ISSN: 2182-2069 / E-ISSN: 2182-2077

Examining Cybersecurity Culture: Trends and Success Factors

Eko Yon Handri[1*], Dana Indra Sensuse[2], and Sofian Lusa[3]

[1*]Assistant Professor, Faculty of Computer Science, Universitas Indonesia, Depok, Indonesia.
eko.yon@ui.ac.id, https://orcid.org/0009-0008-3717-4553

[2]Professor, Faculty of Computer Science, Universitas Indonesia, Depok, Indonesia.
dana@cs.ui.ac.id, https://orcid.org/0000-0002-0012-8552

[3]Lecturer, Faculty of Tourism, Institute of Tourism Trisakti, Jakarta, Indonesia.
sofian.lusa@iptrisakti.ac.id, https://orcid.org/0000-0002-7924-6411

Received: April 06, 2024; Revised: June 12, 2024; Accepted: July 15, 2024; Published: August 30, 2024

Abstract

The human factor, as the weakest link, is a fundamental issue that creates threats and vulnerabilities in cybersecurity implementation. However, the management of human factors has not been addressed comprehensively because it has not fully positioned individuals as integral members of the organization in building a cybersecurity culture. This study examines the development of a cybersecurity culture to effectively manage and direct human factors as part of an organization to address this issue through a philosophical approach to organizational culture. Through a systematic literature review, we explored research trends and identified the success factors in building a cybersecurity culture. The process of synthesizing success factors is based on the concept of organizational culture, considering three layers: artifacts, espoused values, and basic assumptions. A total of 31 success factors were identified and categorized into three levels of organizational culture. This approach provides organizations with comprehensive insights into areas requiring improvement, facilitating a clearer path to strengthening cybersecurity culture and improving preparedness for cyber threats. Additionally, maintaining a balanced approach to success factors ensures a holistic perspective in addressing cybersecurity challenges, preventing the trap of relying solely on technological solutions.

Keywords: Cybersecurity, Cybersecurity Culture, Success Factor, Organization Culture.

1 Introduction

Cybersecurity is defined as a combination of technologies, resources, structures, and cultures used to protect data and systems from vulnerabilities, threats, exposure, and damage to ensure stability and sustainability (Hussain et al., 2020). However, cybersecurity is still viewed merely as the use of technology, and cyberattacks continue to occur, causing financial loss. In 2018, the OAS reported that many countries felt the financial impact of cybercrime, such as Brazil, reaching $8 billion, while in Mexico it reached $3 billion, and Colombia reaching $ 464 million (OAS, 2018). Cybersecurity ventures expect $6 trillion worth of damage annually by 2021 due to cybercrime. Additionally, Gartner projected that global spending on cybersecurity would reach $133.7 billion by 2022, owing to this

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 3 (August), pp. 330-352.
DOI: *10.58346/JISIS.2024.I3.020*

*Corresponding author: Assistant Professor, Faculty of Computer Science, Universitas Indonesia, Depok, Indonesia.

increase in cybercrime (Bertschi, 2020). Gelles (2016) revealed that 23% of cybercrime activities are caused by insiders (Gelles, 2016). Siemens (2018) emphasized that cybersecurity is more than just technology, but must become part of the DNA of every organization (Siemens, 2018). According to recent studies, the human factor is a major culprit, and is perceived as one of the most dangerous issues in cybersecurity, both intentionally and unintentionally (Udayakumar et al., 2023).

Various research streams have identified factors that influence behavioral humans, as individuals follow organizational processes and security control measures (Topa & Karyda, 2015; Yuryna Connolly et al., 2017). Human behavior forms a cybersecurity culture as an integral part of the organization in cyberspace to ensure the adequate protection and preservation of confidentiality, integrity, and availability (Da Veiga et al., 2020). Cybersecurity culture aims to address various human factors that can influence an organization's efforts to implement cybersecurity (Van Niekerk, 2014). A strong cybersecurity culture can help reduce the likelihood of noncompliance with security policies and thus minimize the threat resulting from human behavior (Branley-Bell et al., 2021).

Many studies show that employees are the weakest link, therefore, information security experts recommend that developing an information security culture, including cybersecurity culture, can improve information security in an organization (Nasir et al., 2017). Even a senior manager with poor leadership experience can be the weakest link in an organization's cybersecurity chain (Banks, 2016). There are differences in the position of human factors between information security and cybersecurity cultures (Oleksandr et al., 2024). In an information security culture, the human factor is part of the organizational process, whereas in a cybersecurity culture, the human factor is not only a part of the organization that must be protected, but also a threat that must be prevented (Reegård et al., 2019). Threats caused by unsafe online user behavior make them easy targets for exploitation (Kortjan & Von Solms, 2014). Providing training programs may improve knowledge and skills to prevent the exploitation, but many studies have shown that, although knowledge and awareness are necessary, they are not enough to implement real behavior and influence cultural change (Nasir et al., 2017; OAS, 2018). Several other factors, such as attitudes, norms, personality, superiority, and habits, can also influence human behavior as cyber threats (Glaspie & Karwowski, 2018). Therefore, human factor management must be addressed comprehensively by positioning individuals as members of an organization to build a cybersecurity culture (Ndife et al., 2022). The existence of an organization has a major impact and strong influence on building a cybersecurity culture by involving humans as members of the organization, while instilling beliefs, values, assumptions, symbols, norms, and knowledge related to information security that uniquely represent the organization (Alhogail & Mirza, 2014).

2 Background Information

Organizational Culture

Hofstede (1983) defined culture as 'collective mental programming' commonly held by individuals with similar educational backgrounds and life experiences (Hofstede, 1983). Culture can also be defined as a comprehensive entity comprising knowledge, beliefs, art, morals, laws, customs, and all human capabilities and behaviors acquired by individuals as part of society (Obradovich et al., 2022). Each organization with its own characteristics, has a unique culture compared with other organizations. This is emphasized by Whitmarsh et al., who state that individualistic and collectivistic cultures have different approaches to achieving organizational goals. Some influencing factors include cultural values, environment, and attitudes (Whitmarsh et al., 2017).

Schein (2004) developed the concept of organizational culture and divided its layers into three levels: artifacts, espoused beliefs and values, and basic underlying assumptions (Schein, 2004). These three cultural levels have been widely accepted by several studies (Surendar et al., 2024). Artifacts represent a visible layer of culture and offer tangible elements that can be seen through visual, auditory, or sensory experiences when interacting with a new cultural group. It could be an organizational structure, environment, technology, product, ceremony, and so on. Espoused beliefs and values are the middle layer of culture in which one can sense what should be consciously and become the reason for someone to observe an artifact. For example, a top manager believes in teamwork, and that everyone will improve an organization's performance. This could be addressed in the vision and mission statements of the organization. Basic underlying assumptions, such as tacit assumptions, are the deepest layer of culture and the essence of culture that is deeply embedded and taken for granted unconsciously by individuals towards human behavior, relationships, reality, and truth (Connolly & Lang, 2014; Reegård et al., 2019; Schein, 2004). The levels of organizational culture based on Schein's model consist of artifacts at the surface layer, espoused beliefs and values at the middle layer, and basic underlying assumptions at the deepest layer. All layers of culture influence one another. In particular, the beliefs and values layers exert influence on both the surface and deepest layers (Schein, 2004).

Several studies have adopted an organizational culture approach based on Hofstede's research on cybersecurity. Hussain et al., (2020) investigated the concept of cybersecurity culture and critical success factors in the critical infrastructure sector (Hussain et al., 2020). Onumo et al., (2021) explored cybersecurity culture in the public sector (Onumo et al., 2021). Vashistha et al., (2018) conducted a literature review on cybersecurity culture with demographic factors (Vashistha et al., 2018), including Connolly et al. research on cybersecurity culture in Ireland and the United States (Yuryna Connolly et al., 2017). However, these studies mainly focused on specific sectors or conditions, thus limiting their generalizability to the wider public. Therefore, this study aims to fill this gap by researching a broader scale that can be applied to all types of organizations and sectors, while considering the determinants of success in building a comprehensive cybersecurity culture through a philosophical approach to organizational culture (Desnitsky et al., 2016).

Cybersecurity

Cybersecurity covers a broad domain of technologies and methodologies used to protect computer networks, devices, and data from various security threats (Dykstra, 2015). Turk et al., (2022) emphasized that cybersecurity involves protecting interconnected intelligent systems from unauthorized exploitation, cyber-attacks, and potential damage to hardware, software, and electronic data (Turk et al., 2022). Although there is general confusion between the definitions of cybersecurity and information security, cybersecurity is fundamentally related to various other dimensions of security, including information security, application security, network security, internet security, and critical information infrastructure protection (Sutton, 2017). These interconnected aspects highlight the holistic approach that is required to solve cybersecurity problems from multiple perspectives.

A holistic approach connects various aspects of cybersecurity, starting with information security. Information security is concerned with maintaining confidentiality, integrity, and availability of data across multiple domains, both in cyberspace and beyond. This includes application security, which involves implementing controls and measures within an organization's applications in the form of both software and hardware. The interconnection between these devices forms a network; thus, network security is required, which aims to protect computer networks from internal and external threats such

as servers, server virtualization, and associated management systems. When these networks are connected to the public via the Internet, Internet security is required, which focuses on ensuring the reliability and availability of Internet-based services for organizations while protecting individuals in the workplace and home environment. Finally, all of these security aspects form a critical information infrastructure that must be protected, resulting in infrastructure protection to realize cyber safety for all critical infrastructure elements from cybercrime.

3 Methodology

We followed Kicthenham's guidelines (2004) to identify and evaluate the current state of relevant studies in three phases of Systematic Literature Review (SLR): planning, conducting, and reporting (Kitchenham, 2004), as illustrated in Figure 1. The steps we followed conformed to the latest Kicthenham guidelines (Kitchenham & Brereton, 2013). The planning phase identified the needs of the literature review, including the research questions, review protocol, and number of digital libraries used to search for relevant literature. The conducting stage processed the review protocol to obtain the data required for this study through data extraction and synthesis. The initial literature included 1962 articles. The results are reported at the reporting stage, either directly or through discussion.

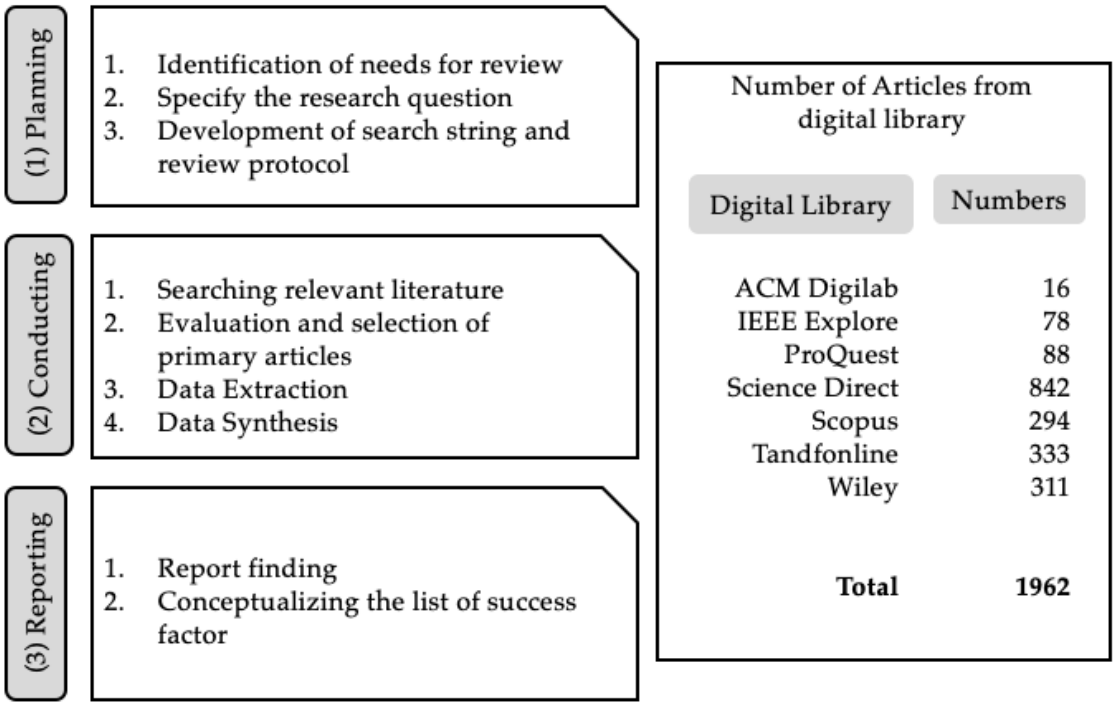

Figure 1: Systematic Literature Review (SLR) Phases

PICOC Criteria and Research Questions

We developed the Population, Intervention, Comparison, Outcomes, and Context (PICOC) criteria to ensure that this SLR provides results that align with the research problem. This study focuses on cybersecurity, which includes various aspects within an organizational environment. The interventions studied included cybersecurity culture, human behavior, and organizational culture, all of which play important roles in shaping the security landscape. The main point of comparison in this study is the information security culture by highlighting its differences or alignment with the factors that influence

the development of cybersecurity culture. The expected outcome of this review is the identification and understanding of the success factors in building cybersecurity culture. This review covers all organizations and sectors to emphasize the importance of comprehensive cybersecurity practices through an organizational culture approach. Table 1 summarizes the PICOC criteria used in this study.

Table 1: PICOC Criteria

Criteria	**Description**
Population	cybersecurity
Intervention	cybersecurity culture, human behavior, organizational culture
Comparison	information security culture
Outcomes	success factor contribution for building cybersecurity culture
Context	all organizations or sectors

In the next step of the first phase, we developed the following 2 Research Questions:

RQ1: What are the research trends regarding cybersecurity culture over the past decade?

RQ2: What are the success factors that influence in building of an organizational cybersecurity culture considering the layers of organizational culture?

Search Strategy

We developed a search string to cover a wide range of studies, using two main keywords.

(“cybersecurity culture” AND “success factor”)

As an initial search, we used Google to identify terms or phrases with similar meanings. We found that the keyword “cybersecurity culture” has four possibilities with similar meanings: “security culture”, “cybersecurity culture”, “cybersecurity culture” (without spaces), and "information security culture”. Therefore, the first keyword of the search string was (security OR "cybersecurity" OR cybersecurity OR "information security") AND culture. The second keyword, “success factor”, has two possibilities: “success factor” and “key factor”. Thus, the second keyword in the search string was (success OR key) AND factor.

Finally, the search string used to capture potentially relevant literature was as follows.

(Security OR "cybersecurity" OR cybersecurity OR "information security") AND culture AND (success OR key) AND factor.

We then defined seven trusted digital libraries: ACM, IEEE Explore, ProQuest, ScienceDirect, Scopus, Taylor and Francis Online, and Wiley, which served as our primary sources of research materials. We considered articles published from 2012 to 2023, including article types as peer-reviewed journals and international conferences, and were only used in English. There were also eight quality assessment criteria to screen relevant studies as primary articles. The detailed review protocol is described in Table 2.

Table 2: The Review Protocol of the Systematic Literature Review (SLR)

No	Protocol Attribute	Description
1	Source Search	ACM, IEEE Explore, ProQuest, ScienceDirect, Scopus, Taylor and Francis Online, Wiley.
2	Search String	(Security OR "cybersecurity" OR cybersecurity OR "information security") AND culture AND (success OR key) AND factor.
3	Inclusion	Publication year from 2012 – 2023, publication sources/document types are peer-reviewed journals and international conference proceedings, written in English, related to the success factor of security culture, the subject area is computer science.
4	Exclusion	Written in non-English, paper cannot be accessed, duplicate paper.
3	Quality Assessment Criteria	• Clarity of research object • Contain a literature review, background, and research question • Contain related work from previous research • Describe the proposed framework or methodology • Have research result • Show relevant conclusions • Have future work recommendation • Scopus indexed
4	Data Extraction Strategy	Contains information on the factors that influence security culture, information security culture, cybersecurity culture, human behavior.
5	Data Synthesis Strategy	Uses a data-driven approach from data extraction to categorize the factor for each paper.

Our search encompassed the following digital library resources.

- ACM Portal (https://dl.acm.org)
- IEEE Xplore (https://ieeexplore.ieee.org/Xplore/home.jsp)
- ScienceDirect (https://www.sciencedirect.com)
- Scopus (https://www.scopus.com)
- ProQuest (https://www.proquest.com/)
- Wiley (https://onlinelibrary.wiley.com/)
- Taylor & Francis Online (https://www.tandfonline.com/)

In the second phase, we conducted a search string for each digital library based on particular search features. There were metadata, abstract, title, keyword, and anywhere that were used to find known primary studies. We used then “abstract” feature in ACM Digital Library, the “all metadata” feature to search relevant studies in IEEE Explore, then “abstract” feature in ProQuest, “title-abstract-keyword” feature in Scopus, “all” feature in Taylor and Francis Online, and “anywhere” feature in Wiley. No special search features were found for ScienceDirect. Table 3 summarizes the search features used in this study.

Table 3: Search Features on Seven Digital Libraries with their Respective Patterns

ACM Digital Library [[Abstract: security] OR [Abstract: "cybersecurity"] OR [Abstract: cybersecurity] OR [Abstract: "information security"]] AND [Abstract: culture] AND [[Abstract: success] OR [Abstract: key]] AND [Abstract: factor]'
IEEE Explore ("All Metadata": security OR "All Metadata":"cybersecurity" OR "All Metadata": cybersecurity OR "All Metadata": "information security") AND ("All Metadata": culture) AND ("All Metadata": success OR "All Metadata": key) AND ("All Metadata": factor)
ProQuest abstract ((security OR "cybersecurity" OR cybersecurity OR "information security")) AND abstract(culture) AND abstract ((success OR key)) AND abstract(factor)
ScienceDirect (Security OR "cybersecurity" OR cybersecurity OR "information security") AND culture AND (success OR key) AND factor
Scopus TITLE-ABS-KEY ((security OR "cybersecurity" OR cybersecurity OR "information security") AND culture AND (success OR key) AND factor)
Taylor and Francis Online [[All: security] OR [All: "cybersecurity"] OR [All: cybersecurity] OR [All: "information security"]] AND [All: culture] AND [[All: success] OR [All: key]] AND [All: factor]
Wiley "(security OR "cybersecurity" OR cybersecurity OR "information security") AND culture AND (success OR key) AND factor" anywhere

We then executed a review protocol to identify all relevant studies and evaluated them to obtain the final articles as the main studies of this research. In total, 1.962 articles were included in the initial selection. We removed duplicate articles and articles that could not be accessed, resulting in 1919 articles. Screening was then performed based on titles and abstracts that contained related work on security culture, resulting in 74 articles. After reviewing the full text, 52 articles were selected. Finally, we selected 45 articles as primary articles based on quality assessment. These steps are illustrated in the following diagram in Figure 2.

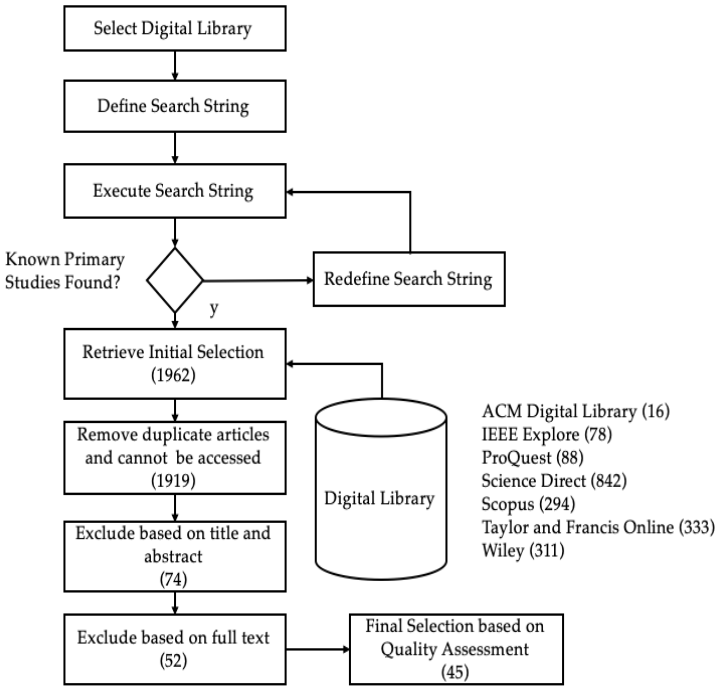

Figure 2: The Process of Selecting Primary Articles

Data Extraction

Derived from the 45 selected primary articles, we extracted all factors affecting security culture, information security culture, cybersecurity culture, and human behavior. In total, 390 factors were identified in this study. However, some factors have similar terminology or notions, such as leadership, training, trust, and costs, which are similar to budgets. These factors were synthesized to determine the different success factors. A comprehensive set of primary articles is presented in Table 4. We facilitated the use of article identification numbers (e.g., A1 and A2) throughout this study for easy reference to the articles reviewed.

Data Synthesis

In this study, a data-driven approach was used to synthesize all the relevant factors identified during data extraction. Differentiated factors were selected from a set of factors that had common terminology or meanings, thus representing success factors. Certain factors found in the common terminology were also categorized as success factors. For example, factors such as gender, religion, and age are integrated into a broader category of success factors in the demographic terminology. Organizational posture, which includes aspects such as organizational size and structural complexity, has been identified as an illustrative example of a success factor.

Table 4: Full List of Primary Articles

ID	Study	ID	Study	ID	Study
A1	(Hussain et al., 2020)	A16	(Zendehdel et al., 2016)	A31	(Jonathan et al., 2021)
A2	(Onumo et al., 2021)	A17	(Ramachandran et al., 2013)	A32	(Bozic, 2012)
A3	(Vashistha et al., 2018)	A18	(Hassan et al., 2013)	A33	(Shah et al., 2023)
A4	(Nasir et al., 2017)	A19	(Alhogail & Mirza, 2014)	A34	(Hassandoust & Johnston, 2023)
A5	(Aman & Shukaili, 2021)	A20	(Yaseen et al., 2016)	A35	(Creese et al., 2021)
A6	(Gcaza et al., 2017)	A21	(Ismail et al., 2022)	A36	(Lehto & Limnéll, 2021)
A7	(Tolah et al., 2021)	A22	(Cellier & Ghernaouti, 2019)	A37	(Box & Pottas, 2014)
A8	(Ioannou et al., 2019)	A23	(Asgarkhani et al., 2017)	A38	(Uchendu et al., 2021)
A9	(Da Veiga et al., 2020)	A24	(Mousavi & Kumar, 2019)	A39	(Alshaikh, 2020)
A10	(Amankwa et al., 2018)	A25	(Al Qahtani et al., 2020)	A40	(Da Veiga & Martins, 2015b)
A11	(Astakhova, 2020)	A26	(Abujassar & Al-Majeed, 2014)	A41	(Da Veiga & Martins, 2015a)
A12	(Doherty & Tajuddin, 2018)	A27	(Mansol et al., 2014)	A42	(Ma, 2022)
A13	(Kortjan & Von Solms, 2014)	A28	(Kalhoro et al., 2021)	A43	(Ameen et al., 2021)
A14	(Romero et al., 2019)	A29	(Desourdis et al., 2016)	A44	(Sharma & Aparicio, 2022)
A15	(Pietruszka-Ortyl et al., 2021)	A30	(Alnatheer, 2015)	A45	(Karjalainen et al., 2020)

4 Results

Research Trends

This section summarizes the research trends derived from the meta-analysis of primary articles. It conveys the distribution of research interest in security culture, which includes cybersecurity culture, information security culture, and human behavior, across different journals, as depicted in Figure 3,

and the publication distribution of articles in recent years, as shown in Figure 4. Figure 5 also illustrates the geographical distribution of authors affiliated with different countries researching this topic. Additionally, cybersecurity culture has varying impacts across sectors, providing a list of sectors that constitute the scope of cybersecurity culture implementation research, as shown in Figure 6.

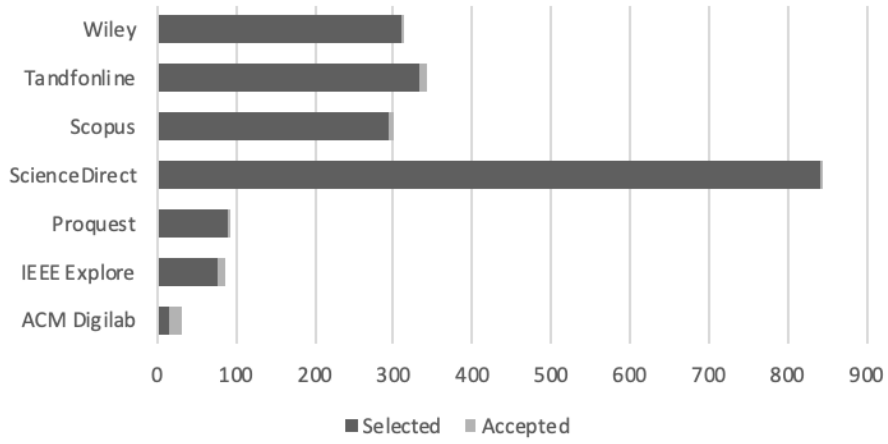

Figure 3: Distribution of Articles Publication Per Sources

Figure 3 also illustrates the distribution of the number of articles and the digital libraries that published them. Among all digital libraries, ScienceDirect published the highest number of selected articles related to cybersecurity culture, namely, 842 (45%), compared to other digital libraries. However, only 9 articles were accepted as primary articles, equivalent to 1.07% of all published articles. Similar to ScienceDirect, Tandfonline experienced similar conditions in publishing 333 articles (16.97%), and two articles were accepted as primary articles (0.60%). The same condition also occurred in Wiley, which published 311 articles (15.85%), with only one article accepted as a primary article (0.32%), the lowest among all digital libraries. Two digital libraries, IEEE Explore and ACM Digital Library, experienced different conditions in providing more articles selected as primary articles. Although IEEE Explore published 78 articles (3.98%), the number) were accepted as primary articles. Meanwhile, the ACM Digital Library published the least number of articles, 16 (0.82%), but contributed four primary articles (25%). This indicates that search features in digital libraries can significantly influence the provision of articles required by researchers. Moreover, it is important to note that publication trends of articles on cybersecurity culture vary across digital libraries.

Research on cybersecurity culture has remained an interesting topic in the last decade, from 2012 to 2023. As shown in Figure 4, 2021 marked the peak in cybersecurity cultural research. Based on this data, it is believed that in the coming years, there will be an increase in new research on cybersecurity culture from various perspectives. This is because the implementation of cybersecurity is no longer only focused on technology but has become more comprehensive by considering human and organizational factors.

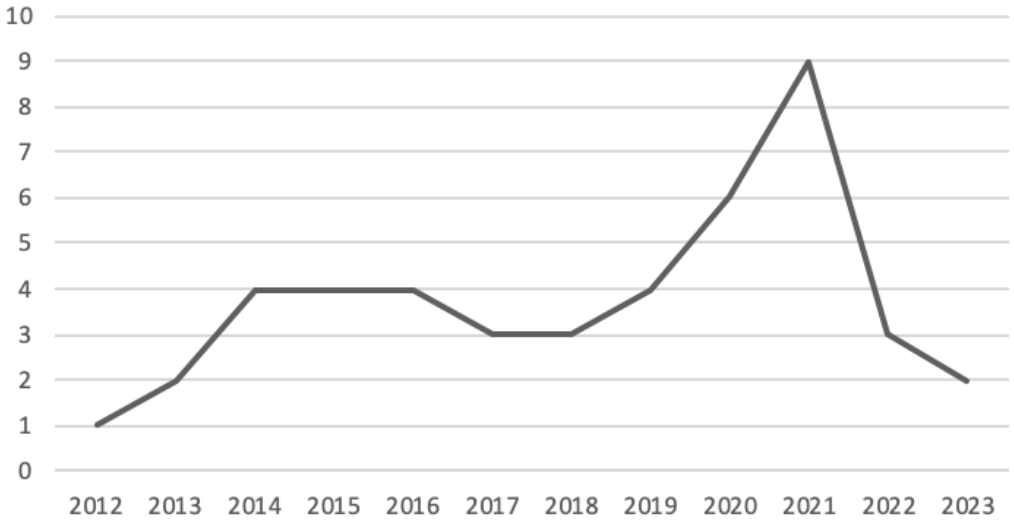

Figure 4: Distribution of Primary Article Publications in Recent Years

Figure 5 shows the geographical distribution of the countries in which the authors studied this topic. Six primary articles were published by researchers from South Africa, followed by Malaysia and the United Kingdom, each contributing five studies, whereas the United States contributed three studies. Based on these data, it is clear that these four countries have contributed significantly to research on cybersecurity culture. Therefore, it can be concluded that they have been able to empower the cybersecurity culture to protect their systems and proactively anticipate potential cyber threats. Overall, researchers from different continents have recognized the importance of cybersecurity culture in improving systems and data protection. The United States and Canada are Americas. Asia includes Brunei, China, India, Jordan, Malaysia, Morocco, Oman and Saudi Arabia. Europe includes Croatia, Finland, Poland, Russia, Spain, Sweden, Switzerland and Turkey. Australia and New Zealand are representative of Australia.

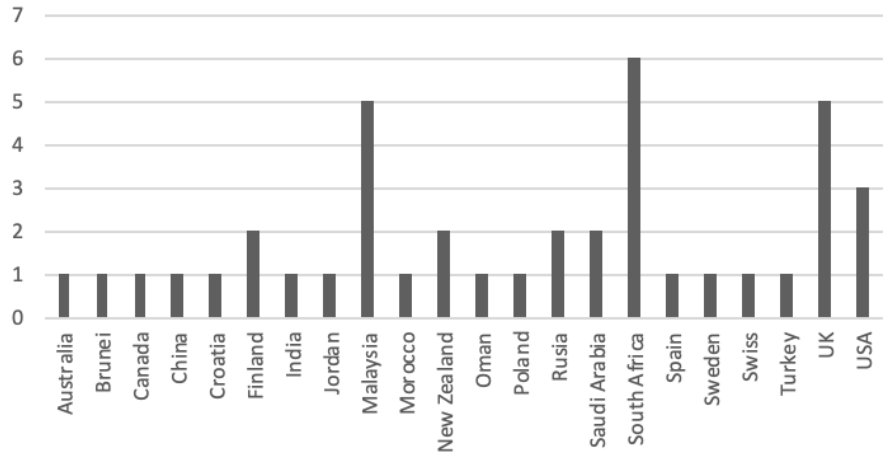

Figure 5: Distribution of Research Authors Affiliated with their Country

A cybersecurity culture is part of an organizational culture in which the adaptation of its implementation is tailored to the characteristics of the organization. This study explored the implementation of cybersecurity culture in various organizational sectors. Articles that do not

explicitly mention a specific sector are generally applicable across all sectors. Figure 6 illustrates the sectors covered in research on cybersecurity culture. A total of 24 articles (42.11%) examined cybersecurity culture across all sectors. The government sector ranked second as the largest research area, comprising 11 articles (19.30%). In addition, there were three sectors, namely the digital economy, health, and information technology, each with four articles (7.02%) on cybersecurity culture research. Other sectors covered included business, construction, education, energy, finance, and industry. The cybersecurity culture can be applied across a wide range of sectors. However, certain sectors, notably the government, digital economy, healthcare, and information technology sectors, require special attention because of the need to secure confidential information from cyber threats.

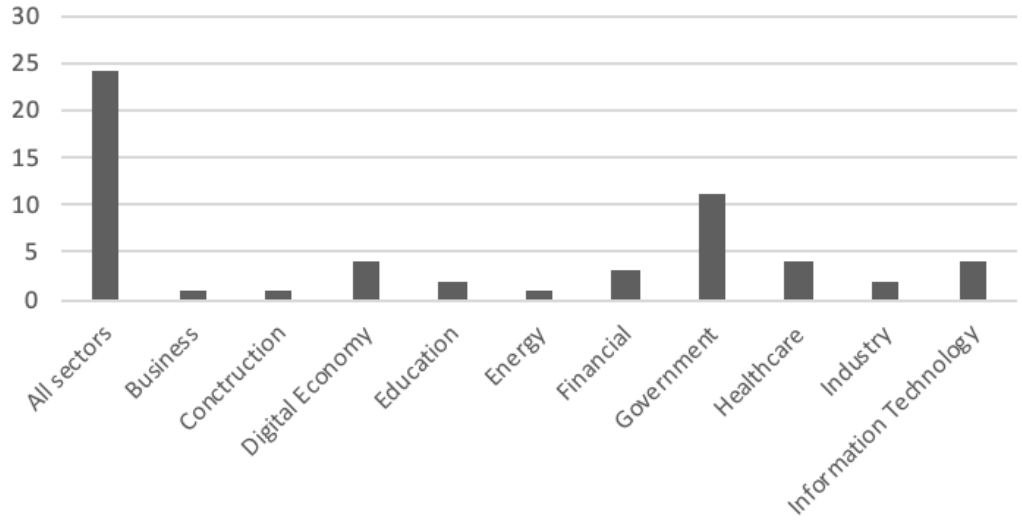

Figure 6: Distribution of Sectors as Research Scope for Cybersecurity Culture Topics

Cybersecurity Culture Success Factors

Success factors can be interpreted as elements that influence success and anticipate mistakes in the process of achieving goals, depending on the substance discussed. For example, (Norman & Yasin, 2013) defined information system security management success factors as elements needed to anticipate and prevent information security failures (Norman & Yasin, 2013). Diesch et al., (2020) define management success factors as elements that consider the condition of a component in making appropriate management decisions in the context of an organization's information security (Diesch et al., 2020). Considering the definition of cybersecurity culture and the layers of organizational culture, we define cybersecurity culture success factors as factors or elements that influence the success of building a cybersecurity culture based on three layers of organizational culture, namely artifacts, espoused values, and basic assumptions, to minimize risks from cyber threats.

From the comprehensive analysis presented in the primary articles, we identified 31 success factors, as shown in Table 5, that contribute to the formation of cybersecurity culture in organizations and can be applied across sectors. To further dissect these elements, we considered three layers of organizational culture: artifacts, espoused beliefs, and underlying assumptions. For example, the aspects of awareness, training, and education, which are often grouped into one factor in a Security Education, Training, and Awareness (SETA) program, can be divided into two distinct success factors. Awareness and training are categorized under the espoused beliefs layer, because organizational members openly and consciously build organizational values. Meanwhile, education is associated with

the basic assumptions layer, as its influence has a long-term impact on the individual as a member of the organization and is often implemented at a subconscious level.

Thirty studies highlighted the importance of awareness and training as success factors in building a cybersecurity culture. Governance was mentioned in 20 studies, including studies A9, A11, A12, A40, A32, and A45, which discussed security policies and regulations that influence the implementation of cybersecurity culture. Commitment and support also appeared in 20 studies that explicitly mentioned managerial involvement in making consistent commitments and supporting subordinate activities as outlined in Studies A9, A30, and A38. The educational factors were mentioned in 19 studies.

The four factors featured 14 articles each: compliance, leadership, trust, and personality values. Except for personality values, the other three factors were clearly articulated as success factors in the cybersecurity culture. These personality traits were also associated with ethical behavior (A9), personal qualities (A11), performance qualities (A14), and personality differences (A18).

Skills and expertise, attitudes, and self-efficacy were explicitly discussed in 12 articles, each as success factors in building a cybersecurity culture. Meanwhile, security behaviors were mentioned in 11 articles, including aspects related to security ownership (A9). Security technology and collaboration were clearly articulated in ten articles each as success factors. Ten articles mentioned organizational posture, which we elaborated on, including those related to organizational size (A5, A35) and structure (A24, A28, and A31).

Security control was explicitly stated as a success factor in nine studies, as was communication. The same applies to change management and experience, which were mentioned in eight studies. Although it has the same number of studies as the previous two factors, demographics have a broader definition and thus include aspects related to gender (A3, A20, A28, A33), religion, or beliefs of the individual (A3, A4, A12, A26), and age (A20, A28). Furthermore, infrastructure was explicitly mentioned in 7 studies. The same goes for the teamwork spirit, which includes team building (A21), along with the motivation that drives their performance (A19, A42, A43).

Risk management, socioeconomic barriers, and subjective norms were explicitly mentioned in six studies each. Action plans were mentioned in 5 studies, including discussions related to change management (A5, A40, A41). Organizational strategy, which includes organizational goals (A13) and a national cultural approach (A11), was mentioned in five studies. Security audit emerged as a success factor in three studies, as did research and innovation.

The last success factor, self-reliance, was mentioned in 3 studies (A5, A33, A36) and it is a success factor that is rarely discussed in cybersecurity culture development. Therefore, this issue was addressed in this study. We argue that self-reliance has a significant impact on cybersecurity culture, because most operations in an organization depend on technology to execute cybersecurity strategies. If an organization fails to adopt technological solutions from external sources, it weakens its ability to effectively secure its systems, thus making it vulnerable (Aman & Shukaili, 2021). Self-reliance in cybersecurity refers to an organization's capacity to independently develop and maintain its capabilities, technologies, and proficiency in protecting its digital infrastructure, data, and information systems and to reduce dependence on external providers for cybersecurity resources and knowledge. Table 5 presents the success factors of cybersecurity culture along with the frequency of each factor and definitions compiled from various relevant studies.

Table 5: List of Success Factors for Building a Cybersecurity Culture

No	Success Factors	Relevant Studies	Total	Description
1	Awareness and Training	A1, A3, A4, A5, A6, A7, A8, A9, A13, A17, A18, A19, A21, A23, A24, A25, A27, A28, A30, A31, A32, A33, A35, A37, A38, A39, A40, A41, A42, A45	30	a program of activities designed to provide organizational members with the skills and abilities of best practices and procedures to mitigate risks from cybersecurity threats
2	Governance	A1, A4, A5, A7, A9, A11, A12, A14, A21, A24, A30, A32, A33, A35, A36, A38, A40, A41, A43, A45	20	preparing, establishing and enforcing policies, procedures and standards to ensure effective management and supervision of cybersecurity related activities in an organization including determining roles, responsibilities and decision-making processes to achieve organizational goals
3	Commitment and Support	A1, A4, A5, A6, A7, A9, A11, A14, A18, A19, A22, A24, A27, A30, A31, A34, A38, A42, A44, A45	20	an expression of dedication and support from the organization's leadership and management towards the implementation of the cybersecurity program
4	Education	A3, A4, A6, A7, A8, A9, A11, A13, A14, A15, A19, A20, A25, A27, A30, A32, A33, A35, A37	19	a long-term formal learning activity to develop individual knowledge and skills in understanding and applying cybersecurity principles, practices and technology
5	Compliance	A1, A2, A4, A5, A6, A7, A9, A10, A11, A16, A17, A21, A30, A45	14	condition of being expected to meet and comply with regulatory requirements, standards and policies governing cybersecurity practices within an organization
6	Leadership	A2, A10, A11, A14, A15, A17, A27, A29, A35, A38, A40, A41, A43, A44	14	a knowledge and ability to mobilize others in the form of guidance, direction, or instructions possessed by organizational leaders to encourage the implementation of cybersecurity initiatives and foster a security culture throughout the organization
7	Trust	A4, A8, A9, A11, A15, A18, A26, A28, A29, A35, A37, A38, A40, A41	14	a relationship of confidence towards each other regarding both in general and in relation to security activities including security measures, processes and systems implemented in an organization
8	Personality Value	A9, A11, A12, A14, A15, A16, A17, A18, A23, A37, A38, A43, A44, A45	14	values that build individual characteristics and traits in determining how to address cybersecurity practices in everyday life and within an organization, such as discipline and empathy
9	Skill and Expertise	A3, A5, A14, A23, A24, A27, A31, A35, A36, A38, A39, A45	12	technical proficiency, knowledge, and abilities necessary to professionally design, implement, manage, and evaluate cybersecurity controls and technologies
10	Attitude	A2, A7, A12, A5, A16, A32, A37, A38, A42, A43, A44, A45	12	an individual's perception and opinion expressed in action regarding cybersecurity practices, risks and responsibilities within an organization
11	Self-efficacy	A7, A15, A18, A19, A26, A28, A32, A37, A38, A42, A43, A44	12	an individual's belief in their own ability to perform certain activities and act in accordance with cybersecurity principles and best practices
12	Security Behaviour	A4, A5, A9, A11, A15, A18, A22, A24, A39, A42, A44,	11	n action and habit demonstrated by individuals or groups within an organization to protect assets from cyber threats and be able to mitigate security risks
13	Security Technology	A2, A3, A9, A11, A13, A19, A22, A28, A40, A41	10	a collection of hardware, software, and other devices used by organizations to identify cyber threats, protect against and detect cyber-attacks, and respond to and recover from cyber incidents
14	Organization Posture	A5, A9, A22, A24, A28, A31, A34, A35, A36, A44	10	the overall status of the organization from its structure and size that presents a holistic picture of its security strengths and weaknesses including those related to hardware, software, data, and user behavior
15	Collaboration	A5, A8, A10, A13, A14, A15, A21, A24, A38, A39	10	a form of cooperation and partnership established among various parties, both internal and external to the organization, to collectively address cybersecurity issues
16	Security Control	A7, A9, A11, A14, A16, A19, A28, A40, A41	9	a collection of protective measures and mechanisms implemented by organizations to manage and mitigate cybersecurity risks
17	Communication	A8, A15, A18, A19, A24, A28, A35, A38, A45	9	information exchange activities including warnings and notifications related to cybersecurity activities between parties within the organization and with external parties

				by using mutually agreed media
18	Demographic	A3, A4, A12, A16, A20, A26, A28, A33	8	a characteristic of society including age, gender, education, occupation, religion, race, and geographic location that can influence individual actions regarding cybersecurity practices
19	Budget	A5, A24, A25, A27, A28, A36, A42, A44	8	the financial resources allocated by an organization to meet the needs of technology, personnel, regulatory development, policy implementation, and other initiatives related to cybersecurity to protect the organization's assets and infrastructure from cyber threats
20	Change Management	A5, A9, A13, A24, A38, A40, A41, A45	8	systematic process of managing changes to systems, processes, people, and policies to achieve organizational goals and minimize security risks
21	Experience	A2, A3, A20, A24, A25, A28, A29, A41	8	a result of direct observation of an event thereby increasing knowledge and insight from the past in the practical context of cybersecurity
22	Infrastructure	A1, A3, A24, A32, A33, A35, A37	7	all structures and facilities that are interconnected and used to operationalize cybersecurity technology to protect an organization from cyber threats
23	Teamwork Spirit	A5, A8, A15, A19, A21, A42, A43	7	a collaborative and cooperative mindset formed among team members to safeguard the organization and jointly overcome cybersecurity challenges
24	Risk Management	A1, A4, A7, A9, A21, A25	6	a systematic and continuous process of identifying, analyzing, evaluating and treating on security risks to reduce the impact and losses to the organization due to cyber threats
25	Socio-Economic Barrier	A2, A3, A9, A11, A28, A33	6	anything that might obstruct or hinder an organization's ability to enact cybersecurity measures and safeguard its assets from influences stemming from social, cultural, economic, and political domains
26	Subjective Norm	A2, A12, A28, A37, A42, A43	6	an individual's perception or interpretation of social norms and how others perceive them leads to considerations about whether to act or not in the context of cybersecurity practices
27	Action Plan	A1, A5, A13, A40, A41	5	a list of specific steps, tasks, and timelines required by an organization to protect its assets and infrastructure from cyber threats
28	Organization Strategy	A5, A11, A13, A19, A31	5	a strategic plan prepared by an organization to manage cybersecurity risks and protect assets and infrastructure in order to achieve cyber resilience
29	Security Audit	A5, A8, A24	3	a systematic and independent examination process for evaluating the implementation of an organization's security policies, procedures, and practices to determine the adequacy of security controls
30	Research and Innovation	A6, A15, A35	3	an exploratory activity to develop new innovations and provide improvements to technology, methodology and approaches in cybersecurity practices
31	Self-Reliance	A5, A33, A36	3	organization's capacity to independently develop and maintain its capabilities, technologies, and proficiency in protecting its infrastructure, data, and information systems, and to reduce dependence on external providers for cybersecurity resources and knowledge

Table 5 also presents interesting findings regarding the top five success factors that confirm previous research and contribute to correcting misperceptions of cybersecurity solutions. Awareness and training have become the most mentioned in primary articles as a success factor in building cybersecurity culture, which is at the espoused value level and strategy dimension. However, awareness and training are insufficient to implement cybersecurity in real behavior (Nasir et al., 2017; OAS, 2018). Education, as the fourth highest success factor, is usually integrated into a single program called the Security Education, Training, and Awareness Program (SETA Program). By contrast, security technology, which is often considered the solution to all cybersecurity problems, has a lower frequency than that mentioned in the primary articles.

As the third-highest success factor, commitment and support have emerged to affirm that human factors are among the most dangerous issues in cybersecurity. All roles within the organization, from end users to top management, must have shared commitment and support to implement cybersecurity properly. Governance and compliance, the second and fifth most successful factors, respectively, are also critical to an organization's cybersecurity success. This can reduce the likelihood of noncompliance with the security policy, and thus minimize cyber threats (Van Niekerk, 2014). However, when establishing a cybersecurity culture, it is insufficient to depend exclusively on these five primary factors, as this can lead to the same misunderstanding of cybersecurity challenges, specifically, an excessive focus on just one factor. Therefore, all these success factors should be implemented proportionally and tailored to the specific circumstances and capabilities of the organization.

5 Discussion

Redefining Cybersecurity Culture

Various studies have defined the cybersecurity culture based on their perspectives and findings. Ioannou et al., (2019) argued that cybersecurity culture refers to the procedures an organization has established for all employees in cyberspace, which directs actions related to data integrity during the course of their duties (Ioannou et al., 2019). Gcaza et al., (2017) suggested that cybersecurity culture should ideally be fostered at all levels, including individual, organizational, national, and international (Gcaza et al., 2017). They also defined cybersecurity culture as an intentional and unintentional manner in which cyberspace is utilized from an international, national, organizational, or individual perspective.

Organizational culture has an information security culture as a subset, therefore, the foundation of information security culture relies on current organizational culture (Alhogail & Mirza, 2014). Astakhova (2020) argued that information security culture is a method of deliberate and constructive joint activities of managers and employees to ensure and increase the level of organizational information security, which is expressed in the values, needs, knowledge, and behavior of managers and employees (Astakhova, 2020). However, there is often confusion regarding the use of terms for information security and cybersecurity, and these terms are often interchanged in the literature. However, (Reegård et al., 2019) emphasized the difference between the two terms in the context of organizational culture. In an information security culture, human factors are considered assets that must be protected from various vulnerabilities and threats, whereas in a cybersecurity culture, human factors are not only considered assets that must be protected but also potentially become vulnerabilities and threats themselves (Reegård et al., 2019).

Based on insights gained from previous research on cybersecurity culture, we present a definition from another perspective that integrates the concept of organizational culture and acknowledges the impact of human factors that distinguish cybersecurity culture from information security culture. Therefore, cybersecurity culture is defined as an organizational approach that leverages all layers of organizational culture, including artifacts, espoused beliefs, and basic assumptions, to protect cyberspace and considers the human factor as both a protected entity and a potential threat or attacker within the organization. The interrelationships among organizational culture, information security culture, and cybersecurity culture are shown in Figure 7.

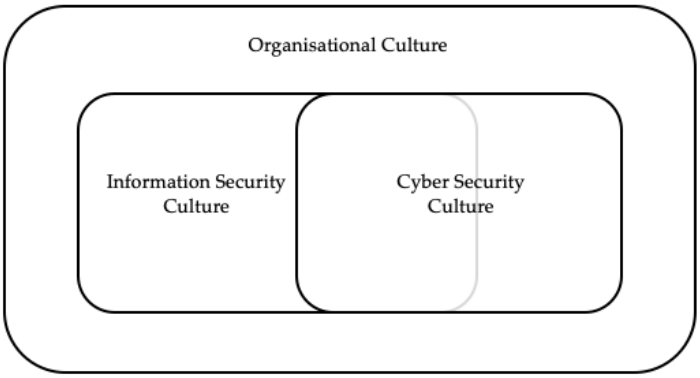

Figure 7: Interrelationships among Organizational, Information Security, and Cybersecurity Culture

Mapping Success Factors

Table 6 illustrates the mapping of success factors at the organizational culture level. Through repeated discussions among the authors, based on Schein's cultural layer model, we categorized the 31 success factors into their respective layers. In the artifact layer, Schein explicitly provides examples, making it easier to map the success factors. However, in the layers of espoused values and basic assumptions, Schein explains implicitly through examples of their application in two organizations: Digital Equipment Corp. (DEC), and Ciba-Geigy Company (Schein, 2004). As a result, expert validation is required to map the success factors in these two layers. Based on primary references, discussions among the authors, and expert validation, the mapping results show that the artifact layer has 11 success factors, espoused values have 12, and basic assumptions have 8 success factors.

Table 6: Mapping Success Factors to Organizational Culture Layers and STOPE Dimensions

Level of Culture	Success Factor	
Artifacts	1. Action Plan	7. Organization Strategy
	2. Budget	8. Research and Innovation
	3. Demographic	9. Security Audit
	4. Governance	10. Security Control
	5. Infrastructure	11. Security Technology
	6. Organization Posture	
Espoused Values	1. Awareness and Training	7. Leadership
	2. Change Management	8. Risk Management
	3. Collaboration	9. Self-Reliance
	4. Commitment and Support	10. Skill and Expertise
	5. Communication	11. Socio-Economic Barrier
	6. Compliance	12. Teamwork
Basic Assumptions	1. Attitude	5. Security Behavior
	2. Education	6. Self-efficacy
	3. Experience	7. Subjective Norm
	4. Personality Value	8. Trust

This mapping of success factors can help organizations gain deeper insight into which layers of their organizational culture require improvement. Previous studies and existing implementations have often neglected this consideration, causing ambiguity about the necessary steps to fortify cybersecurity culture and prepare organizations to handle cyber threats. Such uncertainty may lead to misguided efforts and misallocated resources, focusing on areas that are already adequate, and neglecting critical areas that need immediate attention and action.

To illustrate this scenario, we outline strategies for improving cybersecurity culture from a human-centered perspective, in which organizational members often fall prey to social engineering attacks. It is critical to examine vulnerabilities in the behavior of organizational members. For example, even though the three success factors of training, awareness, and education programs are well in place, individuals still often fall victim to phishing attacks. Therefore, another success factor that may need to be improved is self-efficacy, which empowers individual's confidence in spotting threats and avoids suspicious activities immediately. Alternatively, fostering teamwork that is conducive to vigilance against such attacks is another important factor. This illustration enables a clear identification of the layers of organizational culture and the dimensions that have underlying problems. While initial identification indicated problems with awareness and training in the espoused values layer, subsequent evaluation revealed that the root cause lay in the basic assumptions layer. Based on these findings, organizations can prioritize improving factors in the basic assumptions layer or direct their focus toward improving teamwork in the artifact layer and organizational dimensions. By mapping success factors across organizational culture layers, practical insights can be generated to implement a comprehensive, effective, and efficient organizational culture approach.

Practical Implications

It is important to consider that building a cybersecurity culture should not rely solely on conventional approaches, such as SETA programs alone or only implementing security technologies, as these methods could lead to the wrong direction when addressing cybersecurity issues. All success factors in this study must be applied proportionally, considering the organization's conditions and capabilities. Additionally, the identified success factors can serve as indicators for comprehensively evaluating the level of cybersecurity culture development within an organization. The results of this evaluation can provide insights into an organization's cyber resilience across the three levels of organizational culture: artifacts, espoused values, and basic assumptions. This allows an organization to enhance its cybersecurity strategies and optimize the effectiveness and efficiency of its programs.

6 Conclusion

This study contributes to the literature on research trends and success factors in building a cybersecurity culture. An overview of research trends in cybersecurity culture shows that research on this topic is ongoing across continents annually. This trend highlights some countries' recognition of the importance of cybersecurity culture in achieving holistic cybersecurity practices. Furthermore, this study redefines the cybersecurity culture and provides detailed explanations of each success factor. In particular, the inclusion of the self-reliance factor, which has rarely been discussed, had a significant impact. This differentiates this study from the previous research.

Regarding success factors in building a cybersecurity culture, this study explores the organizational culture layers according to Schein's model, which consists of three layers: artifacts, espoused values, and basic assumptions. This approach empowers the human factor comprehensively as members of the

organization, a practice rarely applied in cybersecurity. The study successfully identified 31 success factors, mapped across the three layers of organizational culture based on the primary literature, repeated discussions, and expert validation. It is crucial to apply all of these success factors proportionally, tailored to the specific needs and capabilities of the organization, to avoid misunderstandings in addressing cybersecurity issues. Mapping the success factors into the three cultural layers aims to provide practical insights for comprehensive, effective, and efficient implementation, thereby reducing uncertainties that could lead to misguided efforts, misallocated improvement initiatives, and neglect of critical areas requiring greater attention.

This study had several limitations and opportunities for further investigation. We limited our coverage to seven digital libraries from 2012 to 2023, thereby leaving room for additional research to enrich the definition and identification of the success factors for cultivating cybersecurity culture. Future research could expand the contribution of cybersecurity culture success factors by integrating them into a cybersecurity framework using a cybersecurity culture approach or by developing an assessment framework for the implementation of cybersecurity culture in organizations.

Acknowledgments

The authors acknowledge the support from the Faculty of Computer Science at the University of Indonesia. This research was also supported by the Educational Fund Management Institution, Ministry of Finance, Indonesia (Lembaga Pengelola Dana Pendidikan/LPDP) for granting the scholarship.

Competing Interests

We have no competing interests.

Authors' Contributions

E.Y.H.: conception and design, acquisition of data, analysis and interpretation of data, drafting, and revising; D.I.S.: conception and design, acquisition of data, analysis and interpretation of data, drafting, drafting, revising, supervision, and approval; S.L.: acquisition of data, analysis and interpretation of data, and revising.

References

[1] Abujassar, R., & Al-Majeed, S. S. (2014). E-commerce: A new framework to aggregate culture with website design. *International Conference on Web and Open Access to Learning (ICWOAL)*, 1–5. https://doi.org/10.1109/ICWOAL.2014.7009225

[2] Al Qahtani, E., Javed, Y., Lipford, H., & Shehab, M. (2020). Do Women in Conservative Societies (Not) Follow Smartphone Security Advice? A Case Study of Saudi Arabia and Pakistan. *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 150–159. https://doi.org/10.1109/EuroSPW51379.2020.00028

[3] Alhogail, A., & Mirza, D. A. (2014). A Framework of Information Security Culture Change. *Journal of Theoretical and Applied Information Technology*, *64*, 540–549.

[4] Alnatheer, M. A. (2015). Information Security Culture Critical Success Factors. *12th International Conference on Information Technology - New Generations*, 731–735. https://doi.org/10.1109/ITNG.2015.124

[5] 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

[6] Aman, W., & Shukaili, J. A. (2021). A Classification of Essential Factors for the Development and Implementation of Cyber Security Strategy in Public Sector Organizations. *International*

Journal of Advanced Computer Science and Applications, *12*(8), 169-176. https://doi.org/10.14569/IJACSA.2021.0120820

[7] Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information & Computer Security*, *26*(4), 420–436. https://doi.org/10.1108/ICS-09-2017-0063

[8] Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior*, *114*, 106531. https://doi.org/10.1016/j.chb.2020.106531

[9] Asgarkhani, M., Correia, E., & Sarkar, A. (2017). An overview of information security governance. *International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, 1–4. https://doi.org/10.1109/ICAMMAET.2017.8186666

[10] Astakhova, L. V. (2020). Issues of the Culture of Information Security under the Conditions of the Digital Economy. *Scientific and Technical Information Processing*, *47*(1), 56–64. https://doi.org/10.3103/S0147688220010062

[11] Banks, N. (2016). Practise what you preach. *Computer Fraud & Security*, *2016*(4), 5–8. https://doi.org/10.1016/S1361-3723(16)30035-5

[12] Bertschi, S. (2020). 5 Things Business Analysts Can Do to Advance Their Cybersecurity Practice. *IEEE Computer Society*. https://www.computer.org/publications/tech-news/trends/advance-cybersecurity-practice

[13] Box, D., & Pottas, D. (2014). A Model for Information Security Compliant Behaviour in the Healthcare Context. *Procedia Technology*, *16*, 1462–1470. https://doi.org/10.1016/j.protcy.2014.10.166

[14] Božić, G. (2012). The role of a stress model in the development of information security culture. *In IEEE Proceedings of the 35th International Convention MIPRO*, 1555-1559.

[15] Branley-Bell, D., Coventry, L., & Sillence, E. (2021). Promoting Cybersecurity Culture Change in Healthcare. *The 14th PErvasive Technologies Related to Assistive Environments Conference*, 544–549. https://doi.org/10.1145/3453892.3461622

[16] Cellier, L., & Ghernaouti, S. (2019). An interdisciplinary approach for security, privacy and trust in the electronic medical record: A pragmatic legal perspective. *IEEE International Conference on E-Health Networking, Application & Services (HealthCom)*. https://doi.org/10.1109/HealthCom46333.2019.9009588

[17] Connolly, L., & Lang, M. (2012). Investigation of cultural aspects within information systems security research. *In IEEE International Conference for Internet Technology and Secured Transactions*, 105-111.

[18] Da Veiga, A., & Martins, N. (2015a). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162–176. https://doi.org/10.1016/j.cose.2014.12.006

[19] Da Veiga, A., & Martins, N. (2015b). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, *31*(2), 243–256. https://doi.org/10.1016/j.clsr.2015.01.005

[20] 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. https://doi.org/10.1016/j.cose.2020.101713

[21] Desnitsky, V., Levshun, D., Chechulin, A., & Kotenko, I.V. (2016). Design technique for secure embedded devices: Application for creation of integrated cyber-physical security system. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *7*(2), 60-80.

[22] Desourdis, R. I., Collins, K. H., & Rosamilia, P. J. (2016). Human collaboration in Homeland security: Collaboration planning for day-to-day and hastily formed networks. *IEEE*

Symposium on Technologies for Homeland Security (HST), 1–8. https://doi.org/10.1109/THS.2016.7568879

[23] Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*, 101747. https://doi.org/10.1016/j.cose.2020.101747

[24] Doherty, N. F., & Tajuddin, S. T. (2018). Towards a user-centric theory of value-driven information security compliance. *Information Technology & People*, *31*(2), 348–367. https://doi.org/10.1108/ITP-08-2016-0194

[25] Dykstra, J. (2015). Essential Cybersecurity Science. *O'Reilly Media*.

[26] Gcaza, N., Von Solms, R., Grobler, M. M., & Van Vuuren, J. J. (2017). A general morphological analysis: Delineating a cyber-security culture. *Information & Computer Security*, *25*(3), 259–278. https://doi.org/10.1108/ICS-12-2015-0046

[27] Gelles, M. G. (2016). *Insider Threat: Prevention, Detection, Mitigation, and Deterrence*. Butterworth-Heinemann.

[28] Glaspie, H. W., & Karwowski, W. (2018). Human Factors in Information Security Culture: A Literature Review. *In D. Nicholson (Ed.), Advances in Human Factors in Cybersecurity*, *593*, 269–280. https://doi.org/10.1007/978-3-319-60585-2_25

[29] Hassan, N. H., Ismail, Z., & Maarop, N. (2013). A conceptual model for knowledge sharing towards information security culture in healthcare organization. *International Conference on Research and Innovation in Information Systems (ICRIIS)*, 516–520. https://doi.org/10.1109/ICRIIS.2013.6716762

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

[31] Hofstede, G. (1983). The Cultural Relativity of Organizational Practices and Theories. *Journal of International Business Studies*, *14*(2), 75–89. https://doi.org/10.1057/palgrave.jibs.8490867

[32] Hussain, A., Mohamed, A., & Razali, S. (2020). A Review on Cybersecurity: Challenges & Emerging Threats. *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, 1–7. https://doi.org/10.1145/3386723.3387847

[33] Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination. *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–4. https://doi.org/10.1109/CyberSecPODS.2019.8885240

[34] Ismail, W. B. W., Widyarto, S., Adiyarta, K., Syafrullah, M., & Tajuddin, L. M. (2022). An Information Security Policy Development Process in Higher Education Institution: A Case Study Approach. *In 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 147–152. https://doi.org/10.23919/EECSI56542.2022.9946593

[35] Jonathan, G. M., Hailemariam, K. S., Gebremeskel, B. K., & Yalew, S. D. (2021). Public Sector Digital Transformation: Challenges for Information Technology Leaders. *In IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 1027–1033. https://doi.org/10.1109/IEMCON53756.2021.9623161

[36] Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review. *IEEE Access*, *9*, 99339–99363. https://doi.org/10.1109/ACCESS.2021.3097144

[37] Karjalainen, M., Siponen, M., & Sarker, S. (2020). Toward a stage theory of the development of employees' information security behavior. *Computers & Security*, *93*, 101782. https://doi.org/10.1016/j.cose.2020.101782

[38] Kitchenham, B. (2004). *Procedures for Performing Systematic Reviews* (TR/SE-0401). Keele University.

[39] Kitchenham, B., & Brereton, P. (2013). A systematic review of systematic review process research in software engineering. *Information and Software Technology*, *55*(12), 2049–2075. https://doi.org/10.1016/j.infsof.2013.07.010

[40] Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber security awareness and education in SA. *South African Computer Journal*, *52*. https://doi.org/10.18489/sacj.v52i0.201

[41] Lehto, M., & Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, *30*(3), 139–148. https://doi.org/10.1080/19393555.2020.1813851

[42] Ma, X. (2022). Is professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management*, *59*(1), 102744. https://doi.org/10.1016/j.ipm.2021.102744

[43] Mansol, N. H., Alwi, N. H. M., & Ismail, W. (2014). Embedding organizational culture values towards successful business continuity management (BCM) implementation. *Proceedings of the 6th International Conference on Information Technology and Multimedia*, 31–37. https://doi.org/10.1109/ICIMU.2014.7066599

[44] Mousavi, M. Z., & Kumar, S. (2019). Analysis of key Factors for Organization Information Security. *In International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, 514–518. https://doi.org/10.1109/COMITCon.2019.8862191

[45] Nasir, A., Arshah, R. A., & Ab Hamid, M. R. (2017). Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture: A Conceptual Framework. *Proceedings of the 2017 International Conference on Information System and Data Mining*, 56–60. https://doi.org/10.1145/3077584.3077593

[46] Ndife, A. N., Mensin, Y., Rakwichian, W., & Muneesawang, P. (2022). Cyber-Security Audit for Smart Grid Networks: An Optimized Detection Technique based on Bayesian Deep Learning. *Journal of Internet Services and Information Security*, *12*(2), 95-114.

[47] Norman, A. A., & Yasin, N. M. (2013). *Information Systems Security Management (ISSM) Success Factor: Retrospection from the Scholars*.

[48] OAS. (2018). *Critical Infrastructure Protection Report Latin America and the Caribbean 2018*. Organization of American States.

[49] Obradovich, N., Özak, Ö., Martín, I., Ortuño-Ortín, I., Awad, E., Cebrián, M., & Cuevas, Á. (2022). Expanding the measurement of culture with a sample of two billion humans. *Journal of the Royal Society Interface*, *19*(190), 20220085. https://doi.org/10.1098/rsif.2022.0085

[50] Oleksandr, K., Viktoriya, G., Nataliia, A., Liliya, F., Oleh, O., Maksym, M. (2024). Enhancing Economic Security through Digital Transformation in Investment Processes: Theoretical Perspectives and Methodological Approaches Integrating Environmental Sustainability. *Natural and Engineering Sciences*, *9*(1), 26-45.

[51] Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures. *ACM Transactions on Management Information Systems*, *12*(2), 1–29. https://doi.org/10.1145/3424282

[52] Pietruszka-Ortyl, A., Ćwiek, M., Ziębicki, B., & Wójcik-Karpacz, A. (2021). Organizational Culture as a Prerequisite for Knowledge Transfer among IT Professionals: The Case of Energy Companies. *Energies*, *14*(23), 8139. https://doi.org/10.3390/en14238139

[53] Ramachandran, S., Rao, C., Goles, T., & Dhillon, G. (2013). Variations in Information Security Cultures across Professions: A Qualitative Study. *Communications of the Association for Information Systems*, *33*. https://doi.org/10.17705/1CAIS.03311

[54] Reegård, K., Blackett, C., & Katta, V. (2019). The Concept of Cybersecurity Culture. *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*, 4036–4043. https://doi.org/10.3850/978-981-11-2724-3_0761-cd

[55] Romero, Á., González, M. De Las N., Segarra, M., Villena, B. M., & Rodríguez, Á. (2019). Mind the Gap: Professionalization is the Key to Strengthening Safety and Leadership in the Construction Sector. *International Journal of Environmental Research and Public Health*, *16*(11), 2045. https://doi.org/10.3390/ijerph16112045

[56] S. Creese, P. E. G., W. H. Dutton, & Shillair, R. (2021). Cybersecurity capacity-building: Cross-national benefits and international divides. *Journal of Cyber Policy*, *6*(2), 214–235. https://doi.org/10.1080/23738871.2021.1979617

[57] Schein, E. H. (2004). In Organizational Culture and Leadership (3rd ed.,). John Wiley & Sons, Inc, 25–37.

[58] Shah, M. U., Iqbal, F., Rehman, U., & Hung, P. C. K. (2023). A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance. *IEEE Access*, *11*, 87970–87984. https://doi.org/10.1109/ACCESS.2023.3296580

[59] Sharma, S., & 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

[60] Siemens. (2018). Cybersecurity in the Modern Industrial World. *Harvard Business Review, Harvard Business School Publishing*.

[61] Surendar, A., Saravanakumar, V., Sindhu, S., & Arvinth, N. (2024). A Bibliometric Study of Publication- Citations in a Range of Journal Articles. *Indian Journal of Information Sources and Services*, *14*(2), 97–103. https://doi.org/10.51983/ijiss-2024.14.2.14

[62] Sutton, D. (2017). *Cyber Security A Practitioner's Guide*. BCS Learning & Development Ltd.

[63] Tolah, A., Furnell, S. M., & Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. *Computers & Security*, *108*, 102354. https://doi.org/10.1016/j.cose.2021.102354

[64] Topa, I., & Karyda, M. (2015). Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance. In S. Fischer-Hübner, C. Lambrinoudakis, & J. López (Eds.), *Trust, Privacy and Security in Digital Business*, *9264*, 169–179. https://doi.org/10.1007/978-3-319-22906-5_13

[65] Turk, Ž., García De Soto, B., Mantha, B. R. K., Maciel, A., & Georgescu, A. (2022). A systemic framework for addressing cybersecurity in construction. *Automation in Construction*, *133*, 103988. https://doi.org/10.1016/j.autcon.2021.103988

[66] Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

[67] Udayakumar, R., Joshi, A., Boomiga, S. S., & Sugumar, R. (2023). Deep Fraud Net: A Deep Learning Approach for Cyber Security and Financial Fraud Detection and Classification. *Journal of Internet Services and Information Security*, *13*(3), 138-157.

[68] Van Niekerk, J. (2014). *Understanding Information Security Culture: A Conceptual Framework*.

[69] Vashistha, A., Anderson, R., & Mare, S. (2018). Examining Security and Privacy Research in Developing Regions. *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*, 1–14. https://doi.org/10.1145/3209811.3209818

[70] Whitmarsh, L., Capstick, S., & Nash, N. (2017). Who is reducing their material consumption and why? A cross-cultural analysis of dematerialization behaviours. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *375*(2095), 20160376. https://doi.org/10.1098/rsta.2016.0376

[71] Yaseen, H., Dingley, K., & Adams, C. (2016). An empirical study of factos influencing e-commerce customers' awareness in Jordan. *International Conference on Information Society (i-Society)*, 63–67. https://doi.org/10.1109/i-Society.2016.7854175

[72] Yuryna Connolly, L., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information & Computer Security*, *25*(2), 118–136. https://doi.org/10.1108/ICS-03-2017-0013

[73] Zendehdel, M., Paim, L. H., & Delafrooz, N. (2016). The moderating effect of culture on the construct factor of perceived risk towards online shopping behaviour. *Cogent Business & Management*, *3*(1), 1223390. https://doi.org/10.1080/23311975.2016.1223390

Authors Biography

Eko Yon Handri, received a degree in cryptography from the National Crypto Institute, Bogor, Indonesia, in 2006 and a master's degree in management information systems from University of Pembangunan Nasional (UPN) "Veteran", Jakarta, Indonesia, in 2013. He is currently pursuing a Ph.D. degree in computer science at Faculty of Computer Science at University of Indonesia, Depok, Indonesia.

From 2007 to 2017, he was a Researcher in Cryptography and Information Security at National Crypto Agency, Jakarta, Indonesia. He was appointed as a structural official in charge of Public Key Infrastructure, Vulnerability Identification and Risk Assessment, and Cybersecurity Maturity from 2018 to 2020. In 2021, he returned as a Researcher in Cybersecurity. His research interests include cryptography, information and data security, cybersecurity, and e-government.

Dana Indra Sensuse, received the Master's degree in Information Studies from Dalhousie University, Canada, in 1994, and a Ph.D. degree in Information Studies from the University of Toronto, Canada, in 2004. He has been a Lecturer with University of Indonesia (UI) where he has been a Professor of Computer Science since 2021. He is a prolific author, with more than 400 journals and conference papers. His research interests include e-government, smart cities, e-commerce/e-business, IT governments, information systems, data mining, knowledge management, and IT plans.

Sofian Lusa, received the Master's degree in Computer Science from Universitas Budi Luhur, Indonesia and a Ph.D. degree in Computer Science from the Universitas Indonesia, Indonesia, in 2015. He has been a Lecturer since the last 18 years beside his business activities, at Faculty of Computer science of Universitas Indonesia and Trisakti University. He has more than 20 years experience as business practitioners, He is actively involved in developing organizations such as Vice Chairman of Indonesian E-Commerce Association (IdEA), E-Commerce Division Head at Indonesian Telecommunication Society (MASTEL), Vice Chairman at KADIN Babel, and General secretary at IKAL Lemhannas.