, organizational subculture, cybersecurity policy compliance, cybersecurity awareness, employee actions or practices, perception, intention, attitude, norm, belief, values, etc.

While several definitions of cybersecurity culture exist (Alshaikh, 2020; Da Veiga, 2016; Van Niekerk & Von Solms, 2006), this study define it as an organizational construct based on Schain's (1999) model of organizational culture and Van Niekerk & Von Solm's (2006) Information Security Culture model that reflects the artifacts, shared tacit assumptions and espoused values of an organization in relation to cybersecurity competencies and the collective and individual goals at all levels of an organization.

Hence, based on the concepts mapped from the literature and the three levels of Schein's (1999) organizational culture and Van Niekerk & Von Solm's (2006) models, this study, therefore, maps to derive elements used to conceptualize and proposes a holistic definition for cybersecurity culture in an organizational context.

Table 2 below shows the dimensions of Schein's organizational culture model and Van Niekerk & Von Solm's models at all levels parallel with the cybersecurity culture concepts mapped from the literature, as well as derived elements/scopes used for contextualization and scope of cybersecurity culture at the organizational level.

levels of Schein's (1999) organizational culture model	**Dimensions of Schein's (1999) organizational culture model**	**CSC concept identified from literature (as shown in Table 1)**	**Derived CSC elements/scopes**
Artifacts	Logo, structure, dressing code, manner of communication, language, hardware, software, and day-to-day activities and practices of employees at all levels.	Day-to-day cybersecurity practice, actions, activities	Cybersecurity Practices
Espoused values	Cybersecurity Policy, guidelines, standards, vision, mission rules regulations, values, principles, ethics, best practices, shared values,	Cybersecurity Policy, compliance, standards, strategies, and guidelines, Mission and vision	Cybersecurity Policy Cybersecurity Goal
Shared assumptions and beliefs	Beliefs, perceptions, norms, thoughts, feelings, values, attitudes, and actions exhibited on an individual, group, and organizational level	Beliefs, perceptions, attitudes, assumptions, norms, and values	Behavior
Information Security Knowledge (ISK)	Education, Training, orientations	cybersecurity education, training and awareness (SETA), knowledge, skill	Cybersecurity Competency

Table 2: Concept from literature mapped with organizational culture model and derived elements/scopes

The last column of the table contains the derived elements that are important for conceptualizing cybersecurity culture at the organizational level. Using the table summarized above (Table 2), we suggested that the concept and scope of cybersecurity culture should include the four essential elements

or pillars to achieve the organization's cybersecurity goal. Each of the elements also has specific dimensions, as discussed below.

- Cs Practice (day-to-day cybersecurity action, activities, communications, and interactions of employees in an organization)
- Cybersecurity Policy (organizational cybersecurity guidelines, protocols, set of standards, strategies, and manuals of best practice for all employees in order to ensure maximum protection from cybersecurity incidents),
- Cs Behavior (belief, attitude, norm, perception, values, and assumption exhibited by individuals and groups of employees or how they manifest with information technologies regarding cybersecurity in an organization)
- Cs Competency (cybersecurity education, training, awareness, knowledge, skill, experience, a capability that leads to effective and efficient performance or decision in an individual's cybersecurity-related actions and activities)

    - Cs Goal : protection of assets from unauthorized access, modification, and destruction that can be done intentionally via attacks, or unintentionally, due to employee mistakes or natural disasters (AlHogail, 2015; Da Veiga, 2016; ENISA, 2017; Gcaza & Solms, 2017; Georgiadou, Mouzakitis, & Askounis, 2022; Alshaikh, 2020)).

The above four essential elements or pillars of cybersecurity culture are highly interrelated with each other and contribute to the common organizational goal of cybersecurity. As shown in Figure 2, the competency element of cybersecurity culture can be described as a combination of knowledge and actions (Hassandoust & Johnston, 2023) that can improve employee cybersecurity behaviors (beliefs, attitudes, norms, perceptions, values, and assumptions), increase compliance with the organization's cybersecurity policies (Alshaikh, 2020), and should embrace the cybersecurity practices.

Cybersecurity policies drive/enforce and direct the day-to-day cybersecurity practices/actions of employees at all levels and cybersecurity practices should ensure adherence to cybersecurity policy, and cybersecurity policy can emerge from best cybersecurity practices (Von Solms & Von Solms, 2004b). Further cybersecurity policy can shape the cybersecurity competency of the employees.

Employee cybersecurity behaviors should also be aligned with and guided by cybersecurity policies so that cybersecurity behaviors can be manifested and/or become the daily activities or practices of an organization (AlHogail, 2015). The proper interaction of each element helps an organization properly conceptualize and foster an appropriate cybersecurity culture that can serve as a true supplement approach for the technical approaches and achieve a defined organizational cybersecurity goal. The model below is based on Schain's (1999) models of organizational culture and Van Niekerk & Von Solm's (2006) Information Security Culture model.

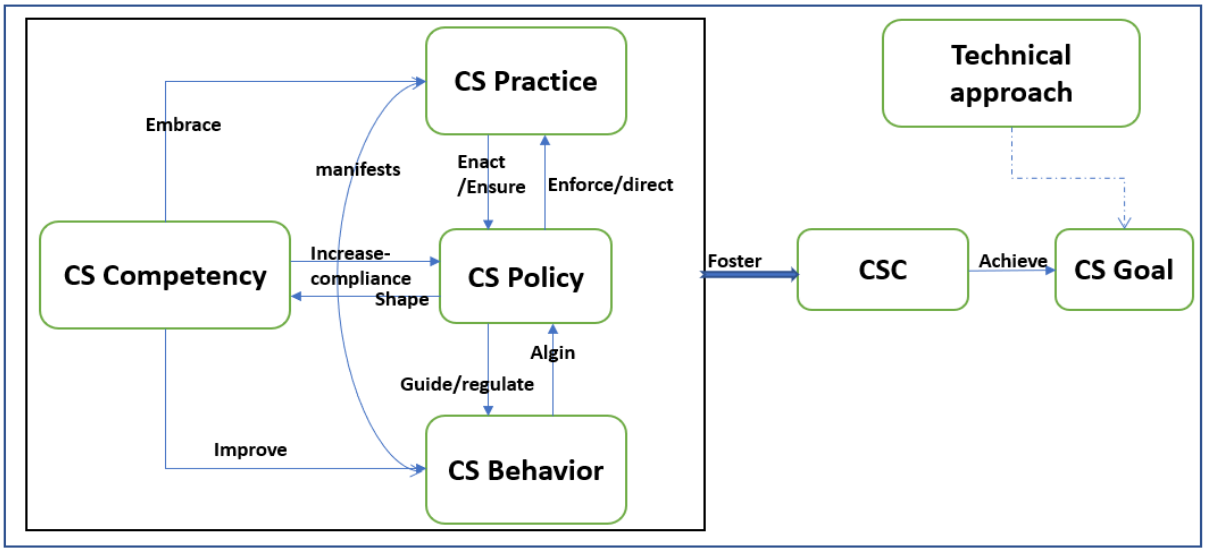

Figure 2: A conceptual model to foster Cybersecurity culture

Further, based on the above conceptual understanding, this study proposes a comprehensive or holistic definition of cybersecurity culture to help organizations understand and foster an appropriate cybersecurity culture. Hence, cybersecurity culture can be defined as:

> *The **competence, behavior** and daily **practice** or action exhibited by individuals and groups at all levels of an organization through adherence to cybersecurity **policies** and procedures to ensure the confidentiality, integrity, and availability of information assets and systems at every point in cyberspace.*

In general, in this study, we conceptualized cybersecurity culture and propose a holistic definition and model based on existing literature and Schein's 1999 organizational culture and Van Niekerk & Von Solm's (2006) Information Security Culture models in an organizational context. To this end, we recommend that future researchers and practitioners consider the important pillars or elements described above to define and conceptualize cybersecurity culture in an organization.

5.3. Lesson Learned to Foster Cybersecurity Culture

In addition to the definition, concept, and scope of cybersecurity culture proposed in the above section, there are several aspects that organizations can learn from the literature to foster their cybersecurity culture. Researchers argued that an appropriate cybersecurity culture is important to prevent human-caused security breaches (Alshaikh, 2020). Hence, organizations need to develop a comprehensive understanding of fostering a cybersecurity culture where security is everyone's responsibility at all levels (AlHogail, 2015; Da Veiga, 2016).

An appropriate organizational cybersecurity culture is based on high employee competency (education, awareness and training) and treating cybersecurity as a key element of culture in the organization (Ubowska & Królikowski, 2022; Corradini, 2020; Tsoeu & Da Veiga, 2022). Organizations should also prepare strong strategies, policies, and procedures to better promote and foster a cybersecurity culture to influence end users' behavior to improve information protection (Tsoeu & Da Veiga, 2022; Reid & Niekerk, 2014) than imposing rules and policies since people do not easily follow rules which are imposed (Corradini, 2020). Employee cybersecurity behaviors must also be aligned with security policies so that cybersecurity culture becomes an organization's daily activities or practices (AlHogail, 2015).

The literature also stated internal and external factors affecting cybersecurity culture in an organization. The most cited internal factors are top management support, awareness, training, policy, education, and procedure (Gioulekas, et al., 2022; Solange Ghernaouti, 2010; Corradini, 2020; Ioannou, Stavrou, & Bada, 2019; Alshaikh, 2020; Reid & Niekerk, 2014). As well as, external factors that affect

cybersecurity culture in an organization include organizational culture (Da Veiga, 2016; Tsoeu & Da Veiga, 2022; Corradini, 2020), international and national cybersecurity policy and standards (Ioannou, Stavrou, & Bada, 2019; Solange Ghernaouti, 2010; Ubowska & Królikowski, 2022), the national culture of the general community (Corradini, 2020), national economic development status (Corradini, 2020; Tsoeu & Da Veiga, 2022) change management (Uchendu, Nurse, Bada, & Furnell, 2021) and national education system (Corradini, 2020; Reid & Niekerk, 2014).

An organization should also understand that cybersecurity culture is unique for an organization and not replicable for others, based on its specific characteristics regarding technologies, processes, and people's values (Corradini, 2020). For instance, according to Corradini (2020) an organization that has never developed security programs has different needs compared to an organization that has already undertaken a security path. In the same way, a small enterprise has different needs compared to a large one (Gioulekas, et al., 2022; Corradini, 2020). Moreover, it must be understood by organizations that it is not important to copy the cybersecurity culture approaches and deploy like the technical cybersecurity solutions in an organization, but it is necessary to contextualize and foster it based on the desires of the organization (Reid & Niekerk, 2014; Tsoeu & Da Veiga, 2022; Kortjan & Solms, 2012). Cybersecurity culture measurement and change should also be done when necessary (Uchendu, Nurse, Bada, & Furnell, 2021) in a seemingly transparent way without affecting their everyday activity, and more importantly, employees need to participate and incorporated in making the improvement, development and change without being discouraged by the radical and rapid changes (Da Veiga, 2016; Georgiadou, Mouzakitis, Bounas, & Askounis, 2022).

Cybersecurity culture could also change over time (Da Veiga, 2016; Georgiadou, Mouzakitis, & Askounis, 2021). Handling a cultural change and fostering an appropriate cybersecurity culture is not a simple process and it requires time, resources, tools, and, above all, active support from top management (Corradini, 2020; Hassandoust & Johnston, 2023).

The other important lesson that organizations can learn from literature is the alignment of cybersecurity culture and risk management strategies. According to the literature, in order to foster a cybersecurity culture and mitigate cybersecurity risks in an organization, it is important to link the individual risks of the traditional silos (Althonayan & Andronache, 2019) and the cybersecurity culture, because nowadays some organizations consider risk responsibility as something that only applies to the individual departments of their organization (Da Veiga, 2016; Hassandoust & Johnston, 2023). This leads to weaknesses in organizational risk defense (due to the silo approach) and can cause serious organizational problems (Althonayan & Andronache, 2019). As employees go about their daily responsibilities, it is the cybersecurity culture that guides their practice about what actions may introduce risk to the organisation, or conversely, reduce such risk (Hassandoust & Johnston, 2023). The security culture also guides how employees communicate with each other and respond to formal and informal organisational risk (Kechagias, Chatzistelios, Papadopoulos, & Apostolou, 2022). Hence, organizations should further consider the proper alignment of risk management and cybersecurity culture strategies to improve their cybersecurity posture in the face of emerging and ever-increasing cyberattacks.

5.4. Future research direction and Limitations

We hope that the results of this study can help future researchers and practitioners clearly understand the definition/concept, and scope and learn how to foster an appropriate cybersecurity culture in an organizational context. The study will also provide practical insights for practitioners to create a valuable cybersecurity policy, address employee competency, and gain valuable insights into employee practice and behavior. Furthermore, organizations can learn from the study to integrate or align cybersecurity culture with other siloed strategies such as organizational risk management and organizational change management strategies.

These results, however, should be viewed in the light of their limitations. First, the research focuses exclusively on the literature on cybersecurity culture. There may be literature on information security culture or security culture that are not considered in this research. It is also possible that some relevant

studies may not be accessible due to search limitations or the scope of the study and have not been included in this study.

Furthermore, future research is invited and crucial to propose a framework to foster an appropriate cybersecurity culture that makes employees at all levels the first line of cyber defense in an organizational context and practice to validate the framework and delineate the proposed definitions using empirical data. We suggest that future research could also focus on aligning organizational cybersecurity culture with organizational change and risk management strategies.

6. Concluding Remarks

The protection of information resources and systems is highly dependent on the organization's cybersecurity culture. Most of the literature indicates that properly understanding and fostering an appropriate cybersecurity culture in an organization, involving all internal and external factors is essential. This study presents the results of a scoping literature review focused exclusively on cybersecurity culture literature and suggests essential elements that can be used to contextualize cybersecurity culture in an organizational context. Furthermore, the study proposes a holistic cybersecurity culture definition and summarizes the key aspects that organizations could learn to foster an appropriate cybersecurity culture. It is important that organizations take a holistic approach to cybersecurity culture that requires collaboration at all levels and is considered an integral part of the organizational culture.

References

AlHogail, A. (2015). Design and validation of information security culture framework. *Computer in Human Behavior, 49*, 567-575.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computer & Security*.

Althonayan, A., & Andronache, A. (2019). Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management alignment. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment.* Oxford.

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. *nternational Journal of Social Research Methodology: Theory and Practice, 8*(1), 19-32. doi:DOI: 10.1080/1364557032000119616

Astakhova, L. (2014). The concept of the information-security culture. *Scientific and Technical Information Processing, 41*, 22-28.

Corradini, I. (2020). *Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology.* Switzerland: Springer Nature.

Corradini, I., & Nardelli, E. (2018). Building Organizational Risk Culture in Cyber Security: The Role of Human Factors. *AHFE 2018 International Conference on Human Factors in Cybersecurity* (p. 201). Florida, USA: Springer Nature.

Da Veiga, A. (2016). A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument. *SAI Computing Conference 2016.* London, UK.

Da Veiga, A. (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information and Computer Security, 26*(5), 584-612. doi:https://doi.org/10.1108/ICS-08-2017-0056

Daudt, H. M., Mossel, C. v., & Scott, S. J. (2013). Enhancing the scoping study methodology: a large, inter-professional team's experience with Arksey and O'Malley's framework. *BMC Medical Research Methodology*.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2010). Enabling Information Security Culture: Influences and Challenges for Australian SMEs. *ACIS 2010.*

ENISA, E. U. (2017). *Cyber Security Culture in organisations.* European Union Agency For Network and Information Security.

Gcaza, N., & Solms, R. v. (2017). Cybersecurity Culture: An Ill-Defined Problem. *IFIP International Federation for Information Processing 2017* (pp. 98-109). Springer International Publishing.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Detecting Insider Threat via a Cyber-Security Culture Framework. *Journal of Computer Information Systems, 62*(4), 906-716.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*.

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., . . . Marin, S. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures . *MDPI Healthcare*.

Gundu, T., & Maronga, V. .. (2019). IoT Security and Privacy: Turning on the Human Firewall in Smart Farming. *Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems* , (pp. 95–104). South Africa.

Gundu, T., Maronga, M., & Boucher, D. (2019). Industry 4.0 Businesses Environments: Fostering Cyber Security Culture in a Culturally Diverse workplace. *4th International Conference on the Internet, Cyber Security and Information Systems. 12*, pp. 85-94. wvvw.easychair.org.

Hassandoust, F., & Johnston, A. C. (2023). Peering through the lens of high-reliability theory:A competencies driven security culture model ofhigh-reliability organisations. *Information Systems Journal*. doi: https://doi.org/10.1111/isj.12441

Huang, K., & Pearlson, K. (2019). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. *52nd Hawaii International Conference on System Sciences.*

Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination. *International Conference on Cyber Security and Protection of Digital Services (Cyber Security).* IEEE.

Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination. *International Conference on Cyber Security and Protection of Digital Services (Cyber Security).* IEEE Xplore. doi:10.1109/CyberSecPODS.2019.8885240

Jennings, C. (2013). *Building Human Firewalls.* Retrieved from Swan Island Network: www.swanisland.net/cybero

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection, 37*. doi:https://doi.org/10.1016/j.ijcip.2022.100526

Kortjan, N., & Solms, v. (2012). Fostering a cyber security culture: a case of South Africa. *Proceedings of the 14th Annual Conference on World Wide Web Applications.*

Levac, D., Colquhoun, H., & O'Brien, K. (2010). Scoping studies: advancing the methodology. *Implementation Science, 5*(1). doi:DOI: 10.1186/1748-5908-5-69

Malmedal, B., & Røislien, H. E. (2014). *The Norwegian Cybersecurity Culture.* Oslo: The Norwegian Business and Industry Security Council.

Mengist, W., Soromessa, T., & Legese, G. (2020). Method for conducting systematic literature review and meta-analysis for environmental science research. *MethodsX, 7*.

Mwim, E., & Mtsweni, J. (2022). Systematic Review of Factors that Influence the Cybersecurity Culture. In N. F. Clarke, *Human Aspects of Information Security and Assurance: IFIP Advances in Information and Communication Technology 2022* (Vol. 658). Springer. doi:https://doi.org/10.1007/978-3-031-12172-2_12

Nasir, A., Arshah, R. A., Hamid, M. R., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications, 44*, 12-22.

National Cyber Security Center. (2017). *Growing positive security cultures*. Retrieved from National Cyber Security Center: https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures

NIST. (2018, April). Framework for Improving Critical Infrastructure Cybersecurity. doi: https://doi.org/10.6028/NIST.CSWP.04162018

Reegård, K., Blackett, C., & Katta, V. (2019). The Concept of Cybersecurity Culture. *Proceedings of the 29th European Safety and Reliability Conference*, (pp. 4036-4043).

Reid, R., & Niekerk, J. V. (2014). From information security to cyber security cultures. *2014 Information Security for South Africa.* IEEE.

Schein, E. (1999). *The corporate culture survival guide.* San Francisco,California, United States of America: Jossey-Bass Publishers.

Solange Ghernaouti. (2010). A national strategy for an effective cybersecurity approach and culture. *International Conference on Availability, Reliability and Security.* IEEE.

Tolah, A., Furnell, S. M., & Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. *Computers & Security, 108*.

Tsoeu, M. A., & Da Veiga, A. (2022). A Cyber4Dev Security Culture Model. In *Communications in Computer and Information Science book series.* Springer Nature.

Ubowska, A., & Królikowski, T. (2022). Building a cybersecurity culture of public administration system in Poland. *Procedia Computer Science*.

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*. doi:https://doi.org/10.1016/j.cose.2021.102387.

Van Niekerk, J., & Von Solms, R. (2006). Understanding Information Security Culture: A Conceptual Framework. *Information Security South Africa - Proceedings ISSA*, (pp. 1-10).

Von Solms, B., & Von Solms, R. (2004b). From policies to culture. *Computer & Security, 23*(4), 275–279.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research, 39*(1), 93-112.

Zakaria, O., Gani, A., Nor, M., & Anuar, N. (2007). Reengineering information Security culture formulation through management perspective. *In Proceedings of the International Conference on Electrical Engineering and Informatics, Institute Teknologi*, (pp. 638–641).

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-computer studies, 131*, 169-187.