BAYBEM
ISSN 2618-6195

İŞLETME EKONOMİ VE YÖNETİM ARAŞTIRMALARI DERGİSİ
THE JOURNAL OF BUSINESS, ECONOMICS AND MANAGEMENT

Yıl: 2024
Cilt/Sayı: 7(1)
Sayfa: 96 - 110

Derleme REVIEW

Gönderilme Tarihi: 10 Ekim 2023; Revize Edilmiş Hali: 7 Aralık 2023; Kabul Tarihi: 15 Aralık 2023

BUILDING A CYBER SECURITY CULTURE FOR RESILIENT ORGANIZATIONS AGAINST CYBER ATTACKS[1]

SİBER SALDIRILARA KARŞI DAYANIKLI ÖRGÜTLER İÇİN SİBER GÜVENLİK KÜLTÜRÜNÜN OLUŞUMU

Cenk Aksoy[1]

Abstract

Cybersecurity has emerged as a critical area requiring 24/7 surveillance, in response to the rapidly increasing frequency of cyber threats. Concurrently, there is a notable amplification in both the allocated budget and the academic interest within this domain. In this cyber risk environment, the success of organizations depends on the weakest link, the human factor. Human errors can be reduced by focusing on the beliefs, values and attitudes guiding employee behavior to protect organizations. In this context, the concept of cybersecurity culture emerges as the key to strengthening cyber resilience in organizations. In this study, the findings obtained from the literature review are presented to determine the definition of cybersecurity culture, its importance and the factors considered important for creating and maintaining this culture. In the study, cybersecurity culture is defined as the set of behaviors formed by beliefs, values and attitudes that shape an organization's approach to cybersecurity. Creating a resilient and sustainable cybersecurity culture is possible by focusing on the human aspects of cybersecurity as much as the technical aspects. Leadership knowledge, skills and abilities, developing cybersecurity awareness throughout the organization, effective communication and acceptance of this transformation as a continuous learning experience are listed among the main factors affecting the cybersecurity culture.

Keywords: Cybersecurity, Organizational Culture, Cybersecurity Culture

Jel Codes: L26, O18, R11, B21

Öz

Siber güvenlik, artan siber tehdit sıklığına yanıt olarak 7/24 gözetim gerektiren kritik bir alan olarak ortaya çıkmıştır. Eş zamanlı olarak hem ayrılan bütçede hem de bu alana olan akademik ilgide dikkate değer bir artış bulunmaktadır. Bu siber risk ortamında, örgütlerin başarısı en zayıf halka olan insan faktörüne bağlıdır. Örgütleri korumak amacıyla çalışan davranışlarını yönlendiren inanç, değer ve tutumlara odaklanarak insan hataları azaltılabilir. Bu kapsamda örgütlerde siber dayanıklılığı güçlendirmenin anahtarı olarak siber güvenlik kültürü kavramı karşımıza çıkmaktadır. Bu çalışmada, siber güvenlik kültürünün tanımı, önemi ve bu kültürü oluşturmak ve sürdürmek için önemli görülen faktörleri belirlemek amacıyla literatür taramasından elde edilen bulgular sunulmuştur. Çalışmada siber güvenlik kültürü, bir örgütün siber güvenliğe yaklaşımını şekillendiren inanç, değer ve tutumların oluşturduğu davranışlar kümesi olarak tanımlanmıştır. Dayanıklı ve sürdürülebilir bir siber güvenlik kültürü oluşturmak, siber güvenliğin teknik yönleri kadar insani yönlerine odaklanmakla mümkündür. Siber güvenlik kültürüne etki eden temel unsurlar arasında liderin bilgi, beceri ve yetenekleri, örgüt genelinde siber güvenlik farkındalığının geliştirilmesi, etkili bir iletişim ve bu dönüşümün sürekli bir öğrenme deneyimi olduğunun kabul edilmesi sıralanmıştır.

Anahtar Kelimeler: Siber Güvenlik, Örgüt Kültürü, Siber Güvenlik Kültürü

JEL Kodları: L26, O18, R11, B21

[1] This study is a revised and expanded version of the paper presented at the 22nd International Business Congress held in Istanbul, Turkey on 7-9 September 2023.

[2] PhD, Mcgill University, drcenkaksoy@gmail.com, https://orcid.org/0000-0003-0763-2847

Citation: Aksoy, C. Building a Cyber Security Culture for Resilient Organizatıons Against Cyber Attacks, İşletme Ekonomi ve Yönetim Araştırmaları Dergisi (2024) 7 (1):96-110, DOI: https://doi.org/10.33416/baybem.1374001

1. INTRODUCTION

Today, cyber means business. It is difficult to underscore the importance of cyber as a fundamental and integral business imperative. This increasingly interconnected phenomenon brings with it new risks and growth opportunities. Digital technologies, exponential growth of data and evolving business needs are expanding the attack threat areas and placing cyber at the center of the business as a strategic business issue. The future of cyber for any organization will be shaped by the business value that the C-suite and the board take on and that the entire organization will be designed with cyber. To preserve this business value in the long term and maintain customer trust, it is critical to neutralize cyber threats (Deloitte, 2023).

Nowadays, managers face enormous challenges in preventing cybersecurity-related attacks in the work environment. In recent years, cybersecurity vulnerabilities have become urgent threats to federal agencies or businesses. Organizations have spent billions of dollars on information technology (IT) systems and software to detect cybersecurity threats (Parenty and Domet, 2019). However, it was understood that the most critical cybersecurity problem is related to the management of individuals (Pollini et al., 2021). However, leaders cannot achieve sufficient success in paying the necessary attention to human behavior in their efforts to keep organizational data safe and plan strategies (Schultz, 2005). For this reason, the phrase "security culture" is a concept that is starting to appear more frequently in the dictionary of security leaders. CISOs (Chief Information Security Officer) and security managers are now beginning to view security culture as a critical element of their security posture. However, because security leaders have very different definitions of security culture, this means that leaders do not really know what they are in for (Roer et al., 2022). In this context, this study, which strives to shed light on the conceptual confusion regarding cybersecurity culture, a relatively new concept that attracts increasing attention, aims to give some clues that can be a resource for security managers and researchers. From this point of view, “Why do organizations need a robust cybersecurity culture?” The answer to the question has been sought.

2. CONCEPT OF CYBERSECURITY

Cybersecurity is typically defined as 'measures taken to protect a computer or network system (such as on the Internet) against unauthorized access or attack' (Merriam-Webster, 2023). The first comprehensive published work that laid the groundwork for the field of cybersecurity was a technical report called Security Control for Computer Systems in 1970 (Ware, 1970). However, cybersecurity has begun to attract more attention in recent years with increasing cyber-attacks.

Warren Buffett, one of the world's most successful investors, sees cybersecurity as more dangerous than nuclear attacks and the number one problem facing humanity. According to the World Economic Forum, most business leaders said cyber attacks were their most significant concern in 2018. Much of the reason for this concern likely stems from the fact that the cost of cybercrime has grown significantly. In just three short years, cybercrime damages are estimated to reach $6 trillion per year, making cyberattacks more profitable than the trade of all illegal drugs (Comptia, 2018).

Technically, many types of cyberattacks arise from various vulnerabilities, weaknesses, and opportunities. Essentially, the first way to classify attacks would be by separating them into two distinct characteristics – malicious and unintentional threats. Speaking, malicious threats can be made by external attackers, malicious employees, or greedy employees looking to sell company data to make a quick buck. Unintentional threats are created by careless employees who act without considering the consequences of their actions. Clicking on emails from unknown sources, opening websites displaying attractive products, or opening emails from outside the office network are prime examples of such attacks (Sandhu, 2021).

In an effort to understand the impact of human factors on cybersecurity, IBM conducted a comprehensive study in 2014, analyzing cyber breaches across a diverse set of thousands of customers in over 130 countries (IBM, 2014). This pivotal study, noted for its extensive scope at that time, found that human error was a significant contributor to cybersecurity incidents, being the primary cause in 95% of all cases examined. These findings have been consistently validated by subsequent research, including a notable study by Nobles in 2018, which reconfirmed the crucial role of human error in cyber breaches (Nobles, 2018). The IBM report's insights are particularly striking when considering the potential impact of these errors: if human mistakes had been eliminated, it is estimated that up to 95% of the breaches analyzed in the study, equivalent to 19 out of every 20 incidents, might have been prevented (IBM, 2014). This highlights the urgent need for comprehensive strategies that address human factors in cybersecurity, emphasizing the importance of training, awareness, and robust security protocols to mitigate the risk of human error. These violations caused by human error can only be prevented by training and raising awareness about security vulnerabilities, that is, by establishing a culture of awareness and alertness in organizations (Sandhu, 2021).

3. CYBERSECURITY CULTURE

3.1. Organizational Culture

Organizational culture, a term that has become common in discussions about corporate dynamics, management practices, and employee behavior, has its roots in the history of organizational and management research. Its introduction to academic discussions can be traced back to the late 1970s, marking a new approach to understanding organizational dynamics beyond just structures and strategies (Glynn et al., 2013). Its growth from a new idea to a central point of organizational studies began in the early 1980s, with scholars giving it more and more attention.

Andrew Pettigrew is often seen as the leading force behind the formal study of organizational culture. In his important study, Pettigrew (1979) described organizational culture as a mix of beliefs, identities, rituals, and myths that collectively guide behavior and decisions within an organization. This definition, while basic, opened the door for many other interpretations and examinations by later scholars.

Building on Pettigrew's ideas, Schein (1985) proposed a layered model of organizational culture, breaking it down into visible signs, stated beliefs and values, and deeper, hidden assumptions. Schein stressed that these layers, while different, work together to shape an organization's mindset. Visible signs, like office decor or company slogans, are just the beginning. The real depth comes from the deep values and assumptions that guide decisions, ways of resolving conflict, and how the organization adapts to change (Schein, 1985).

The late 20th century saw more research exploring how organizational culture affects outcomes. Cameron and Quinn (2006) argued that organizational culture plays a key role in things like performance, employee satisfaction, and overall organizational strength. The research points to four main types of cultures: clan, adhocracy, market and hierarchy. Each of these has its own characteristics, benefits and challenges. As global business grew, the importance of understanding different cultures became more important. Hofstede (1991) studied national and organizational cultures, identifying areas like power relationships, comfort with uncertainty, individual versus group focus, and gender roles. Hofstede's study showed that while businesses might operate globally, cultural differences deeply influence management practices and employee expectations (Hofstede, 1991). In "Dimensionalizing Cultures: The Hofstede Model in Context," Geert Hofstede presents a six-dimensional framework for understanding national cultures. These dimensions, namely Power Distance, Uncertainty Avoidance, Individualism/Collectivism, Masculinity/Femininity, Long/Short Term Orientation, and Indulgence/Restraint, provide insight into various cultural traits. The model is particularly useful in organizational settings for analyzing the impact of cultural differences on management styles and employee expectations. Each dimension offers a distinct perspective on how cultural norms and values shape organizational behavior and attitudes (Hofstede, 2011).

The move into the 21st century brought new challenges and opportunities, making the study of organizational culture even more relevant. With advances in technology and the rise of online workspaces, the idea of culture expanded to include how organizations operate online. Gibson and Gibbs (2006) looked at the challenges of creating a shared culture in online teams, emphasizing the need for trust, clear communication, and mutual understanding.

Also, a growing focus on sustainability and corporate responsibility changed organizational goals. Linnenluecke and Griffiths (2010) examined how culture drives sustainable practices and the importance of adding environmental values to the organization.

Recently, the COVID-19 pandemic showed how important organizational culture is when facing unexpected challenges. Adaptive cultures, marked by flexibility, understanding, and teamwork, became important support pillars for organizations during these uncertain times (Denison et al., 2020).

Starting from historical academic discussions, organizational culture remains a changing and growing field. As organizations navigate the changing business world, the role of culture as a guiding force is clear. The beliefs, rituals, values, and myths, as Pettigrew (1979) first mentioned, shape daily operations and help decide the strategic direction, ensuring long-term success.

Highlighting the evolution of cultural understanding within organizations, the journey from Pettigrew's foundational insights to Hofstede's intricate models underscores how culture shapes organizational dynamics. As we transition into the digital era, we face challenges and opportunities that redefine these cultural frameworks. The upcoming exploration of digital transformation reveals how this shift revolutionizes not only technological aspects but also the cultural fabric of organizations, necessitating a shift in values, practices, and approaches to adapt and thrive in a rapidly evolving business landscape.

3.2. Digital Transformation of Organizational Culture

In today's digital era, the transformation of organizations extends beyond just technologies and operations; it profoundly impacts the very fabric of organizational culture. Digital transformation, a term popularized in the last decade, reflects the integration of digital technologies into all business areas, leading to fundamental changes in how organizations operate and deliver value to their stakeholders (Westerman et al., 2014). However, it is the deeper cultural shift that genuinely characterizes the essence of this transformation.

Organizational culture, the shared values, beliefs, and practices of members within an organization (Schein, 1985), experiences significant disruption with digital integration. This is not just due to the introduction of new technologies but also because of the evolving ways of thinking and working that these technologies facilitate. Such changes necessitate a cultural adaptation to fully harness the potential of digital tools.

The onset of digital transformation has compelled organizations to foster a culture of continuous learning. As technologies such as artificial intelligence, big data, and the Internet of Things become integral to operations, there's an imperative need for employees at all levels to adapt and upgrade their skills (Berman & Bell, 2011). Traditional hierarchical structures are giving way to more agile and flexible models that promote collaboration, innovation, and quick decision-making.

Moreover, as Kane et al. (2015) observed, digitally maturing organizations are more likely to experiment and take calculated risks. This change fosters a culture where failure is seen not as a setback but as a learning opportunity. This shift in perspective, where experimentation is encouraged and failure is accepted as a part of the growth process, stands in stark contrast to traditional organizational cultures that might resist change.

Bridging the digital skills gap is a significant challenge in the digital transformation journey. While younger employees, often termed 'digital natives', might be more comfortable with new technologies, organizations must ensure that all members, irrespective of age or background, are equipped to function in a digital-first environment (Schwartz & Murnane, 2018). Organizational culture should thus emphasize inclusivity, ensuring that no one is left behind in the digital shift.

Digital transformation also reshapes communication dynamics within organizations. The growth of remote working and the reliance on digital communication tools necessitates a culture of transparency and effective communication. The traditional boundaries defined by physical presence are blurred, and teams across geographies must collaborate seamlessly. As Fitzgerald et al. (2013) highlighted, a digitally transformed organizational culture promotes open communication, leveraging digital tools to enhance rather than impede human connection.

Furthermore, digital transformation influences organizational values and ethics, especially concerning data privacy and cybersecurity. As organizations handle vast amounts of data, there's a growing responsibility to protect customer and employee information. This challenge necessitates a cultural emphasis on ethical data handling and robust cybersecurity practices (Verma & Bhattacharyya, 2017).

However, it's not just the challenges that define the digital transformation of culture; it's also the plethora of opportunities. Organizations can foster a culture of global collaboration, leveraging digital tools to unite teams from diverse cultural backgrounds. This can lead to enriched organizational practices, drawing from a broader pool of experiences and insights (Bharadwaj et al., 2013).

The digital transformation of organizational culture is an intricate journey beyond the mere adoption of new technologies. It is about reshaping values, beliefs, practices, and mindsets to thrive in a digital-first world. As organizations navigate this transformation, they must emphasize continuous learning, inclusivity, agility, effective communication, and ethical practices. By doing so, they can harness the full potential of digital tools while fostering a resilient, innovative, and forward-looking culture.

3.3. Concept of Cybersecurity Culture

Culture is everywhere. Just as every organization has its own organizational culture, every organization also has its own security culture. This means that organizations already have a safety culture, even if they do not yet have established culture management programs. Safety culture is often thought of as a separate concept in itself. The idea that security culture is something new, something that exists by itself and for itself in a special, possibly even secret, place in the organization is not true. Safety culture is not independent of the organizational environment but is a part of the organizational culture (Alnatheer et al., 2012). It is not separate or more critical than organizational culture. Safety culture is a subculture within a broader organizational culture (Wiley et al., 2020). Just as organizational culture exists throughout the organization, so does security culture. Just as corporate culture changes over time, sometimes intentionally, because it is not managed correctly, the same is true for security culture (Carpenter and Roer, 2022).

Cybersecurity culture is based on an organization's specific attributes, tools, practices, and community values. It is about employees making cybersecurity issues an integral part of their work, habits and behavior and incorporating them into their daily actions. A resilient cybersecurity culture relies on employees willingly adopting and proactively using cybersecurity practices, both professionally and personally. It is up to business managers to ensure that the cybersecurity culture reflects the knowledge, beliefs, values, and behaviors that accurately represent the targeted culture (Triplett, 2021).

When the definitions regarding cybersecurity culture are examined, Huang and Pearlson (2019) state that the concept "is the beliefs, values, and attitudes that guide employee behavior in organizations to protect and defend against cyber attacks" (p.6399); Alshaikh (2020) states that human behavior towards the protection of processed information is addressed in an organizational context through regular communication, awareness, training, and education initiatives in line with the information security policy, and Roer et al. (2022) stated that "an organization has ideas, traditions, and social behaviors that affect its cybersecurity" (p.6).

Although it is not possible to find a standard definition in the literature, the definitions reveal that cybersecurity culture is a combination of thought processes and knowledge, habits adopted by employees, and behaviors exhibited in the workplace. From this point of view, in this study, cybersecurity culture is defined in the most general sense as "the set of behaviors formed by beliefs, values and attitudes that shape an organization's approach to cybersecurity".

Cybersecurity culture has been systematically evaluated in seven different dimensions (Roer et al., 2022; Carpenter and Roer, 2022). These are attitudes, behaviors, cognition, communication, compliance, norms, responsibilities.

1. Attitudes: Employees often harbor certain emotions and convictions concerning security procedures. Beyond these feelings about protocols, it is beneficial to grasp the deeper value and motive behind these measures, urging individuals to recognize not only the "what" and "how" but also the underlying "why."

2. Behaviors: Employee actions, whether direct or indirect, influence an organization's security posture. Viewing these behaviors as cultivated habits rather than singular actions offers a comprehensive perspective. Cultivating a habitual mindset towards security can make it second nature for employees, driving proactive actions, reducing mistakes, and anticipating threats.

3. Cognition: An employee's grasp, awareness, and insight into security topics are paramount. Coupling this understanding with the ability to think critically and adapt swiftly offers a balanced approach. With the evolving nature of cyber threats, continuous learning and upskilling align an employee's cognitive prowess with the latest threat scenarios.

4. Communication: The caliber of dialogue channels when broaching security matters determines the organization's responsiveness to threats. Fostering an environment of openness and transparency, combined with quality communication, encourages employees to report security issues, making feedback integral in shaping the organization's security strategy.

5. Compliance: Being informed about security policies is essential, and the degree of adherence showcases an organization's commitment to these policies. Compliance, however, benefits from adaptability to the fluctuating cyber environment. Regularly revising and making policies pertinent and viewing compliance in a favorable light facilitates intuitive adherence for employees.

6. Norms: Knowledge and alignment with an organization's implicit behavioral rules establish its cultural foundation. These norms, when flexible, adjust to the organization's evolving needs. Underlining shared cybersecurity values fosters a sense of communal responsibility, making accountability a collective endeavor.

7. Responsibilities: Employees' sense of duty, whether safeguarding or potentially impacting security, remains a crucial factor. Broadening this sense of responsibility beyond their roles instills a sentiment of collective ownership. When cybersecurity becomes a communal effort, the entire organization, irrespective of its hierarchy, engages in a proactive cybersecurity stance.

These dimensions can be used to increase security awareness and reduce vulnerabilities by covering all aspects of an organization's cybersecurity culture. These dimensions are important for developing safety strategies and influencing employees' safety-related behavior.

3.4. The Importance of Cybersecurity Culture

Cybersecurity culture is an emerging approach for organizations and individuals to develop appropriate behaviors shaping their cybersecurity approach. The primary purpose of cybersecurity culture is to ensure that individuals and organizations take cybersecurity measures to prevent the occurrence of cyber threats and minimize

cybersecurity risks. A resilient cybersecurity culture can help prevent data breaches, protect customer data, and prevent attacks in the first place.

There are many benefits to having a robust cybersecurity culture within an organization. Perhaps most importantly, it helps reduce the likelihood of a successful attack. This is because employees who are aware of the importance of security are more likely to notice potential threats and report them before they cause any harm (Reid and Van Niekerk, 2014). A good cybersecurity culture contributes to developing personnel's knowledge, skills, and abilities to restore the interrupted system as soon as possible during an attack. Organizations with a robust security culture instill trust in customers and business partners, which can help strengthen business relationships. These organizations can make the connection between cybersecurity efforts and business value. Initiatives to improve cybersecurity culture have the power to create a largely positive impact on the following topics (Deloitte, 2023):

Brand Reputation: A robust cybersecurity culture can significantly elevate an organization's brand reputation. As consumers, suppliers, and partners interact with businesses, their trust is invariably linked to the company's security protocols. Ensuring business operations are conducted securely and that data is protected, instills a sense of reliability. By forestalling potential data breaches, an organization not only safeguards its assets but also solidifies the trust of its stakeholders, ultimately amplifying the brand's overall standing.

Customer and Digital Trust: The sanctity of data is paramount in today's digital era, making cybersecurity a cornerstone of building and maintaining trust. When customers and partners have confidence in an organization's commitment to protect their data, it strengthens the foundation of digital trust. An effective cybersecurity culture assures stakeholders of the company's dedication to data protection, which can manifest as increased loyalty and potentially uncover new avenues of business collaboration.

Operational Stability Including Supply Chain and Partner Ecosystem: Operational stability extends beyond an organization's immediate environment. As businesses become more intertwined, the security of external entities, like supply chains and business partners, becomes integral. Cultivating a cybersecurity culture that promotes secure data exchange practices with these external entities ensures that the entire operational ecosystem is safeguarded. By proactively preventing data breaches and fortifying external collaborations, an organization ensures continuity, making its operations more resilient to cyber threats.

Revenues: The financial implications of cybersecurity cannot be overlooked. Strategic investments in cybersecurity not only serve to protect the organization's assets but also have the potential to drive revenue growth. The company can avoid several associated costs by averting data breaches, from potential customer attrition to legal repercussions. In a market where security can be a differentiator, displaying a fortified environment can attract more business opportunities, thereby leading to increased revenues.

Today, businesses are moving away from asking how much cybersecurity costs and towards asking how much it costs not to have a cybersecurity program. However, by eliminating this question, cybersecurity should be integrated into the organizational culture and how security can be maintained as cyber factors change should be questioned.

3.5. Technical and Behavioral Aspects of Cybersecurity

The evolving landscape of cybersecurity emphasizes a dual-pronged approach, as underscored by existing literature. Historically, researchers and industry experts have divided their analysis of organizational cybersecurity into two distinct yet interrelated paradigms: the technical (or technological) and the behavioral (or sociological) dimensions (Schultz, 2005; Corradini, 2020). This division stems from the innate nature of cybersecurity challenges that straddle the realms of tangible technology and intangible human behavior.

While technological solutions are often at the forefront of cybersecurity discussions, they represent only half of the broader equation. The pivotal role of human behavior in determining the efficacy of these technological solutions cannot be understated. A common misconception highlighted by Metalidou et al. (2014, p. 425) is the overreliance on technology as a complete solution for information security challenges, often overlooking the crucial human element that is fundamental to security. Essentially, while advanced software may be used to protect data, the human interaction with these systems can, unintentionally, make them susceptible to vulnerabilities.

Recognizing and understanding this human-centric facet of cybersecurity becomes imperative. The essence of creating a resilient organizational framework hinges on the philosophy of centering people within the design and implementation of security structures and policies. This is more than just understanding technical know-how; it encompasses recognizing the intricacies of human behavior, preferences, motivations, and potential oversights. Nobles (2018) echoed a similar sentiment, highlighting that while there's an overwhelming focus on technical nuances in cybersecurity literature, people's actual behavior, needs, and day-to-day operations are sometimes relegated to the background.

Such a skewed emphasis has tangible repercussions. Decision-makers, swayed by the allure of cutting-edge technologies, may heavily invest in state-of-the-art systems while concurrently sidelining or even bypassing investments in the organizational apparatus. These apparatuses, like nurturing an informed organizational culture, are pivotal in bolstering cyber resilience. As Triplett (2021) aptly posits, technology alone cannot be the bulwark against cyber threats. The linchpin often is the collective behavioral disposition of an organization's members. Irrespective of the technological defenses in place, uninformed or complacent decisions by individuals can jeopardize the entire security framework.

This intertwining of technology and behavior extends from the boardroom to the grassroots of an organization. It's not merely a matter of individual cognition regarding cybersecurity but encompasses broader organizational values, priorities, and collective actions. Ensuring this synergy is maintained requires an understanding that cybersecurity isn't a siloed domain. It necessitates a convergence of technological advancements and organizational behavioral insights.

Corroborating this perspective, recent research findings, such as those presented by Huang and Pearlson (2019), underline that the blueprint for a genuinely cyber-resilient organization is predicated on harmonizing technological advancements with strategic organizational investments. This synthesis ensures that while technology provides the tools to counter cyber threats, the informed, vigilant, and proactive behavior of the organization's members ensures these tools are wielded effectively.

The interplay between the technical and behavioral aspects of cybersecurity is akin to a precisely choreographed dance, requiring balanced attention to both elements. For organizations seeking to strengthen their cybersecurity defenses, it's essential to adopt a comprehensive approach that not only incorporates advanced technology but also deeply understands human behavior.

3.6. Conceptual Difference Between Cybersecurity and Information Security

Both cybersecurity and information security are vital areas in the digital world, often generating similar discussions due to their interconnected nature. While they share many similarities, both in concept and in the managerial practices they emphasize, a deeper look reveals distinct differences. Wiegmann et al. (2002) highlighted these shared traits, which are frequently mentioned in scholarly literature on security culture. These include:

- The foundation of shared values within a group or the entire organization.
- A close relationship with management structures and control systems.
- The strong emphasis on full participation, involving every member within the organization.
- A direct impact on the behavioral patterns shown by organizational members in their work roles.

However, these broad similarities should not hide the clear differences between "cybersecurity" and "information security". Although sometimes used interchangeably in academic writing (Reid and Van Niekerk, 2014), these terms cover different aspects of the digital security field. As clarified by Von Solms and van Niekerk (2013, p. 101), "Information security is about protecting information - a valuable asset, from potential harm caused by various threats and security weaknesses." In contrast, "cybersecurity goes beyond just the protection of the digital space to also safeguard the users operating within this space and their assets that can be accessed online."

A key difference appears when considering the role of people in these areas. Information security mainly connects the human element with specific roles people play in security processes. On the other hand, cybersecurity offers a broader view. It sees individuals as possible targets of cyber attacks or even as people who might unknowingly help in these attacks (Reegård et al., 2019).

Using foundational definitions, like those given by the National Institute of Standards and Technology (NIST) in 2013, provides further clarity. While information security focuses on "protecting the safety, completeness, and availability of information and its systems from unauthorized actions that could cause breaches ensuring privacy," cybersecurity aims to build an organizational ability to "defend against possible cyber attacks." While the first stresses following established information security policies, the latter includes this adherence and adds active personal involvement in strengthening the wider cyber environment (Huang and Pearlson, 2019).

A different viewpoint by Von Solms (2010) adds another layer to this discussion. He suggests that cybersecurity might be seen as the next step in the development of information security. Such an idea highlights the changing nature of this field and its ongoing growth in response to new threats.

This close relationship between information security culture and cybersecurity culture requires an understanding that while they have similar focuses, they are not the same. At its core, the information security culture is about

the safety and protection of data and information. However, cybersecurity culture, while including these focuses, also looks at a wider network of digital interactions and potential risks (Astakhova, 2014).

The distinction between cybersecurity and information security, while subtle, is important. Recognizing their differences and similarities ensures a more complete and informed approach to digital protection, allowing for a strategy that properly addresses the challenges of today's digital age.

4. FUNDAMENTAL FACTORS FOR ESTABLISHING A ROBUST CYBERSECURITY CULTURE

Uchendu et al., (2021) identified and analyzed 58 research articles between 2010 and 2020 on what elements are required to create and maintain a cybersecurity culture. Elements often considered important for creating and maintaining a cybersecurity culture: senior management support, leadership, security policy, security awareness, security training, change management, compliance, information, accountability and responsibility, security risk, commitment, communication, motivation, trust, national culture, ethical behavior, regulations, rewards and sanctions (Uchendu et al., 2021).

Reegård, Blackett, and Katta (2019), who conducted a literature review of 69 articles to determine the dimensions of cybersecurity culture and how organizations can target them, found that the essential practices for developing cybersecurity culture are similar to those emphasized in security culture in the literature and that these include management support, policy, awareness. He stated that education, participation and communication, and learning from experiences.

As organizational leaders identify human behavior and processes and collaborate with followers aiming for the same goal, cybersecurity culture and strategy within an organization can improve significantly. Cybersecurity has become an expanding focus for human factors. It may be unintentional due to human error, poor execution or planning. The results show that humans are the weakest link when transmitting secure data. Therefore, implementing cybersecurity should focus on education, awareness, and communication (Triplett, 2022). In the light of the literature, this study discussed the factors of leadership, awareness, communication and education among the factors that play an important role in forming a robust cybersecurity culture.

4.1. The Crucial Role of Leadership in Shaping Cybersecurity Culture

Leadership is a pivotal cornerstone in the edifice of an organization's culture, particularly in the realm of cybersecurity. Leaders act as shields at the helm, safeguarding the organization from external influences. Concurrently, they have the authority to allocate limited resources, making them the prime decision-makers. But beyond this functional role, leaders shape the very mindset of their employees. Witnessing leaders actively engaging in and emphasizing the importance of cybersecurity operations greatly boosts the morale and commitment of employees to these practices (Huang and Pearlson, 2019).

While it's apparent that leaders oversee cybersecurity operations at a broad level, the depth of this responsibility is often underestimated. Leadership isn't merely about direction; it's about possessing the right caliber. This involves having an in-depth understanding and the required skills to address the multifaceted challenges that arise in cybersecurity, encompassing its technical, managerial, governance, and institutional dimensions (Kuusisto and Kuusisto, 2013).

Technical proficiency, while undeniably vital, isn't the only requisite in this domain. The ability to engage, communicate, and influence is just as crucial, if not more. Without effective communication and the willingness to shoulder responsibility for the security practices of their subordinates, a leader's technical prowess loses its significance. This underscores the importance of social competencies and the accumulation of social capital for leaders, which enable them to effectively guide non-technical personnel in the realm of cybersecurity (Rotherberger, 2016).

Setting the right objectives is another critical aspect of leadership. In the context of cybersecurity, these objectives should ideally be aligned with ensuring the sanctity of the digital business framework. Moreover, leadership isn't just about being proactive but also reactive. Being equipped to handle unforeseen challenges, managing disruptions, and orchestrating coherent action plans are paramount. The strength and clarity of leadership, particularly on cybersecurity matters, are indispensable in realizing an organization's vision for digital safety (Lehto and Limnell, 2020).

Now, understanding the historical context further underscores the importance of leadership in cybersecurity. In the early days of digital transformation, cybersecurity was often an afterthought. However, as cyber threats evolved and became more sophisticated, organizations began to realize the importance of a proactive approach to cybersecurity. Influential leaders recognized these evolving threats early on and took decisive actions to mitigate

risks. As the digital landscape changed, so did the nature of threats. Leaders had to deal with external and internal threats. Insider threats, often overlooked, became a significant concern for many organizations. In this case, effective leadership involved creating a culture of trust, transparency, and continuous education. Encouraging employees to report suspicious activities without fear of repercussions became an essential strategy, and leaders played a crucial role in instilling this culture. With the advent of new technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI), the attack surface for cyber threats expanded exponentially. Leaders had to be agile, constantly updating their knowledge and strategies to address these ever-evolving challenges. They also had to ensure that their teams were equipped with the necessary skills and tools to tackle new threats. Leadership's role in cybersecurity is multifaceted, encompassing the strategic and operational aspects of an organization's defense mechanisms. Leaders not only set the tone and direction for cybersecurity practices but also play a critical role in molding the mindset of their employees. Their actions, decisions, and priorities significantly influence how cybersecurity is perceived and practiced within an organization.

4.2. Communication as a Pivotal Element in Fostering Cybersecurity Culture

The interplay between communication and cybersecurity is multifaceted and profound. Communication, at its core, acts as a linchpin that reinforces cybersecurity principles. In contexts where collaboration is essential, communication emerges as a crucial component driving the overarching strategy for security (Kuusisto and Kuusisto, 2013).

For corporate entities, the role of communication extends beyond just cybersecurity implementations. It significantly impacts both cyber and human dimensions within and beyond organizational boundaries. This vital function determines not just the efficacy of cybersecurity measures but also the long-term viability of an enterprise. A discordant communication strategy or approach can, conversely, impede the desired outcomes of cybersecurity initiatives (Uchendu et al., 2021). The restrictive flow of information within the IT sector, especially, can set managers up for failure. The incessant challenge of keeping up with evolving cyber threats can amplify the stress and strain on both managers and their teams, potentially leading them to become detached from colleagues. In this light, companies aiming for a robust cybersecurity posture should expand their competency evaluations, moving beyond mere technical prowess to include facets of communication and interpersonal skills (Dawson and Thompson, 2018).

Creating a resilient cybersecurity ethos necessitates leaders to be not just articulate but also resonant in their communication. Tailoring messages to align with varied audiences is indispensable. Additionally, in an era marked by global operations, leaders' proficiency in cross-cultural communication becomes paramount. Such leaders often find themselves steering teams hailing from diverse cultural backdrops, thereby presenting distinct challenges (Matveev and Nelson, 2004). Mastery over the nuances of such communication is essential, demanding both acumen and adaptability to ensure harmonious interactions with individuals of assorted cultural affiliations.

The labyrinth of cross-cultural interactions is intricate, and successfully maneuvering through it isn't trivial. Building a robust cybersecurity ethos while simultaneously managing cultural transitions calls for a blend of patience, adeptness, and strategic insights. The requisite tools and resources further complement this, all anchored by unwavering leadership support. As the landscape of cybersecurity and cultural challenges augments, there will be an escalating need for leaders adept in mending communication fissures (Triplett, 2021).

As organizations ventured into the digital domain, the focus primarily lay on technical advancements. However, with the rise of global operations, the emphasis on effective communication, especially in the context of cybersecurity, has seen a substantial surge. Leaders today recognize that a holistic cybersecurity approach goes beyond just technology; it necessitates a seamless integration of communication strategies, both within and outside the organization. The changing nature of threats in the digital era, both from internal and external sources, highlights the importance of transparent and effective communication. Organizations have now realized that fostering a culture of open communication can significantly mitigate risks by encouraging employees to report suspicious activities promptly. Understanding local norms, behaviors, and cultural nuances becomes crucial as organizations expand their operations across different regions. In such scenarios, communication isn't just about language but understanding and adapting to these local nuances, which can significantly impact cybersecurity practices. Communication stands at the confluence of effective cybersecurity practices and cultural understanding. As organizations traverse the digital transformation journey, the role of effective communication, both in terms of strategy and execution, will be paramount in shaping a resilient and adaptive cybersecurity culture.

4.3. Importance of the Awareness Factor in Nurturing a Cybersecurity Culture

Safeguarding an organization's digital assets has transcended beyond being just an obligation for the IT sector. Today, fostering a culture of cybersecurity demands collective awareness and participation from all tiers of the organization (NIST, 2018). The commencement of this security-oriented culture pivots on the axis of awareness.

Indeed, one of the most influential factors bolstering an organization's resilience to cyber threats is heightened employee cognizance regarding cyber-attacks. When employees grasp the nuances of cyber threats and recognize their individual roles in combatting these risks, the organization's cyber defenses naturally amplify (World Economic Forum, 2023).

Achieving optimal cybersecurity within professional environments hinges on the proactive involvement of employees in risk mitigation and enhancement of cyber defenses. This necessitates fostering a heightened sense of cyber awareness among the workforce. This initiative, termed the "human factor of cybersecurity," delves deep into shifting human behaviors in synergy with technological systems, policies, and protocols. The essence of this approach is to acknowledge the pivotal role of human interactions with technology and craft security strategies that resonate with this understanding (Da Veiga et al., 2020).

When dissecting the anatomy of a robust security culture, the recurring motif is that of security awareness. This facet is either the core of security culture definitions or a dominant element of it (Nel and Drevin, 2019). Security awareness can be encapsulated as a state where organizational members are aligned with and deeply committed to the security agenda (Siponen, 2000). The transition towards a culture steeped in cybersecurity aims to seamlessly integrate organizational cyber awareness with its broader cultural ethos, ensuring the human element remains central to this transformation.

Historically, as technology rapidly permeated the organizational landscape, there was a disproportionate focus on technological advancements, often sidelining the human elements. However, as cyber threats grew in complexity and stealth, it became evident that technology alone wasn't the panacea. Studies showed that human error or oversight was a recurring theme in many cybersecurity breaches. This revelation shifted the narrative towards integrating human-centered strategies in cybersecurity frameworks. Organizations started recognizing that even the most advanced technological defenses could be rendered futile if employees were not cognizant of basic cyber hygiene practices. Simultaneously, the ever-evolving digital landscape brought forth challenges like social engineering attacks, which specifically targeted the human element. Phishing, for instance, became a prevalent method where attackers duped employees into revealing sensitive information. Such threats underscored the need for continuous employee training and awareness programs, ensuring they remain vigilant and updated about emerging threats (Adams and Rogers, 2016).

Another dimension to consider is the diverse makeup of modern workplaces. With employees from varied backgrounds and varying degrees of tech-savviness, it became essential to tailor awareness programs that catered to this diverse audience. Tailored training modules ensured that all employees, regardless of their technical proficiency, understood the basics of cyber threats and the best practices to counter them. In essence, the interplay between humans and technology is at the heart of contemporary cybersecurity strategies. An organization's cybersecurity posture is as robust as its least informed member. Hence, instilling a culture of continuous learning, awareness, and vigilance is indispensable in today's digital age.

4.4. The Impact of Education in Shaping a Cybersecurity Culture

Cybersecurity, an ever-evolving domain, greatly benefits from comprehensive educational undertakings designed to elevate skills, deepen knowledge, and amplify awareness. The essence of these educational ventures is not merely about information absorption, but an active transformation in the way individuals perceive and engage with information security. A widespread practice among organizations is the initiation of new recruits into the world of cybersecurity through dedicated training modules, ensuring they start their journey with a firm grasp of organizational security protocols. Yet, a single bout of onboarding training might not suffice in ensuring persistent secure behaviors. Instead, a rhythmic cadence of updated, periodic, and varied training sessions is advocated for true cybersecurity mastery (Huang and Pearlson, 2019).

To truly instill a culture that prioritizes cybersecurity, the educational lens must focus on ensuring every employee is adept at identifying potential breaches, making them sentinels against vulnerabilities. Tailoring training to resonate with individual needs can be achieved by profiling employees based on their awareness and inclination towards adhering to cybersecurity norms. At its heart, the human element emerges as the linchpin in an organization's cyber defense mechanism, effectively dictating the triumph or setback in cybersecurity endeavors (Glaspie and Karwowski, 2018).

The promotion of formidable cyber defense mechanisms leans heavily on education and training. The onus of championing these pillars rests on the shoulders of organizational leaders. Their role transcends mere policy implementation; it's about stewarding and infusing vitality into training regimes (Parenty and Domet, 2019). This leadership role isn't limited to orchestrating employee training. Cybersecurity stalwarts stand as bulwarks against sophisticated cyber adversaries, achieved by crafting a holistic learning ecosystem. Such systems amalgamate both technical acumen and sociocultural insights, continuously honing their competencies for unparalleled cybersecurity prowess (Burrell, 2021).

Historically, as organizations burgeoned in the digital landscape, there was a keen emphasis on rapid digitalization, often sidelining the importance of robust security education. However, as cyber threats began to loom larger and became intricate, the narrative experienced a shift. A study revealed that well-informed employees acted as the first line of defense against potential cyber threats, significantly reducing breaches' incidence (Smith and Patel, 2020).

Education and training, thus, became indispensable tools for organizations aiming to bolster their cybersecurity posture. As digital transformations took organizations to global frontiers, the need for a unified cybersecurity culture became paramount. Tailored training sessions catering to regional nuances and sensitivities ensured that global teams were in sync with the organization's cybersecurity ethos, irrespective of their geographical locations. Additionally, with the advent of new-age technologies and practices, organizations recognized the importance of continuous learning. Training sessions evolved from being mere theoretical knowledge dissemination sessions to hands-on, scenario-based training modules. Simulating real-world cyber threats in a controlled environment ensured that employees could practice their responses, making them better prepared for real-world scenarios. The fabric of a robust cybersecurity culture is interwoven with threads of comprehensive education and training. As organizations navigate the intricate maze of the digital world, fostering a culture steeped in cybersecurity awareness and preparedness will be their guiding light.

5. CONCLUSION AND RECOMMENDATIONS

In this study, findings from a literature review trying to explain the concept of cybersecurity culture in organizations are presented. The study's findings highlight the definition and significance of cybersecurity culture, identifying human vulnerability as a critical aspect in security systems. Cybersecurity culture is not for computers, but primarily for people, who are the key to a secure culture. They are people who click on things they receive in email and unintentionally believe what bad actors tell them, while computers do exactly what they are told to do. A cybersecurity culture is needed to provide this awareness, training and support to people who want to do the right things in organizations and seek a safe working atmosphere. It has been determined that among the main concepts similarly emphasized in the literature on improving cybersecurity culture are issues such as leadership, awareness, communication and education (Reegård, Blackett and Katta 2019; Uchendu et al., 2021; Triplett, 2022).

Cybersecurity has become increasingly important in the digital age as businesses must ensure the security of their digital data and networks. A secure cybersecurity culture is essential for any business to protect its data, reputation and customers. Creating a safe cybersecurity culture is a process that requires ongoing dedication and investment. Identifying and addressing potential risks, training employees, and implementing the right security measures are essential components of a safe cybersecurity culture. This study discusses basic information on how to create a safe cybersecurity culture for businesses through organizational mechanisms. Business owners and senior executives can use this information to protect their data and networks against cyber threats.

In a safe cybersecurity culture, employees understand their roles and responsibilities regarding cybersecurity. Employees know how to identify and report potential risks and are trained to prevent or reduce these risks. They also understand how their actions and habits affect the cybersecurity of the business. Ensuring a safe cybersecurity culture means engaging employees in an ongoing process of cybersecurity awareness and training. It also means integrating cybersecurity into all business processes, including recruiting, operations and management. If employees understand how their actions impact cybersecurity, they will be more likely to report potential risks or make cybersecurity improvements. Additionally, a safe cybersecurity culture means the organization is prepared to respond to and recover from cyber incidents.

In enhancing cybersecurity values and attitudes, managerial decisions about performance, oversight, and governance play a pivotal role. This research highlights actionable steps for building a cybersecurity-focused organizational culture, which is vital for enhancing cyber resilience. The study points out four main areas: the importance of top management actively engaging in cybersecurity actions, raising awareness of cyber threats across the organization, the need to craft effective communication strategies, and ensuring ongoing and current training in cybersecurity.

Among these, the foremost is effective leadership. It's up to the managers to shape an organizational culture that prioritizes cybersecurity. Effective leadership, especially from senior executives familiar with cybersecurity challenges, is crucial. Such leaders can institute transformative changes. A culture endorsed by upper management can foster a collaborative and innovative workspace. It's essential for senior leaders to work closely with chief information security officers in charting out a cybersecurity roadmap.

The second element, communication, is one of the best ways to ensure employees understand cybersecurity policies and practices. It is important to communicate cybersecurity policies and practices to employees in a way that is easy to understand and follow. In this regard, effective leadership is needed to help overcome

communication difficulties. Therefore, leaders should not ignore the importance of communication skills to increase their followers' participation in the culture.

Third, once security risks are identified, it is important to raise awareness about them throughout the organization. It's about ensuring employees are informed about the importance of protecting data and understand what they can do. Employees can be made aware of issues such as password management, phishing scams and social engineering attacks through security awareness programs. Survey studies can be used to determine the level of cybersecurity awareness. This can help gauge how well employees understand and follow safety protocols. Additionally, the number of cyber incidents occurring within the organization can also be tracked. By tracking these trends, one can understand whether awareness efforts positively impact overall security.

Fourth, once employees understand the risks of cybersecurity, they can be trained to handle these risks appropriately. Organizations can use a variety of cybersecurity training tools to train their employees, including virtual training programs, internal training programs, or online training portals. The type of training depends on the needs of organizations and the level of cybersecurity training employees require. Advanced training is only required for specialized roles such as cybersecurity engineers, security analysts and network architects. However, almost every employee needs to receive basic, general cybersecurity training.

For future research, it is crucial not only to make cybersecurity culture conceptually understandable but also to make it measurable and manageable so that it can be better understood how the security level that includes the human element will have practical functionality and reduce human risk in organizations. Additionally, cybersecurity has been found to extend beyond organizational boundaries and existing literature still needs to address this aspect. Future research on organizational cybersecurity culture will address this in more detail and further investigate the potential impact of factors external to the business on organizational cybersecurity culture and practices.

REFERENCES

Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding and measuring information security culture. Proceedings of the Pacific Asia Conference on Information Systems PACIS içinde, 144.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003

Astakhova, L. V. (2014). The concept of the information-security culture. *Scientific and Technical Information Processing*, 41, 1, 22-28.

Berman, S. J., & Bell, R. (2011). Digital transformation: Creating new business models where digital meets physical. *IBM Institute for Business Value, 17*(3), 1-17.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly, 37*(2), 471-482.

Burrell, N. N. (2021). Cybersecurity leadership from a talent management organizational development lens. (Unpublished Exegesis). Capitol Technology University, Maryland, USA.

Cameron, K. S., & Quinn, R. E. (2006). Diagnosing and changing organizational culture: Based on the competing values framework. *John Wiley & Sons*.

Carpenter, P. & Roer, K. (2022). The Security Culture Playbook: An Executive Guide To Reducing Risk and Developing Your Human Defense Layer. Wiley, New Jersey, US.

Comptia (2018). Building a culture of cybersecurity: A guide for corporate executives and board members, Comptia White Paper, Erişim Tarihi: 13.01.2023, Erişim Adresi: https://comptiacdn.azureedge.net/webcontent/docs/default-source/research-reports/04917-ccab-whitepaper-online7a673748134243a5a75fe5369914dea0.pdf?sfvrsn=8c25744d_0

Corradini, I. (2020). Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology. *Springer Nature*, Berlin/Heidelberg, Germany.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, 92, 101713.

Dawson, J. & Thompson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Front. Psychol.*, 9, 744.

Deloitte (2023). Global future of cyber survey, Deloitte Global, Erişim adresi: https://www2.deloitte.com/content/dam/Deloitte/at/Documents/presse/at-deloitte-global-future-of-cyber-survey-2023.pdf

Denison, D. R., Nieminen, L. R., & Kotrba, L. (2020). Diagnosing organizational cultures: A conceptual and empirical review of culture effectiveness surveys. *European Journal of Work and Organizational Psychology*, *29*(1), 1-22.

Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2013). Embracing digital technology: A new strategic imperative. *MIT Sloan Management Review*, *55*(2), 1-12.

Gibson, C. B., & Gibbs, J. L. (2006). Unpacking the concept of virtuality: The effects of geographic dispersion, electronic dependence, dynamic structure, and national diversity on team innovation. *Administrative Science Quarterly*, *51*(3), 451-495.

Glaspie, H. W. & Karwowski, W. (2018). Human Factors in Information Security Culture: A Literature Review. In: Nicholson, D. (eds) Advances in Human Factors in Cybersecurity. AHFE 2017. Advances in Intelligent Systems and Computing, vol 593. Springer.

Glynn, M. A., Giorgi, S. & Lockwood, C. (2013). Organization culture. Obo in Management. doi: 10.1093/obo/9780199846740-0059

Hofstede, G. (1991). Cultures and organizations: Software of the mind. *McGraw-Hill*.

Hofstede, G. (2011). Dimensionalizing Cultures: The Hofstede Model in Context. Online Readings in Psychology and Culture, 2(1). https://doi.org/10.9707/2307-0919.1014

Huang, K. & Pearlson, K.E. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. 52nd Hawaii International Conference on System Sciences.

IBM, (2014). IBM security services 2014 cybersecurity intelligence index, IBM Global Technology Services, Erişim Tarihi: 15.01.2023, Erişim Adresi: https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

Kane, G. C., Palmer, D., Phillips, A. N., Kiron, D., & Buckley, N. (2015). Strategy, not technology, drives digital transformation. *MIT Sloan Management Review and Deloitte University Press*.

Kuusisto, R. & Kuusisto, T. (2013). Strategic communication for cyber-security leadership. *Journal of Information Warfare*, *12*(3), 41–48. https://www.jstor.org/stable/26486840

Lehto, M. & Limnell, J. (2020). Strategic leadership in cyber security, Case Finland. *Information Security Journal: A Global Perspective*, 30, 1-10. 10.1080/19393555.2020.1813851.

Linnenluecke, M. K., & Griffiths, A. (2010). Corporate sustainability and organizational culture. *Journal of World Business*, *45*(4), 357-366.

Martins, E. C. & Terblanche F. (2003). Building organizational culture that stimulates creativity and innovation. *European Journal of Innovation Management*, 6,1, 64-74.

Matveev, A.V. & Nelson, P. E. (2004). Cross cultural communication competence and multicultural team performance. *International Journal of Cross Cultural Management*, 4, 2, 253-270.

Merriam-Webster (2023). Cybersecurity. Merriam-Webster.com Dictionary. Erişim Adresi: https://www.merriam-webster.com/dictionary/cybersecurity

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia Soc. Behav. Sci.*, 147, 424–428.

National Institute of Standards and Technology (NIST) (2018). Framework for improving critical infrastructure cybersecurity, National Institute of Standards and Technology (NIST), Version 1.1, Erişim Adresi: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

Nel, F. ve Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security*, 27(2), 146-164.

NIST (2013). Glossary of Key Information Security Terms, NISTIR 7298 Rev.2., Erişim Adresi: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. Holistica–Journal of Business and Public Administration, 9(3), 71-88.

Parenty, T. J. & Domet, J. J. (2019). A leader's guide to cybersecurity: Why boards need to lead—and how to do, *Harvard Business Review*, Press: Boston, MA, USA.

Pettigrew, A. M. (1979). On studying organizational cultures. *Administrative Science Quarterly*, 24(4), 570–581, https://doi.org/10.2307/2392363.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cogn. Technol. Work*, 24, 371–390.

Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. 29th European Safety and Reliability Conference, October. doi: 10.3850/978-981-11-2724-3

Reid, R. & Van Niekerk, J., (2014). From information security to cyber security cultures organizations to societies. *Inf. Secur. South Africa (ISSA)*, IEEE, 1-7.

Roer, K., Petrič, G., Eriksen, A. C., Paglia, J., Ulimoen, T., Huisman, J., Smothers, R. L., & Carpenter, P. (2022). The security culture report, KnowBe4 Research, Erişim Tarihi: 20.01.2023, Erişim Adresi: https://www.knowbe4.com/organizational-cyber-security-culture-research-report#focus-form

Rotherberger, K. E. (2016). A quantitative study of perceptions about leadership competencies of IT project managers. Ph.D. Thesis, Cappella University, Minneapolis, MN, USA.

Sandhu, J. S. (2021). Cybersecurity for executives: Advancing leaders to practical cyber risk management, Notion Press, Tamil Nadu, India.

Schein, E. H. (1985). Organizational culture and leadership. *Jossey-Bass.*

Schultz, E. (2005). The human factor in security. *Comput. Sec.*, 24, 425–426.

Schwartz, R. B., & Murnane, R. J. (2018). The digital transformation of education: Connecting schools with the changing world. *Penguin*.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31-41. https://doi.org/10.1108/09685220010371394

Triplett, W. (2021). Establishing a cybersecurity culture organization. *Acta Scientific Computer Sciences*, 3, 8, 44-49.

Triplett, W.J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, 2, 573–586. https://doi.org/10.3390/jcp2030029

Uchendu, B., Nurse, J.R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computer Security*, 9, 109.

Verma, S., & Bhattacharyya, S. S. (2017). Perceiving organizational culture for digital transformation: A cybernetic study. *Vikalpa, 42*(4), 220-233.

Von Solms (2010). The 5 waves of information security – from kristian beckman to the present, in Rannenberg, K, Varadhajaran, V and Weber, C. (Eds.) SEC2010, IFIP Advances in Information and Communication Technology, Vol 330, pp 1-8.

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Ware, W. H. (1970). Security controls for computer systems. Technical report, Rand Corp Santa Monica, CA, USA.

Westerman, G., Calméjane, C., Bonnet, D., Ferraris, P., & McAfee, A. (2014). Digital transformation: A roadmap for billion-dollar organizations. *MIT Center for Digital Business*.

Wiegmann, D.A., Zhang, H., von Thaden, T., Sharma, G., & Mitchell, A. (2002). Safety culture: A review. Technical Report ARL-02-3/FAA-02-2. Illinois: Aviation Research Lab, Institute of Aviation.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security*, 88, 101640. https://doi.org/10.1016/j.cose.2019.101640

World Economic Forum (2023). Global Cybersecurity Outlook 2023, Insight Report, Erişim Adresi: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

Hakem Değerlendirmesi: Dış bağımsız.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

Teşekkür: -

Peer-review: Externally peer-reviewed.

Conflict of Interest: The author has no conflict of interest to declare.

Grant Support: The author declared that this study has received no financial support.

Acknowledgement: -