 https://doi.org/10.57017/jorit.v2.2(4).05

The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture

Michael Mncedisi WILLIE ✉ ✉
Council for Medical Schemes
Policy Research and Monitoring, Pretoria, South Africa

Abstract

In today's digital age, organizations have harnessed unprecedented connectivity and technological advancements, leading to enhanced efficiency and productivity. However, this progress has also exposed businesses to a multitude of cyber threats, including data breaches, ransomware attacks, and social engineering exploits. This research explores the relationship between organizational culture and cybersecurity practices, emphasizing the importance of fostering a security-first culture within organizations. While technical measures are crucial, neglecting the role of organizational culture can hinder effective cybersecurity.

The study is grounded in the theory of planned behaviour and the cultural dimensions theory, providing a solid theoretical foundation. Moreover, the investigation delves into the Denison organizational culture model, particularly focusing on the role of participation in nurturing a security-first culture. This becomes particularly relevant when assembling collaborative, inclusive, and communication-driven multi-disciplinary teams. Leadership emerges as a pivotal aspect in establishing a security-first culture. The onus lies with executive leadership at the highest echelons of the organization. However, it is concerning that in certain well-established companies, some senior executives continue to perceive cybersecurity as the sole responsibility of the IT department, overlooking its leadership significance.

Keywords: organizational culture; cybersecurity; security-first culture; employee behaviour; leadership practices.
JEL Classification: I32; O32; M14; M15; G32.

Introduction

During the digital era, organizations encounter a growing risk of cyber-attacks, prompting them to adopt heightened vigilance to safeguard their assets. Alawida et al. (2022) conducted an in-depth investigation into cybersecurity challenges during the Covid-19 pandemic. The study revealed that hacking attacks were the most common cyber-attack technique, followed by spam emails (Alawida et al., 2022). It is widely recognized that COVID-19 has accelerated the adoption of technology, making it an integral part of daily life and organizational operations as more companies embrace remote working (Amankwah-Amoah et al., 2021, Battisti, Alfiero and Leonidou, 2022). As technology advances, so do the methods employed by malicious actors, making it crucial for organizations to prioritize cybersecurity (McKinsey & Company, 2020; Pranggono and Arabo, 2021). While technology and processes play a significant role in protecting against cyber threats, the role of organizational culture in cybersecurity is equally important (Everard, 2008; Michael, 2008; Ismail, 2017; Maalem et al., 2020).

The role of organizational culture in cybersecurity is well documented however has gained even more popularity in recent years due to the escalating threat landscape (Ismail, 2017; Maalem et al., 2020). Organizations now acknowledge and embrace the fact that relying solely on technology is insufficient to safeguard against cyber-attacks. They are increasingly adopting proactive and up-to-date processes to effectively prevent and mitigate cyber threats (Everard, 2008; Michael, 2008; Ismail, 2017; Maalem et al., 2020). The necessity of cultivating a security-first culture arises to prevent and efficiently mitigate cybersecurity risks, which can significantly impact organizations (McKinsey & Company 2020; Pranggono and Arabo, 2021; Samurai, 2023). To achieve cyber security in current populations and to assure continuity in future populations, Reid, van Niekerk (2014) argue that a " self-renewing " belief that influences behaviour is required. In addition, the authors argued that this need is satisfied by nurturing an information security culture (ISC).

The digital age has brought about unprecedented connectivity and technological advancements, enabling organizations to operate more efficiently and effectively (De', Pandey, 2020; Economic Commission for Latin America and the Caribbean (ECLAC), 2021; Haleem, Javaid, Qadri et al., 2022). It has also exposed them to a variety of cyber threats, such as data intrusions, ransomware attacks, and social engineering exploits (Samurai, 2023; Chigada and Madzinga, 2021; Li and Liu, 2021; Alawida et al., 2022). These threats not only compromise sensitive information but also disrupt business operations, erode customer trust, and incur substantial financial and reputational damage (Alawida et al, 2022). While organizations have traditionally focused on implementing technical measures such as firewalls, antivirus software, and intrusion detection systems, they are increasingly realizing that a comprehensive approach to cybersecurity requires addressing human factors as well (Pollini et al., 2022; Nifakos et al., 2021; Tariq et al., 2023; Jang-Jaccard and Nepal, 2014; Perwej et al. 2021).

Critical is the impact of organizational culture on employee attitudes, behaviours, and cybersecurity awareness. Building a security-first culture involves creating an environment where cybersecurity is prioritized, understood, and integrated into the fabric of daily operations (Corriss, 2010; Hassandoust and Johnston, 2023). It requires a collective commitment from leadership, employees, and all stakeholders to embrace and champion cybersecurity principles (Corriss, 2010; Hassandoust, and Johnston, 2023; Rathod, 2023).

1. Background Research

The increasing threat of cyber-attacks in today's digital age has highlighted the need for organizations to prioritize cybersecurity (Alawida et al., 2022). While technological advancements and security measures play crucial roles in safeguarding against cyber threats, the role of organizational culture in cybersecurity practices has gained recognition (Li and Liu, 2021; Corriss, 2010; Hassandoust and Johnston, 2023; Rathod, 2023).

However, there is a lack of comprehensive understanding regarding the influence of organizational culture on building a security-first culture within organizations (Chia, Maynard and Ruighaver, 2002). The problem at hand is the limited understanding of how organizational culture shapes cybersecurity practices and the strategies needed to foster a security-first culture (Chia, Maynard and Ruighaver, 2002; Reegård, Blackett and Katta, 2019). Existing research fails to provide a comprehensive framework that addresses the multifaceted aspects of organizational culture and its impact on cybersecurity (da Veiga et al., 2020; Cano, 2021; Hassandoust and Johnston, 2023). This knowledge gap hinders organizations from effectively developing and implementing a security-first culture, leaving them vulnerable to cyber-attacks and information breaches (Cano, 2021; Hassandoust and Johnston, 2023).

Additionally, while there is a consensus on the importance of leadership commitment in cybersecurity, there is a lack of research exploring the specific role of middle management in shaping cybersecurity culture (Cano, 2021; Hassandoust and Johnston, 2023). Middle managers play a crucial role in translating organizational objectives into actionable strategies and shaping employee conduct (Cano, 2021). Without a clear understanding of their role and effective strategies to engage them, organizations may struggle to cultivate a security-first culture throughout all levels of the organization (Cano, 2021; Hassandoust and Johnston, 2023). Furthermore, the limited research on the long-term sustainability and resilience of a security-first culture poses a significant challenge (de Bruijn and Janssen, 2017; Cano, 2021; Hassandoust and Johnston, 2023).

2. Research Methods

This study sought to examine the impact of organizational culture on cybersecurity and delve into the establishment of a security-first culture within organizations. The primary objective of this research is to investigate the correlation between organizational culture and cybersecurity practices within these entities.

To address the problem statement regarding the role of organizational culture in cybersecurity and building a security-first culture, a comprehensive literature review was conducted. The literature review served as a valuable research method to explore existing theories, models, and empirical studies related to organizational culture and its impact on cybersecurity practices (de Bruijn and Janssen, 2017; Cano, 2021; Hassandoust and Johnston, 2023). A systematic approach was employed to identify relevant literature sources. Comprehensive searches were conducted in academic databases, such as IEEE Xplore, ACM Digital Library, Scopus, and Google Scholar, using keywords and combinations related to organizational culture, cybersecurity, security-first culture, and related concepts (Cremer et al., 2022; Rohan et al., 2023). The search strategy included a combination of controlled vocabulary terms (e.g., subject headings) and free-text keywords.

3. Theoretical Framework and Concepts

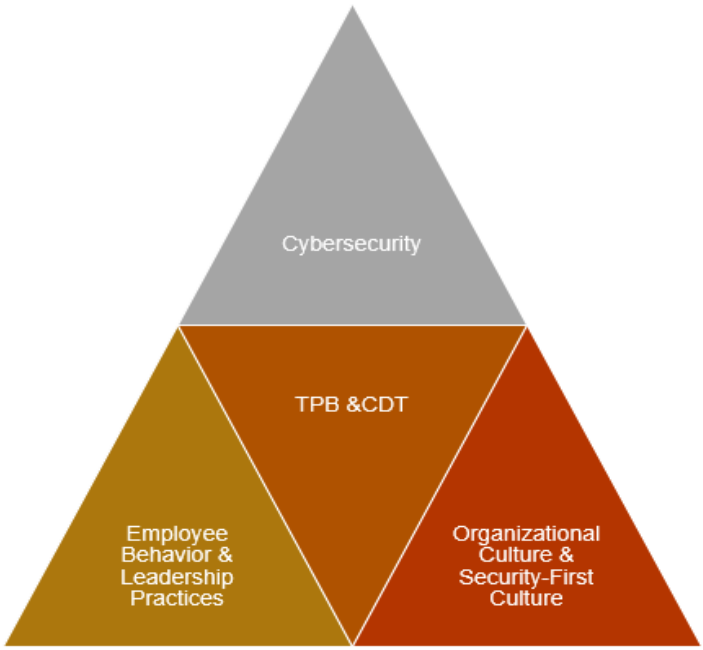
This research is underpinned by two key theories, namely the Theory of Planned behaviour (TPB) and Cultural Dimensions Theory (CDT), which provide a theoretical framework for understanding the dynamics of cybersecurity within organizations. The TPB posits that individual behavioural intentions are one of three theories widely promoted or considered by many scholars in relation to information security matters (Ong and Chong, 2014; Jalali et al., 2020; Maalem et al., 2020). The TPB suggests that employees' intentions to adhere to secure practices are shaped by their attitudes toward cybersecurity, the social norms prevailing within the organization regarding cybersecurity, and their perception of the ease or difficulty of implementing secure behaviours (Onumo, Awan and Cullen, 2021).

Understanding compliance behaviour becomes essential for organizations seeking to improve their information security through their human capital (Bulgurcu, Cavusoglu and Benbasat, 2010; Safa et al., 2015). Recognizing that employees who adhere to the organization's information security rules and regulations play a crucial role in bolstering security (Safa et al., 2015). According to Safa et al. (2015), the significance of information security extends to both private and business aspects. Experts assert that relying solely on technology cannot ensure a completely secure environment for information. They emphasize the crucial role of users' behaviour as a significant factor in this context (Kando et al., 2021),

While the TPB primarily focuses on the behavioural patterns of employees and staff, the CDT, on the other hand, delves into how cultural values and norms influence individuals' behaviour within organizations. Cultural Dimensions Theory highlights dimensions such as power distance, individualism versus collectivism, and uncertainty avoidance, which vary across different cultures and can significantly influence cybersecurity practices (Alowais et al., 2022). According to Hofstede's five cultural dimensions, power distance demonstrated a significant negative association and individualism vs. collectivism displayed a significant positive relationship (Hofstede, 2011; Alshahrani, 2017). Collectivistic cultures emphasize the interdependence of individuals within groups such as families, tribes, and countries, fostering mutual obligations. Conversely, individualistic cultures emphasize the independence of individuals from one another (Alshahrani, 2017).

Understanding the cultural dimensions at play within an organization enables the tailoring of cybersecurity strategies to align with the prevailing cultural context, facilitating better acceptance and adoption of secure practices (European Union Agency for Network and Information Security (ENISA), 2017); Uchendu et al., 2021; Schoenmakers et al., 2023). In organizations with a high-power distance, employees may be more hesitant to report security incidents or vulnerabilities to higher-ups, potentially hindering timely response and resolution (Morrison, 2014). Organizations that foster positive attitudes and culture change toward cybersecurity through security awareness training and emphasizing the significance of secure practices ultimately lead to a proactive and resilient approach to safeguarding digital assets (ENISA, 2017; Akter et al., 2022). The Figure 1 below depicts two theories that this study is centred on, and the clarification of concepts used.

Figure 1. Theoretical and conceptual framework



Source: Author own construction

The interplay between Organizational Culture and Cybersecurity, particularly the importance of cultivating a security-first culture, is directly influenced by employee behaviour and leadership practices (ENISA, 2017). A security-first culture refers to an organizational environment where cybersecurity is deeply ingrained in the mindset and actions of all employees, from top leadership to frontline staff (ENISA, 2017; Uchendu et al., 2021; Schoenmakers et al., 2023). This cultural shift involves fostering a strong sense of responsibility and awareness regarding cybersecurity practices, emphasizing the protection of sensitive data and the proactive identification and mitigation of potential threats (Akter et al., 2022).

Employee behaviour plays a critical role in the effectiveness of cybersecurity measures within an organization (Kando et al., 2021; Moustafa, Bello and Maurushat, 2021). A Security-First Culture encourages employees to adopt best practices and adhere to cybersecurity protocols, reducing the likelihood of human errors and minimizing the risks associated with cyber threats (Li and Liu, 2021; Kando et al., 2021).

3.1. Organizational Culture in Cybersecurity

Organizational culture refers to the shared values, beliefs, and behaviours that shape an organization's collective mindset (Schein, 2004). It encompasses the attitudes, awareness, and actions of employees regarding security practices (de Bruijn and Janssen, 2017; Akter et al., 2022; Rathod, 2023; Rohan et al., 2023). Research shows that a positive cybersecurity culture significantly reduces the likelihood of successful cyber-attacks (Herath and Rao, 2009). Organizational culture refers to the shared values, beliefs, norms, and behaviours that define an organization's identity and regulate its members' actions (Cano, 2021; Hassandoust and Johnston, 2023). Several researchers have emphasized the influence of organizational culture on cybersecurity practices (Cano, 2021; Hassandoust and Johnston, 2023).

Organizational culture shapes employees' attitudes and behaviours toward security, influencing their adherence to security policies and procedures (Karlsson et al., 2022). This highlights the significance of a security-oriented culture in promoting cybersecurity practices within an organization (Cano, 2021; Hassandoust and Johnston, 2023). Moreover, organizational culture influences employees' perceptions of cybersecurity. Research of D'Arcy and Greene (2014) demonstrates that a strong organizational culture emphasizing the importance of security fosters positive attitudes and perceptions toward cybersecurity. When employees perceive cybersecurity as a critical aspect of the organizational culture, they are more likely to comply with security protocols and assume a heightened sense of responsibility for safeguarding organizational assets (Cano, 2021; Hassandoust and Johnston, 2023).

3.2. Leadership Influence

Leadership is instrumental in establishing and promoting a security-first culture within an organization (de Bruijn and Janssen, 2017). The behavior, actions, and priorities demonstrated by leaders significantly influence cybersecurity practices (Ubowska and Królikowski, 2022). When leaders actively participate in security initiatives, communicate the importance of cybersecurity, and allocate resources to support security measures, they set an example for employees to follow (Khando et al., 2021). Strong leadership commitment fosters a culture where security is integrated into strategic decision-making processes and becomes a shared organizational goal (Cano, 2021; Hassandoust and Johnston, 2023).

Leadership and management are key drivers in shaping organizational culture and, consequently, cybersecurity practices. Leadership commitment is vital in fostering a security-first culture by prioritizing cybersecurity, allocating resources, and leading by example. This sends a clear message to employees about the significance of cybersecurity. Additionally, middle managers also play a critical role in shaping cybersecurity culture (de Bruijn and Janssen, 2017; Cano, 2021; Hassandoust and Johnston, 2023). They act as intermediaries between senior leadership and frontline employees, translating organizational goals into actionable cybersecurity strategies and engaging employees at all levels (Govender and Bussin, 2020). Their active involvement significantly impacts the integration of cybersecurity practices within the organization (Govender and Bussin, 2020; Haney and Lutters, 2020; Li and Liu, 2021).

3.3. Employee Behaviour and Practices

The role of organizational culture in cybersecurity is paramount, as building a security-first culture empowers employees, enhances their awareness, and promotes a proactive approach to cybersecurity (de Bruijn and Janssen, 2017; Cano, 2021; Nifakos et al., 2021; Akter et al., 2022; Hassandoust and Johnston, 2023). Organizational culture significantly influences employee behaviour and practices regarding cybersecurity (Cano, 2021; Hassandoust and Johnston, 2023). A culture that encourages open communication, knowledge sharing, and collaboration regarding cybersecurity fosters collective responsibility for protecting the organization's assets (de Bruijn and Janssen, 2017; Cano, 2021; Hassandoust and Johnston, 2023). Employees feel empowered to contribute to cybersecurity efforts by promptly reporting security incidents, participating in training programs, and adhering to security practices both inside and outside the workplace (Li and Liu, 2021). In contrast, a culture that lacks trust, accountability, or awareness regarding cybersecurity may result in risky behaviour, such as sharing passwords for accessing sensitive information on unsecured devices, and even sharing confidential information.

3.4. Organizational Learning and Adaptability

Organizational culture impacts the ability of an organization to learn from cybersecurity incidents, adapt to emerging threats, and continuously improve security practices. A culture that values learning, and adaptability encourages post-incident analysis, knowledge sharing, and the implementation of corrective measures to prevent future incidents (Cano, 2021; Hassandoust and Johnston, 2023). It encourages employees to report near-misses, share lessons learned, and contribute to the organization's collective knowledge. In contrast, a culture that avoids accountability or views cybersecurity incidents as isolated events inhibits organizational learning and hinders the development of effective security practices. Building a security-first culture requires organizational change and adaptation to evolving cyber threats de (Bruijn and Janssen, 2017; Cano, 2021; Hassandoust and Johnston, 2023). Li et al. (2016) suggest the promotion of a culture that encourages knowledge sharing among employees to enhance cybersecurity knowledge and awareness. A culture that encourages experimentation, innovation, and a proactive approach to security enhances an organization's resilience against cyber threats (Cano, 2021; Hassandoust and Johnston, 2023).

3.5. Encouraging Accountability, Collaboration, and Communication

A security-first culture instils a sense of responsibility among employees, encouraging them to take proactive measures in identifying and reporting security incidents (de Bruijn and Janssen, 2017; Cano, 2021; Hassandoust and Johnston, 2023). It empowers employees to protect the organization's assets, including sensitive data and digital infrastructure. Organizations can cultivate a cybersecurity-centric environment throughout their operations by allocating resources to training, promoting accountability, fostering collaboration, and setting a leading example (IEA, 2021). This comprehensive approach helps mitigate the risks associated with cyber threats and bolsters overall resilience. Notably, accountability plays a critical role in reducing the likelihood of insider threats (IEA, 2021). Fostering a security-first culture facilitates open communication and collaboration among different departments and stakeholders (de Bruijn and Janssen, 2017; Cano, 2021; Hassandoust and Johnston, 2023). This facilitates the exchange of information about potential vulnerabilities and emerging threats, leading to a proactive response. Collaborative efforts may involve cross-functional teams such as information technology, legal, and human resources, who work together to develop effective cybersecurity policies and procedures (Van der Kleij, Kleinhuis and Young, 2017), see one for core and non-core members of a CSC working group (Alvarez-Dionisi, 2019). Involvement in organization culture is also covered extensively in the Denison Organizational Culture Model and considered dimensions such as involvement in fostering a security-first culture (Denison, 1984).

Organizational culture significantly influences cybersecurity practices within an organization. The values, beliefs, norms, and behaviours that shape the culture have a profound impact on how cybersecurity is perceived, prioritized, and integrated into daily operations (Cano, 2021; Hassandoust and Johnston, 2023). Edgar Schein's model of organizational culture provides a valuable framework for understanding the layers of culture within an organization (Schein, 2004). This model further depicts the Artifacts and behaviours within the organization and is very clear on the visible aspects of culture, while espoused values are the stated beliefs and norms (Schein, 2004). Recognizing the influence of organizational culture on cybersecurity practices is vital for organizations aiming to cultivate a security-first culture (de Bruijn and Janssen, 2017; Cano, 2021; Hassandoust and Johnston, 2023). Establishing inclusive structures within the organization that emphasize collaboration and hold everyone accountable is essential (Shore et al. 2018). Employees should recognize the value they contribute within these structures. Furthermore, it is important to consider the inclusion of non-core members in the working group, including individuals from external organizations or institutions who have a vested interest in the group's efforts, as well as expert consultants who offer valuable guidance and support (Kozlowski and Ilgen, 2006). Their involvement can bring fresh and independent perspectives and provide assessments from outside the organization.

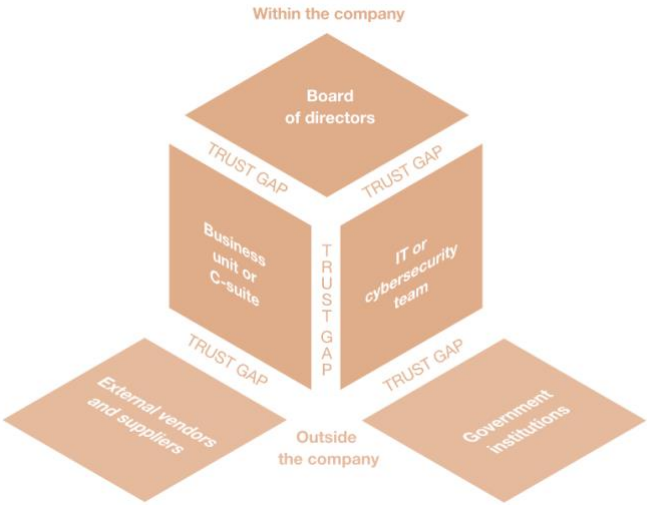
Figure 2. Core and non-core members of a CSC working group

Source adapted from Alvarez-Dionisi (2019)

Moreover, one aspect that requires further exploration is the implementation of a security-first culture within a multi-party business model where certain functions are outsourced to third parties (de Bruijn and Janssen, 2017; Cano, 2021; Hassandoust and Johnston, 2023). This scenario presents unique challenges and considerations that should be thoroughly examined to ensure the effectiveness of cybersecurity practices and the alignment of a security culture across all involved parties (Cano, 2021; Hassandoust and Johnston, 2023).

Figure 3 below depicts cyber security trust gaps that can exist at many levels across the corporate ecosystem by McKinsey & Company cited in (Choi, Kaplan and Lung, 2017) who also highlight the importance of factoring external vendors and suppliers. Trust gaps in the organization could result in power dimensions that may exist between leadership and employees, in some instances third parties. Da Veiga, Astakhova, Botha, et al (2020) emphasize the importance of establishing a trusting relationship between management and employees to achieve high compliance with security policies and foster a strong commitment to information security.

Figure 3. Cybersecurity trust gaps can exist on many levels across the corporate ecosystem



Source: adapted from Choi, Kaplan and Lung (2017), McKinsey & Company (2020)

One of the most prominent models that aim to bridge the trust gap in the organization is the Cultural Dimensions Theory (CDT), which is utilized to comprehend organizational cultures (Hofstede, 2011). It encompasses dimensions such as power distance and individualism vs. collectivism, making it a proposed model for promoting workplace harmony in a multicultural business environment (Cortina, Arel, and Smith-Darden, 2017). Some critics however still maintain that Geert Hofstede's CDT model can't be effectively implemented in the era of rapidly changing environment, convergence, and globalization and the model does not account for third-party models and unprecedented events such as COVID-19 (Shaiq et al., 2011).

Organizational culture plays a crucial role in cybersecurity practices, even in outsourced models where certain functions are delegated to third parties (Cano, 2021; Hassandoust and Johnston, 2023). The Denison Organizational Culture Model and similar models become highly relevant as they assess an organization's performance across multiple dimensions, providing valuable insights into its culture, including the level of involvement in fostering a security-first culture (Denison, 1984; Metz, Ilieș and Nistor, 2020). In such models, it is essential to establish a strong culture of cybersecurity that extends beyond the boundaries of the organization to encompass all parties involved (Chia, Maynard and Ruighaver, 2002; Jang-Jaccard and Nepal, 2014; Battisti, Alfiero and Leonidou, 2022).

This is further supported by Wiley and McCormac (2020), who argue that organizations should focus on security culture rather than organizational culture to improve information security awareness (ISA), saving time and resources.

Table 1 below shows some of the parameters that are of key consideration in an outsourced model setting on enhancing security culture.

Table 1. Parameters that are of key consideration in an outsourced model setting

Shared Values and Expectations	The organization and the outsourced partners should share common values and expectations regarding cybersecurity. This includes a mutual understanding of the importance of security, compliance requirements, and the need for proactive risk management.
Clear Communication	Open and transparent communication channels should be established to facilitate the exchange of information related to cybersecurity. This includes sharing security policies, incident response procedures, and any relevant threat intelligence to ensure all parties are well-informed.
Collaboration and Coordination	Collaboration and coordination between the organization and outsourced partners are essential to address cybersecurity challenges effectively. This can involve joint training programs, periodic security assessments, and regular meetings to discuss security issues and updates.
Contractual Obligations	Contracts and service-level agreements (SLAs) should explicitly address cybersecurity responsibilities and expectations. The outsourced partners should adhere to the organization's cybersecurity policies and procedures, as well as comply with relevant industry regulations and standards.
Ongoing Monitoring and Auditing	Regular monitoring and auditing of the outsourced partners' cybersecurity practices should be conducted to ensure compliance and adherence to established security standards. This helps identify any potential vulnerabilities or gaps that need to be addressed promptly.
Continuous Improvement	A culture of continuous improvement should be fostered, encouraging all parties to regularly assess and enhance their cybersecurity measures. This can involve sharing best practices, and lessons learned from security incidents and implementing feedback mechanisms for ongoing improvement.

3.6. Attitudes and Awareness

Organizational culture greatly influences employee attitudes and awareness regarding cybersecurity (Hassandoust and Johnston, 2023; Rohan et al., 2023). A culture that values and prioritizes security creates an environment where employees recognize the importance of cybersecurity and their role in protecting the organization's digital assets (Akter et al., 2022). Such a culture fosters a sense of responsibility and vigilance among employees, making them more proactive in identifying and reporting potential security threats (Cano, 2021; Hassandoust and Johnston, 2023). On the other hand, a culture that downplays the significance of cybersecurity or lacks awareness regarding potential threats may result in a lackadaisical approach toward security measures (Akter et al., 2022; Hassandoust and Johnston, 2023; Rohan et al., 2023). A security-first culture also plays a crucial role in promoting security awareness and training programs (de Bruijn, Janssen, 2017; Akter et al., 2022; Hassandoust and Johnston, 2023; Rohan et al., 2023). Chang and Lin (2007), find that an organization's culture significantly influences the effectiveness of security training programs.

A culture that values continuous learning and knowledge sharing creates an environment conducive to effective cybersecurity training initiatives (Cano, 2021; Hassandoust and Johnston, 2023). This underscores the importance of embedding security awareness and training within the organizational culture to enhance cybersecurity practices (de Bruijn and Janssen, 2017; Akter et al., 2022; Hassandoust and Johnston, 2023; Rohan et al., 2023). Security leaders play a crucial role in implementing and enhancing training and awareness programs to improve security-related behaviour among users. While these programs cannot guarantee absolute security-related behaviours, they do contribute positively to the overall security posture (Blum, 2020).

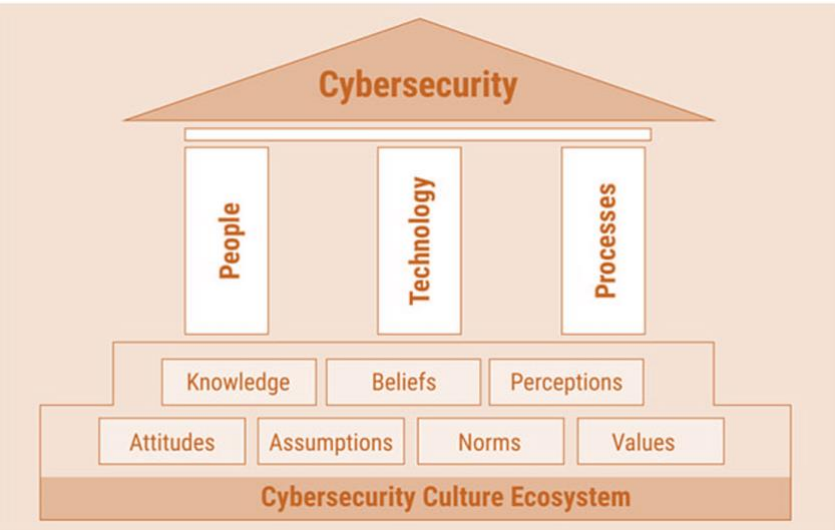
3.7. Compliance and Adherence

The influence of organizational culture on employee compliance with cybersecurity policies and procedures is crucial. A strong security-oriented culture reinforces the importance of following established security protocols and ensures consistent adherence to cybersecurity guidelines. When cybersecurity is deeply ingrained in the organizational culture, employees understand that adherence to security measures is not optional but necessary for protecting the organization's sensitive information. Conversely, a weak or inconsistent culture may lead to lax compliance, leaving vulnerabilities that can be exploited by cybercriminals (Cano, 2021; Hassandoust and Johnston, 2023). Handy's Four types of culture model become more applicable in ensuring compliance as it takes into consideration role culture, task culture, and person culture, especially in the context of cybersecurity (Handy, 1995; Cacciattolo, 2014) This model transfers the responsibility for cybersecurity to varying hierarchies within the organization, from the process level down to the individual level.

4. Evolving Cyber Security Culture Ecosystems and the Impact of Covid-19

The concept of cybersecurity culture ecosystem refers to the collective environment, practices, and mindsets concerning cybersecurity within a particular group or society (Cano, 2021; Hassandoust and Johnston, 2023). It encompasses various aspects that contribute to the development of a strong cybersecurity culture and the protection of digital systems, data, and infrastructure. Research on defining, evaluating, and enhancing cybersecurity culture, which comprises seven key elements: knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values depicted in Figure 4 (Alvarez-Dionisi, 2019), is limited (Cano, 2021; Hassandoust and Johnston, 2023). This presents an opportunity for scholars and professionals to conduct a focused study on cybersecurity culture (Cano, 2021; Hassandoust and Johnston, 2023).

Figure 4. Cybersecurity culture ecosystem



Source: adapted from op cit. ENISA and op cit Trim et al. cited in Alvarez-Dionisi (2019)

The COVID-19 pandemic has had a profound effect on the cybersecurity culture ecosystem, resulting in increased awareness, improved employee education, increased collaboration, and an increased emphasis on resilience and proactive cybersecurity measures (Everard, 2008, Cano, 2021; Hassandoust and Johnston, 2023). Organizations have come to acknowledge the vital significance of cybersecurity in facilitating digital operations and safeguarding sensitive data within a highly interconnected world (Akter et al., 2022). The risk remains elevated, particularly as most organizations have embraced remote work as a permanent and preferred practice (Adekoya, Adisa, Aiyenitaju, 2022; Vyas, 2022). Webinars and virtual meetings continue to be hosted by organizations,

allowing employees to connect and collaborate remotely. Table 2 below depicts some of the areas that emerged during Covid-19.

Table 2. Key of cyber security that emerged during the pandemic

Factor/ Attribute	Description
Accelerated Digital Transformation	The pandemic hastened the rate of digital transformation in numerous industries. The accelerated adoption of new technologies and digital tools to facilitate remote work, online collaboration, and digital services by organizations. This accelerated digital transformation increased the attack surface for cybercriminals, necessitating a more robust cybersecurity culture to safeguard the expanded digital ecosystem.
Increased Cyber Threats	As organizations transitioned swiftly to remote work, the pandemic created a perfect storm for cybercriminals. This abrupt change led to an increase in cyber hazards such as phishing, malware, ransomware, and social engineering. Fear and uncertainty surrounding the pandemic were utilized by cybercriminals to initiate targeted attacks.
Heightened Awareness	Individuals and organizations are now more aware of the importance of cybersecurity as a result of the pandemic. As more people work remotely and rely on digital technologies for communication and collaboration, the need for strong cybersecurity practices and awareness of potential threats has become more apparent.
Remote Work Challenges	During the pandemic, the widespread adoption of remote work presented organizations with new challenges in terms of securing remote access, safeguarding sensitive data, and maintaining secure communication channels. Cybersecurity teams were required to rapidly adapt to the changing environment and implement additional security measures to mitigate the risks posed by remote work.
Emphasis on Employee Education	As cyber threats increased, businesses realized the importance of educating employees on cybersecurity best practices. Numerous organizations provided their employees with training and awareness programs so they could identify and respond to potential hazards. This has increased the emphasis on cybersecurity education and awareness among the workforce.
Increased Collaboration	The pandemic highlighted the need for collaboration and information sharing among cybersecurity professionals and organizations. Cybersecurity communities, both public and private, played a crucial role in sharing threat intelligence, best practices, and mitigation strategies to counter the evolving cyber threats related to the pandemic. This collaborative approach is likely to continue in the post-pandemic cybersecurity ecosystem.
Focus on Resilience	The pandemic exposed vulnerabilities in existing cybersecurity infrastructure and strategies. Organizations realized the importance of building resilient cybersecurity systems that can withstand unexpected disruptions. The focus has shifted towards proactive measures such as incident response planning, business continuity, and disaster recovery strategies to ensure that cybersecurity remains robust in the face of future crises.

5. Cyber Security Frameworks and Approaches Post-COVID

The lessons, processes, and tools developed to deal with cyber security during the pandemic are expected to be carried forward into the post-COVID world (Tasheva, 2021). The author emphasizes that, for many years, cybersecurity was considered a niche ICT issue. Nonetheless, this perception has changed considerably over time.

Organizations will certainly need to consider reinforcing their existing cybersecurity frameworks or adopting innovative strategies to further enhance their defences against cyber threats. These frameworks serve as essential guidelines and structures that enable organizations to systematically identify, assess, and mitigate cyber risks. They encompass a variety of recommended practices, controls, and procedures that aim to protect information

systems and sensitive data from potential threats. In the post-COVID era, Table 3 provides an overview of the main security measures that are fundamental to cybersecurity.

Table 3. Core measures that are key to cyber security post-COVID

Zero Trust Architecture	The Zero Trust model has gained prominence as a cybersecurity framework post-COVID. It assumes that no user or device should be trusted by default, even if they are within the organization's network perimeter. Zero Trust focuses on verifying and authenticating every user and device attempting to access resources, regardless of their location.
Cloud Security	As a result of the pandemic's rapid adoption of cloud services, organizations are concentrating on establishing robust cloud security frameworks. This involves instituting security controls, encrypting data, managing access permissions, and ensuring cloud environments have secure configurations. Additionally, cloud service providers play a vital role in providing secure infrastructure and services.
Secure Remote Access	As remote work continues to be prevalent, secure remote access has become a top priority. Organizations are implementing multi-factor authentication (MFA), virtual private networks (VPNs), and secure remote desktop protocols (RDPs) to ensure secure connections between employees and corporate networks.
Incident Response and Business Continuity	COVID-19 has emphasized the need for effective incident response and business continuity plans. Organizations are investing in robust response strategies, including identifying and mitigating threats, communicating effectively during incidents, and ensuring quick recovery and restoration of services.
Employee Awareness and Training	Cybersecurity awareness and training programs have become even more crucial in the post-COVID world. Organizations are focusing on educating employees about potential risks, phishing attacks, secure remote work practices, and data protection guidelines to mitigate human-related vulnerabilities.
AI and Machine Learning	Artificial intelligence (AI) and machine learning (ML) technologies are increasingly used to detect and respond to threats in real time in cybersecurity. These technologies are capable of analysing immense amounts of data, recognizing patterns, and assisting organizations in defending proactively against cyber threats that are constantly evolving.
Regulatory Compliance	In response to the changing nature of cyber threats, regulatory bodies have enacted or revised regulations. Organizations must remain current on these regulatory requirements, such as the General Data Protection Regulation, and ensure compliance to avoid legal and financial repercussions.
Supply Chain Security	COVID-19 highlighted global supply chain vulnerabilities. Organizations are instituting measures to ensure the security of their products, services, and data throughout the entire supply chain lifecycle.
Threat Intelligence Sharing	Collaboration and sharing of threat intelligence among organizations, sectors, and governments have become crucial in the post-COVID world. Information-sharing platforms and initiatives enable the rapid dissemination of actionable intelligence to detect and mitigate emerging threats effectively.
Privacy and Data Protection	The pandemic has raised concerns about privacy and data protection as organizations collect and process more personal data. Ensuring compliance with privacy regulations, implementing data protection measures, and being transparent about data practices are essential for maintaining customer trust.

6. Discussion

A company's cybersecurity practices are heavily influenced by its organizational culture. The shared values, beliefs, norms, and behaviours that define an organization's culture influence how cybersecurity is perceived, prioritized, and integrated into daily operations (Chang and Lin, 2007; de Bruijn and Janssen, 2017; Sharma and Aparicio, 2022). Connolly et al. (2016) suggest that organizations can create a cybersecurity-conscious environment by investing in training, promoting accountability, fostering collaboration, and setting a positive example for employees. This approach ensures that cybersecurity becomes an integral part of every aspect of the organization's operations.

This comprehensive approach enhances overall resilience and effectively mitigates the risks posed by cyber threats. The literature conducted revealed that a strong organizational culture that emphasizes the importance of security fosters positive attitudes and perceptions toward cybersecurity leading to increased compliance with security protocols and a heightened sense of responsibility for safeguarding organizational assets. The study also explored the Denison Organizational Culture Model, with a focus on involvement in fostering a security-first culture, which is especially relevant in building multi-disciplinary teams that are collaborative, inclusive, and promote effective communication. Furthermore, the literature emphasizes the essential role of leadership in creating a security-first culture. This begins at the highest level, with executive leadership taking the lead (Connolly et al., 2016). However, it is regrettable that even in well-established companies, some senior executives still perceive cybersecurity matters as solely the responsibility of the IT team, failing to recognize their significance as a leadership concern (Gilliland, 2023). The author strongly emphasizes the importance of leadership in fostering a security-first culture.

Dedicating resources, and leading by example in adhering to security practices, leaders effectively convey the importance of cybersecurity to their employees (de Bruijn and Janssen, 2017; Gilliland, 2023). Additionally, middle managers play a vital role in shaping the cybersecurity culture within an organization. According to the 2017 European Union Agency for Cybersecurity report (ENISA, 2017) middle managers have the power to translate organizational objectives into practical cybersecurity strategies and engage employees across all levels. Their role as intermediaries between senior leadership and frontline employees significantly impacts the integration of cybersecurity practices (Baham, 2021).

A culture of continuous improvement and adaptability is essential in addressing emerging cybersecurity challenges. There is a need for organizations to foster a culture that encourages experimentation, innovation, and a proactive approach to security. Such a culture enhances an organization's resilience against cyber threats. To build a security-first culture, organizations must address several challenges and gaps (Cano, 2021). Future research should focus on developing comprehensive frameworks that consider the multidimensional aspects of organizational culture and their specific impact on cybersecurity practices. Additionally, research should explore the long-term sustainability of a security-first culture and the challenges organizations face in maintaining it over time (Cano, 2021).

Conclusions

Organizational culture plays a crucial role in cybersecurity and establishing a security-first culture within organizations. Leadership Practices are instrumental in shaping the organizational culture and setting the tone for cybersecurity. Effective leaders prioritize cybersecurity as a strategic priority, invest in cybersecurity training and awareness programs, and lead by example to demonstrate the significance of safeguarding sensitive information. When leaders prioritize cybersecurity, allocate resources, and lead by example, it sends a clear message to employees about the significance of security.

Organizations should foster a culture that encourages experimentation, innovation, and a proactive approach to security. This enables them to effectively address emerging cybersecurity challenges and enhance their resilience against threats. While progress has been made in understanding the role of organizational culture in cybersecurity, there are still challenges and gaps that need to be addressed. The theoretical contribution of this study lies in its exploration of the role of Organizational Culture in Cybersecurity, centred around the TPB and CDT. While the TPB and CDT were the main focus, the literature review revealed the potential applicability of other theoretical models for assessing the establishment of a Security-First Culture within organizations.

Among the additional theoretical models identified are the Denison Organizational Culture Model, Handy's four types of culture model, and Geert Hofstede's model, which have been extensively covered in existing literature. However, their specific application and effectiveness in unique situations, such as during unprecedented events like the COVID-19 pandemic, remain relatively unexplored. This study emphasizes the importance of further research to assess the applicability and effectiveness of alternative theoretical models in various organizational contexts, especially during times of major disruptions.

Recommendations

This study further makes management and practical implications, first organizational culture plays a crucial role in cybersecurity and cultivating a security-first mindset. Leadership involvement is essential in achieving this goal. Senior leaders should demonstrate commitment by allocating resources, adhering to security practices, and making cybersecurity a strategic priority. Managers should also support cybersecurity efforts and communicate effectively with employees at all levels. Comprehensive security training and awareness programs that align with the organizational culture are recommended. Collaboration and knowledge sharing among employees, suppliers, and stakeholders is essential for fostering a collective security mindset. Long-term strategies and plans focused on preventive measures are vital to sustaining a security-first culture. Integration of cybersecurity practices into policies, procedures, and performance metrics, along with ongoing training and reinforcement, are necessary for the long-term success of the security culture.

Future research

Despite considerable advancements in comprehending the significance of organizational culture in cybersecurity, there are still numerous challenges and gaps that need to be addressed. Future research endeavours should concentrate on formulating comprehensive frameworks that encompass the multidimensional aspects of organizational culture and their specific influences on cybersecurity practices, especially when involving third parties, particularly those contracted for long-term engagements.

Ethical consideration

The study did not involve accessing or disclosing participants' personal or clinical data, nor did it directly involve the treatment of patients. The data were evaluated and reported only at an aggregated level to ensure privacy and confidentiality. Relevant sources were also acknowledged and cited accordingly.

Declaration of interests

The author states that there are no financial or personal affiliations that could have unduly influenced the content of this article.

References:

[1] Adekoya, O. D., Adisa, T.A., and Aiyenitaju, O. (2022). Going forward: Remote working in the post-COVID-19 era. *Employee Relations*, 44(6), 1410-1427. https://doi.org/10.1108/ER-04-2021-0161

[2] Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., and Hossain, M. A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research*, 2(1), 1-26. https://doi.org/10.1007/s10479-022-04844-8

[3] Alawida, M., Omolara, A. E., Abiodun, O. I., and Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University -Computer and Information Sciences*, 34(10), 8176-8206. https://doi.org/10.1016/j.jksuci.2022.08.003

[4] Alowais, S., Armeen, I., Sharma, P., and Johnston, A. (2022). Cyber hygiene practices across cultures: A cross cultural study of the US and Saudi Arabia based Information systems users. *Procedia Computer Science*, 219, 744–750. https://doi.org/10.7759/cureus.33211

[5] Alshahrani, A. (2017). Power distance and individualism-collectivism in EFL learning environment. *Arab World English Journal*, 8(2). https://dx.doi.org/10.24093

[6] Alvarez-Dionisi, L. E. (2019). *Implementing a cybersecurity culture*. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/implementing-a-cybersecurity-culture

[7] Amankwah-Amoah, J., Khan, Z., Wood, G., and Knight, G. (2021). COVID-19 and digitalization: The great acceleration. *Journal of Business Research*, 136, 602-611. https://doi.org/10.1016/j.jbusres.2021.08.011

[8] Baham, D. (2021). *The role of leaders in creating a cybersecurity culture*. https://insights.pecb.com/leaders-creating-cybersecurity-culture/

[9] Battisti, E., Alfiero, S., and Leonidou, E. (2022). Remote working and digital transformation during the COVID-19 pandemic: Economic–financial impacts and psychological drivers for employees. *Journal of Business Research*, 150, 38-50. https://doi.org/10.1016/j.jbusres.2022.06.010

[10] Blum, D. (2020). *Strengthen security culture through communications and awareness programs*. In: Rational Cybersecurity for Business. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-5952-8_4

[11] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548. https://doi.org/10.2307/25750690

[12] Cacciattolo, K. (2014). Understanding organisational cultures. *European Scientific Journal*, 2, 1–7. https://eujournal.org/index.php/esj/article/view/4782

[13] Cano, J. (2021). *Organizational culture for information security: A systemic perspective on the articulation of human, cultural, and social systems*. https://www.isaca.org//media/files/isacadp/project/isaca/articles/journal/2021/volume-3/organizational-culture-for-information-security_joa_eng_0621.pdf

[14] Chang, S. E., and Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, *107* (3), 438-458. https://doi.org/10.1108/02635570710734316

[15] Chia, P. A., Maynard, S. B., and Ruighaver, A. B. (2002). Understanding organizational security culture. *Pacis*, 1-23. https://people.eng.unimelb.edu.au/seanbm/research/PacisChiaRuighaverMaynard.pdf

[16] Chigada, J., and Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, 23(1), 1-11. https://dx.doi.org/10.4102/sajim.v23i1.1277

[17] Choi, J., Kaplan, J., and Lung, H. (2017). *A framework for improving cybersecurity discussions within the organization.* McKinsey.com. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/A%20framework%20for%20improving%20cybersecurity%20discussions%20within%20organizations/A-framework-for-improving-cybersecurity-discussions-within-organizations.pdf

[18] Connolly, L., Lang, M., Gathegi, J., and Tygar, J.D. (2016). *The effect of organizational culture on employee security behavior: A qualitative study.* In N. Clarke and S. Furnell (Eds.), 10th International Symposium on Human Aspects of Information Security and Assurance (HAISA), pp. 33-44. Frankfurt: Plymouth University.

[19] Corriss, L. (2010). *Information security governance: Integrating security into the organizational culture*. GTIP '10: Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies, ACM, 35–41. https://doi.org/10.1145/1920320.1920326

[20] Cortina, K. S., Arel, S., and Smith-Darden, P., J. (2017). School belonging in different cultures: The effects of individualism and power distance. *Frontiers in Education*, 2, 274387. https://doi.org/10.3389/feduc.2017.00056

[21] Cremer, F., Sheehan, B., Fortmann, M., et al. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Papers on Risk and Insurance Issues and Practice*, 47, 698–736. https://doi.org/10.1057/s41288-022-00266-6

[22] Da Veiga, L. V., Astakhova, A., Botha, A., and Herselman, M. (2020). Defining organisational information security culture - Perspectives from academia and industry. *Computers & Security*, *92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

[23] D'Arcy, J., and Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22* (5), 474-489. https://doi.org/10.1016/j.procs.2022.09.180

[24] De Bruijn, H., and Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

[25] De', R., Pandey, N., and Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, *55*, 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171

[26] Denison, D. R. (1984). Bringing corporate culture to the bottom line. *Organizational Dynamics*, 13(2), 4-22.10.1016/0090-2616(84)90015-9

[27] Everard, T. (2008). *What is cyber security culture and why does it matter for your organization?* https://www.paconsulting.com/insights/what-is-cyber-security-culture-and-why-does-it-matter-for-your-organisation

[28] Gilliland, A. (2023). *Building a security-first culture: The key to cyber success*. https://www.forbes.com/sites/forbestechcouncil/2023/01/03/building-a-security-first-culture-the-key-to-cyber-success/?sh=39a87c69a10f

[29] Govender, M., and Bussin, M. (2020). Performance management and employee engagement: A South African perspective. *SA Journal of Human Resource Management*, *18*, 19. https://doi.org/10.4102/sajhrm.v18i0.1215

[30] Haleem, A., Javaid, M., Qadri, M. A., and Suman, R. (2022). Understanding the role of digital technologies in education: A review. *Sustainable Operations and Computers*, 3, 275-285. https://doi.org/10.1016/j.susoc.2022.05.004

[31] Handy, C. (1995). *Gods of management, the changing work of organizations*. Oxford. Oxford University Press, 254 pp. ISBN: 0195096177, 978-0195096170

[32] Haney, J., and Lutters, W. (2020). Security awareness training for the workforce: Moving beyond "Check-the-Box" compliance. *Computer (Long Beach Calif),* 53(10). https://doi.org/10.1109/mc.2020.3001959

[33] Hassandoust, F., and Johnston, A. C. (2023). Peering through the lens of high-reliability theory: A competencies driven security culture model of high-reliability organizations. *Information Systems Journal*, 33(5), 1212–1238. https://doi.org/10.1111/isj.12441

[34] Herath, T., and Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, 18, 106-125. https://doi.org/10.1057/ejis.2009.6

[35] Hofstede, G. (2011). Dimensionalizing cultures: The Hofstede model in context. *Readings in Psychology and Culture*, 2(1). https://doi.org/10.9707/2307-0919.1014

[36] Ismail, N. (2017). *The importance of creating a cyber security culture*. https://www.information-age.com/importance-creating-cyber-security-culture-5399/

[37] Jalali, M. S., Bruckes, M., Westmattelmann, D., and Schewe, G. (2020). Why employees (Still) click on phishing links: An investigation in hospitals. *Journal of Medical Internet Research*, 22(1), e16775. https://doi.org/10.2196/16775

[38] Jang-Jaccard, J., and Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Science*s, 80(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

[39] Khando, K., Gao, S., Islam, S. M., and Salman, A. (2021). Enhancing employees' information security awareness in private and public organizations: A systematic literature review. *Computers & Security*, 106, 102267. https://doi.org/10.1016/j.cose.2021.102267

[40] Karlsson, M., Karlsson, F., Åström, J., and Denk, T. (2022). The effect of perceived organizational culture on employees' information security compliance. *Information and Computer Security*, 30(3), 382-401. https://doi.org/10.1108/ICS-06-2021-0073

[41] Kozlowski, W. J., and Ilgen, D. R. (2006). Enhancing the effectiveness of work groups and teams. *Psychological Science in the Public Interest*, 7(3). https://doi.org/10.1111/j.1529-1006.2006.00030.x

[42] Li, L., Xu, L., He, W., Chen, Y., and Chen, H. (2016). Cyber security awareness and its impact on employee behaviour. *International Conference on Research and Practical Issues of Enterprise Information Systems*, 103–111). Springer. https://inria.hal.science/hal-01630550/document

[43] Li, Y., and Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

[44] Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., and Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, 3(1), 1-18. https://doi.org/10.1186/s42400-020-00050-w

[45] Metz, D., Ilieș, L., Nistor, R. L. (2020). The impact of organizational culture on customer service effectiveness from a Sustainability Perspective. *Sustainability*, 12(15), 6240. https://doi.org/10.3390/su12156240

[46] Michael, K. (2008). *Social and organizational aspects of information security management*, IADIS e-Society, 9-12 April, Algarve, Portugal pp. 1–8 https://ro.uow.edu.au/cgi/viewcontent.cgi?article=1598&context=infopapers

[47] Morrison, E. W. (2014). Employee voice and silence. *Annual Review of Organizational Psychology and Organizational Behaviour*, *1*(1), 173-197. 10.1146/annurev-orgpsych-031413-091328

[48] Moustafa, A. A., Bello, A., and Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, 12, 561011. https://doi.org/10.3389/fpsyg.2021.561011.

[49] Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., and Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organizations: A systematic review. *Sensors (Basel),* 21(15), 5119. PMID: 34372354; PMCID: PMC8348467. https://doi.org/10.3390/s21155119

[50] Ong, L.-P., and Chong, C.-F. (2014). *Information security awareness: An application of psychological factors – A study in Malaysia.* In Proceedings of the 2014 International Conference on Computer, Communications, and Information Technology (pp. 98-101). Atlantis Press.

[51] Onumo, A., Awan, I. U., and Cullen, A. J. (2021). Assessing the moderating effect of security technologies on employees' compliance with cybersecurity control procedures. *ACM Transactions on Management Information Systems*, 12(2), 11. https://doi.org/10.1145/3424282

[52] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., and Jaiswal, A. K. (2021). A systematic literature review on cyber security. *International Journal of Scientific Research and Management*, 9(12), 669-710. https://doi.org/ff10.18535/ijsrm/v9i12.ec04ff final-03509116

[53] Pollini, A., Callari, T.C., Tedeschi, A. et al. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cogn Tech Work*, 24, 371–390. https://doi.org/10.1007/s10111-021-00683-y

[54] Rathod, N.N. (2023). *Building a cybersecurity culture: Strategies for awareness and training*. https://www.socinvestigation.com/building-a-cybersecurity-culture-strategies-for-awareness-and-training/

[55] Reegård, K., Blackett, C., and Katta, V. (2019). The concept of cybersecurity culture. Proceedings of the 29th European Safety and Reliability Conference, 4036-4043. https://doi.org/10.2991/ccit-14.2014.27

[56] Reid, R., and van Niekerk, J. (2014). *From information security to cyber security cultures organizations to societies.* 10.1109/ISSA.2014.6950492

[57] Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., and Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon,* 9(3). https://doi.org/10.1016/j.heliyon.2023.e14234

[58] Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., and Herawan, T. (2015). Information security awareness: An application of psychological factors – a study in Malaysia. *Computers & Security,* 53, 65-78. http://dx.doi.org/10.1016/j.cose.2015.05.012

[59] Samurai XDR. (2023). *Global threat intelligence report*.

[60] Schein, E. (2004). Organizational culture and leadership (3rd ed.). San Francisco, CA: Jossey-Bass. 45A pp. ISBN-10: 0787975745, ISBN-13: 978-0787975746

[61] Schoenmakers, K., Greene, D., Stutterheim, S., Lin, H., and Palmer, M. J. (2023). The security mindset: Characteristics, development, and consequences. *Journal of Cybersecurity*, 9(1). https://doi.org/10.1093/cybsec/tyad010

[62] Shaiq, H. M. A., Khalid, H. M. S., Akram, A., Ali, B. (2011). Why not everybody loves Hofstede? What are the alternative approaches to the study of culture? *European Journal of Business and Management*, 3(6), 101.

[63] Sharma, S., and Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among IT employees. *Computers & Security*, 120, 102774. https://doi.org/10.1016/j.cose.2022.102774

[64] Shore, L. M., Randel, A. E., Chung, B. G., Dean, M. A., Holcombe Ehrhart, K., and Singh, G. (2018). Inclusion and diversity in work groups: A review and model for future research. *Human Resource Management Review,* 28(2), 176-189. https://doi.org/10.1016/j.procs.2022.01.138

[65] Tariq, U., Ahmed, I., Bashir, A. K., and Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the Internet of things: A comprehensive review. *Sensors,* 23(8), 4117. https://doi.org/10.3390/s23084117

[66] Tasheva, I. (2021). *Cybersecurity post-COVID-19: Lessons learned and policy recommendations*. European View. https://doi.org/10.1177/17816858211059250

[67] Ubowska, A., and Królikowski, T. (2022). Building a cybersecurity culture of the public administration system in Poland. *Procedia Computer Science*, 207, 1242-1250. https://doi.org/10.1016/j.procs.2022.09.180

[68] Uchendu, B., Nurse, J. R., Bada, M., and Furnell, S. (2021). *Developing a Cyber security culture: Current practices and future needs.* ArXiv. https://doi.org/10.1016/j.cose.2021.102387

[69] Vyas, L. (2022). "New normal" at work in a post-COVID world: Work–life balance and labour markets. *Policy and Society*, 41(1), 155-167. https://doi.org/10.1093/polsoc/puab011

[70] Wiley, A., McCormac, A. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers and Security, 88*. https://doi.org/10.1016/j.cose.2019.101640

*** Economic Commission for Latin America and the Caribbean (ECLAC). (2021). Digital technologies for a new future (LC/TS.2021/43), Santiago.

*** EU Agency for Network and Information Security (ENISA). (2017). Cyber security cultures in organizations. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/@@download/fullReport

*** IEA (2021). Enhancing cyber resilience in electricity systems, IEA, Paris. Link, License: CC BY 4.0

*** McKinsey & Company. (2020). Digital McKinsey and Global Risk Practice Cybersecurity in a Digital Era. https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/cybersecurity%20in%20a%20digital%20era/cybersecurity%20in%20a%20digital%20era.pdf

Cite this article:

Willie, M. M. (2023). The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture. *Journal of Research, Innovation and Technologies*, Volume II, 2(4), 179-198. https://doi.org/10.57017/jorit.v2.2(4).05

Article's history:

Received: 14th of September, 2023; Revised: 5th of October, 2023; Accepted for publication: 15th of October, 2023; Available online: 15rd of October, 2023.
Published: 30th of December, 2023 as article in Volume II, Issue 2(4).