Cultural Influences on Human Cybersecurity Behaviour: A Study of Switzerland and Cameroon

Franka Ebob Enow Ebai[1][0009-0007-5921-4862], Simon Eyongabane Ako[2] [0000-0002-3504-7939], Bettina Schneider[1][0000-0001-8460-3658], George Fonkeng Epah[2], Gaius Ngong Mufua[2], Willibroad Abongwa Acho[2], Williams Boma[2], Williams Boma[2], Delbert Akom Afumbom[2], Veronica Ika K. Visemih[2], Samuel Nemkul Lackbuin[2] and Mary Feh[2]

[1] University of Applied Sciences and Arts Northwestern Switzerland, Basel, Switzerland
[2] Biaka University of Buea, Cameroon

Abstract. Culture—be it national or organizational culture—shapes the behaviour, mindset and decision-making of individuals. Since human behaviour is considered the most vulnerable link in the security chain, it is worth examining the relationship between culture and human behaviour in the field of cybersecurity. This paper examines culture as a fundamental element of cybersecurity, highlighting its impact on security awareness, decision-making, and risk perception. Specifically, we explore how national and organisational culture shape cybersecurity practices in cross-cultural contexts. Using a qualitative approach, we conduct episodic and focus group interviews with cybersecurity professionals, educators, Chief Security Officers, and students from diverse educational backgrounds in Switzerland and Cameroon. Our findings reveal that cultural dimensions such as power distance, individualism, and uncertainty avoidance significantly influence cybersecurity behaviour. This study expands the body of literature on culture and individual cybersecurity behaviour and provides new, practical implications for integrating culture into cybersecurity training in educational institutions and organisations.

Keywords: Cross-cultural Contexts, Culture, Human Cybersecurity Behaviour

1 Introduction

Security risks transcend borders affecting both developed and developing countries. Evidence of this includes such attacks as the WannaCry Ransomware and the NotPetya attacks that occurred in 2017. These cyber-attacks impacted multiple organisations in countries around the globe [1]. About 88% of data breaches are caused by employees' mistakes, and humans are termed the weakest link in the security chain [2]. Although often ignored, authors such as [3] and [4] have highlighted the importance of human factors in cybersecurity. Risky cybersecurity behaviour has been linked to human traits such as internet addiction and a dismissive attitude to threats [3] as well as time pressure [4].

This is a preprint version. The final version will be published in:
Corradini, F.; Hinkelmann, K.; Re, B., Smuts, H., eds. (2025). Proceedings of the 5th Conference Society 5.0 - Co-Existence Between Human Being and Machine Being. Springer CCIS. San Benedetto del Tronto, Italy, 25-27 June 2025.

Considering the role of human behaviour in data breaches, it is important to examine how one's cultural background and/or the culture of their work environment influences human action in relation to cybersecurity. This is particularly relevant because cultural background, also referred to as national culture, influences an individual's way of life and decision-making process [5]. Similarly, organisational culture also shapes individuals' behaviour as it comprises a system of shared values that define what is important and shared norms that guide appropriate attitudes and behaviours [6].

While researchers continue to explore the role of human behaviour in cybersecurity, the influence of culture—both national and organisational—on cybersecurity behaviour remains underexamined. Some existing studies [7] and [8] have emphasised the importance of fostering a cybersecurity culture within organisations. However, culture-specific elements, stemming from the organisational environment and national culture, that influence human cybersecurity behaviour remain largely unexplored. Therefore, the gap we aim to address lies in understanding how cultural-specific factors—both at the organisational and national levels—shape human cybersecurity behaviour.

We therefore address two main research objectives: 1) To investigate the role of national culture in human cybersecurity behaviour in Switzerland and in Cameroon. 2) To investigate the role of organisational culture in human cybersecurity behaviour in Switzerland and in Cameroon. Our findings will be valuable for cybersecurity practitioners across government, education, and industry, enabling them to adapt cybersecurity policies and training for students and workers. Our aim is not to compare Switzerland and Cameroon in terms of which country is better regarding cybersecurity. Rather, we seek to identify key cultural contexts from both countries that influence human cybersecurity behaviour. Therefore, we focus specifically on the cultural and organisational contexts of the two countries.

In the next sections, we present our theoretical framework, literature review, methodology, discuss key findings and conclude.

2 Theoretical Framework and Literature Review

2.1 Theoretical Framework

To research cultural factors impacting individual cybersecurity behaviour, we primarily focused on Hofstede's Cultural Dimensions as the basis for our work. Although we also drew slightly on the Iceberg Theory of Culture to identify key elements that define organisational culture, our overall aim was to link the identified national and organisational elements to Hofstede's cultural dimensions.

Referring to the Iceberg theory, the larger portion of an organisation's culture – about 90%, is hidden [9]. This includes core values, customs, beliefs, and assumptions, while the remaining 10% forms the visible part, such as, greetings, music and dress code. The elements were explored through our conducted interviews.

Hofstede Cultural Dimensions: Cameroon and Switzerland. Here, we primarily illustrate how the two countries differ culturally, reinforcing our aim to understand how

national culture might influence human cybersecurity behaviour. These differences can be examined through the following dimensions: *Power distance, Individualism, Uncertainty avoidance, long term orientation, and indulgence.* Due to Cameroon not being among the investigated countries in Hofstede's original study, we mainly relied on the study of [10] and [11] to draw some cultural aspects of Cameroon.

Power Distance (PDI). Switzerland is a low-power distance society [12]. There is a belief in minimizing inequality among people. Power within organizations is decentralized, with employees expecting to be consulted and managers relying on the experience of their employees. Cameroon has a score of 54 for PDI [10], which is lower than coutries in West Africa but higher than of Western nations like Germany and USA with lower PDI scores.

Individualism (IDV). Switzerland is classified as an "I" society. Individuals prioritize taking care of themselves and their immediate social circles [12]. Meanwhile, Cameroon is a collective society [10]. In such a society, people are integrated into strong, cohesive in-groups from birth [13].

Uncertainty Avoidance (UAI). In Switzerland, the French-speaking strongly prefers rigid rules and structured environments than the German-speaking region [12]. Similarly, the Cameroonian society prefers avoiding uncertainty [11]. Managers in the country do not like ambiguous conditions. However, this finding is contradicted by [10], who found that Cameroon has low uncertainty avoidance, implying that the society tolerates uncertainty.

Long Term vs. Short-Term Orientation. In Switzerland, there is a preference for traditional cultures and norms that emphasize long-standing values and practices. Cameroon, on the other hand, leans towards short term orientation relative to other African countries. This demonstrates that society is present-oriented with a focus on quick results [10].

Indulgence. In Switzerland, people have a strong willingness to enjoy life, a positive attitude and a high value for leisure activities. Meanwhile, Cameroon values moderate restraint due to social norms [10].

2.2 Literature Review

Guided by the theoretical framework, we conducted a literature review on the impact of culture on cybersecurity, considering both national and organisational contexts.

The Role of National Culture in Cybersecurity. Hofstede's Cultural Dimensions have mainly been related to a countries' cybersecurity development (for instance, [14]; [15]; [16]), individuals' cybersecurity behaviour and privacy (for instance, [17]; [18]; [19]). Referring to the level of cybersecurity development, countries associated with low power distance, low uncertainty avoidance, high individualism, high long-term

orientation and high masculinity show a high level of cybersecurity development based on the analysis of global cybersecurity index of 2015 [14].

Countries linked to short term orientation tend to pay less attention to their long-term security. Hence, they demonstrate low level of cybersecurity maturity [15]. Cybersecurity maturity is also lower in high power distance countries due to heavy reliance on the leaders to ensure security. Meanwhile, people in individualistic society lean towards keeping their online identities private.

Further, surveying over 4'650 people, consisting of Chief Information Security Officers (CISOs), Chief Security Officers, and Chief Technology Officers (CTOs) in various business regions revealed that an individual's intention to comply with security policies positively correlates with masculinity, power distance, and long-term orientation [17]. On the other hand, research investigations in Ghana and USA showed that uncertainty avoidance played a significant role in individuals' security behavioural intention relative to individualism and collectivism. That is, people from cultures with high uncertainty avoidance express high discomfort when faced with unfamiliar risks. They also have high levels of self-efficacy, and they perceive risk-mitigation costs to be lower [18]. While individuals from collectivist societies perceive response cost to avoid risks to be lower.

The Role of Organisational Culture in Cybersecurity. Robust top management commitment, proficient IT personnel, and regular training ensure an organisation's cybersecurity readiness [20]. Including cybersecurity considerations into business strategies as well as security professionals in decision-making processes enhance cybersecurity behaviour in organisations [8]. Additionally, the involvement of leadership in security topics and processes lures employees to positively react to security measures and enhances their cognitive understanding in cybersecurity management [21]. Contrarily, [22] found no significant link between top management commitment to security and employees' security compliance.

Fostering a pro-security culture within organisations also positively influences cybersecurity behaviour [8]. Organisational culture also positively correlates with security culture and information security awareness. Individuals in organisations with a stronger security culture are likely to demonstrate more security awareness [7]. Community, a component of security, is one of the positive influences on employees' security compliance behaviour [22]. While aspects such as rule-orientation was found to not impact employees' compliance attitude.

Our literature review revealed that there is still room to apply Hofstede's cultural dimensions to the analysis of national and organizational culture in the context of human cybersecurity development. Only a few studies have applied this framework in relation to country-level cybersecurity development, particularly considering a European and an African country. Past studies have also overlooked the role of broader organisational culture—beyond security-specific initiatives—including implicit factors like norms and branding. These gaps justify our aim to explore these cultural influences and connect them to Hofstede's theory.

3 Methodology and Data Collection

To develop a theory in an under-researched area, we adopted a qualitative approach, gathering data through episodic interviews and focus groups. Additionally, we employed a cross-sectional research design, collecting data at a single point in time [23].

The episodic interview is a combination of narrative interviews and semi-structure interviews [24, p. 208]. The method enables research participants to present their experiences in a general, comparative form [25, p. 2]. Following the example of [24, p. 289], we started by asking a generative narrative question aimed at stimulating the interviewee's narrative, then listened attentively and guided the interviewee to certain scenarios where need be.

Focus group interviews refer to "*group discussion that gathers together people from similar backgrounds or experiences to discuss a specific topic of interest to the researcher"* [26]. This interviewing method is suitable for sensitive topics [27] , and is therefore well-suited for our study which touches on culture. Following the method of [26], after welcoming the participants, we introduced the interviewing team, explained the purpose of the study, and how the focus group discussion will be done. Then we led with an ice breaker question – for example, *what comes to your mind when they hear of cybersecurity?* Next, we asked the questions in our interview guide without disrupting the flow of the discussion.

We chose our interview participants through purposive sampling strategy. That is, sampled cases of participants ought to be relevant to the research question [28, p. 418]. In this light, we chose participants based on their field of work and field of study in Switzerland and Cameroon.

Nine episodic interviews were conducted in Switzerland via Zoom, while six in-person episodic interviews took place in Cameroon. The participants included cybersecurity teachers, specialists, CTOs and general employees. Two focus group discussions were held in Cameroon: one with five ICT and Engineering students and another with eight students from various backgrounds, including business, nursing, and education. In Switzerland, we primarily conducted one focus group with five Business Information Systems students. A second focus group was planned but was not conducted due to time constraints and difficulty in reaching students from various fields.

To analyse our data, we applied both the In-vivo and descriptive coding methods, as elaborated by [29, p. 74]. First, we captured short phrases or words in the participants' own language to highlight their individual voices. These formed our first-level codes. Next, we summarized the data into a word or short phrase to create second-level codes, applying the descriptive coding method [29]. This approach allowed us to draw connections between these codes and make comparisons.

4 Main Findings

We present key findings from our qualitative study in Switzerland and Cameroon. A summary of the main findings is also displayed in Table 2 below.

4.1 The Role of National Culture in Human Cybersecurity Behaviour

The Perspective of Interviewees in Switzerland. Perspectives of the interviewees in Switzerland unravelled such national cultural elements geographical and personal contexts, regulatory influences, attitude to trust and privacy, and fear of the unknown.

Starting with **geographical and background contexts**, a few interviewees explained that people based in countries with strong cybersecurity development will demonstrate higher cybersecurity awareness than those in countries with a lower level of cybersecurity development. Additionally, people's upbringing, such as their attitude towards work and self-discipline, can influence how they approach cybersecurity.

Secondly, all interviewees pointed to the **influence of rules or power distance** on cybersecurity behaviour. Some stated that in certain countries, cybersecurity policies should be enforced more strictly to influence people's behaviour. The state plays a central role in such cases. In cultures with high respect for authority, people are more likely to strictly follow established guidelines and may hesitate to speak up, even when they notice something suspicious.

Furthermore, **trust** emerged as a cultural element that influences how people from certain cultures approach cybersecurity and can be exploited by hackers. One interview participant pointed out that some Swiss may easily trust others because they live in a generally safe country.

Moreover, another cultural element **concerns people's knowledge and approach to privacy**. Some interviewees mentioned that data privacy awareness positively affects cybersecurity behaviour. However, one argued that privacy concerns and the tendency to avoid sharing, such as information about experiences with cyberattacks, could hinder the development of a solid cybersecurity culture. Similarly, individuals from cultures that prioritize privacy, and restraint may overlook cyber threats originating from a more collectivist perspective

Finally, people's **attitude towards the unknown** was mentioned by half of the total interviewees. They explained that individuals who tend to enjoy the moment or are open to taking risks may fall prey to scams. On this point regarding the unknown, one participant explained how their Swiss employees would question policies, while employees from other cultures tend to accept the same policies without resistance.

The Perspective of Interviewees in Cameroon. Our analysis showed that cultural elements influencing human cybersecurity behaviour include cultural vulnerability, religious beliefs, attitude toward sharing, resistance to change, policy and governance, and trust. In terms of cultural vulnerability, some interviewees mentioned that the lack of cybersecurity resources in local languages negatively impacts people's cybersecurity behaviour.

Regarding **religious beliefs**, some interviewees stated that some Cameroonians may believe their faith can shield them from digital harm, prompting less caution online. This belief also connects to the **attitude towards sharing**. The act of sharing links, such as Christian messages via WhatsApp, can inadvertently expose people to social engineering attacks. On another note, three interviewees explained that some

communities can become more resilient against cyberattacks by sharing collective knowledge and experiences. Meanwhile, negative cybersecurity behaviour can arise when individuals prioritize personal needs over the safety of the community, potentially compromising collective security in favour of individual convenience.

Another argument was linked to Cameroon's **lack of comprehensive frameworks and policies**, which results in people not taking cybersecurity seriously in the country. This leads to cybersecurity vulnerabilities, particularly in rural areas. Finally, **trust** was also identified as a cultural element by many Cameroonian interviewees. A few interviewees mentioned that Cameroonians have a mindset of blind trust in authorities, making them more susceptible to cyberattacks.

4.2 The Role of Organisational Culture in Human Cybersecurity Behaviour

The Perspective of Interviewees in Switzerland. Some identified organisational cultural elements include communication style & transparency, authority and Hierarchy, work-related factors and training or skill development. First, some interviewees argued that open **communication and transparency** would enable employees to understand what is happening in other sectors of the company, including the organisation's stance on security. Concerning **hierarchy,** most interviewees in Switzerland highlighted that lower-level employees in highly hierarchical organisations may become overly dependent on leaders for cybersecurity-related decisions. The perspectives of such employees may also be overlooked, or they may act against their own judgement to please their superiors.

Moreover, having **clear objectives** beyond just a vision can positively influence people's cybersecurity behaviour. Clear cybersecurity objectives help establish the organisation's stance and set expectations for both employees and customers.
Lastly, in terms of **work pressure**, some interviewees noted that employees may pay less attention to security measures when under high pressure or dealing with excessive workloads. Additionally, employees in certain departments may be more likely to click on phishing links than those in other departments due to the nature of their work.

The Perspective of Interviewees in Cameroon. From this side, we saw factors like the organisational environment, policy and governance, training and awareness, company structure and vision, and work pressure. Referring to the **organisational environment**, some of our interviewed cybersecurity experts revealed that many Cameroonian companies lack a cybersecurity culture, with security-related policies either absent or not effectively implemented. Additionally, envy and jealousy among employees in the workplace can lead them to deliberately violate some of the organisation's security procedures.

Regarding **training and awareness**, most organisations do not prioritise cybersecurity education. Furthermore, proactive practices such as frequent password changes are often neglected. **Company structure and vision** were also identified as cultural factors by some interviewees. The use of a top-down approach can discourage lower-level

employees from actively participating in cybersecurity matters, as they may feel that their opinions are not valued.

Lastly, some interviewees highlighted employees' **poor digital mindset** and lack of interest in cybersecurity. For instance, some staff do not fully understand the significance of web cookies and occasionally grant strangers access to their machines, increasing the risk of cybersecurity intrusions.

Table 1. Summary of Main Findings

Cultural Factors Influencing Individual Cybersecurity Behaviour from **Empirical Study**		
	National	**Organisational**
Switzerland	• Influence of geographical contexts • Influence of rules • Attitude towards trust • Attitude towards privacy • Attitude towards uncertainty	• Influence of communication • Influence of hierarchy • Influence of clear objective • Influence of work pressure
Cameroon	• People's religious beliefs • Attitude towards sharing • Lack of cybersecurity frameworks	• Influence of work environment • Influence of security training • Influence of company vision • Poor digital mindset

5 Discussion and Implications

When linking perspectives from Cameroon and Switzerland on the influence of national culture, several common elements emerged, including state regulatory influences, attitudes toward trust and sharing, and fear of the unknown. Both sides emphasised the pivotal role of the government in shaping people's cybersecurity behaviour, particularly in high power distance cultures. The presence of cybersecurity policies and their stringent enforcement can drive positive cybersecurity practices.

The identified factor of trust aligns with the study by [30], which concluded that people's trust is often rooted in their cultural backgrounds and can lead to risky cybersecurity behaviour. Additionally, sharing experiences of cyberattacks fosters a stronger cybersecurity culture, but individuals must remain cautious of blind trust.

The relationship between collectivism and cybersecurity behaviour contradicts the findings of [15], who argued that high individualism is positively related to a country's cybersecurity maturity. However, a few interviewees in Switzerland also supported this perspective.

Lastly, fear of the unknown or uncertainty avoidance was a common theme among interviewees from both countries. However, its impact on cybersecurity behaviour depends on how individuals respond. When people question new rules due to their unfamiliarity, they are less likely to fall victim to cyberattacks. Conversely, when individuals entirely avoid new rules or technologies—including cybersecurity measures—due to unfamiliarity, they may increase their exposure to cyber threats.

Turning to organisational cultural elements, key points highlighted by both interview groups included authority and hierarchy, training, objectives, and vision. Like the findings of [15], strong hierarchical structures within organisations can negatively impact employees' cybersecurity behaviour, leading to over-reliance on leaders for decision-making.

In line with [20], our findings suggest that regular cybersecurity training positively influences cybersecurity behaviour. Conversely, the absence of such training leaves employees unable to recognise cyber threats, making them more vulnerable to attacks.

Lastly, having a clear vision and cybersecurity objectives, particularly in highly hierarchical companies, plays a crucial role in steering employees toward positive cybersecurity behaviour. When cybersecurity goals are well-defined, employees are more likely to understand their role in maintaining security within the organisation.

6 Conclusion and Outlook

By synthesising perspectives from Switzerland and Cameroon, this study has highlighted cultural elements that influence human cybersecurity behaviour, considering both national and organisational culture. Additionally, we have successfully linked cybersecurity behaviour to Hofstede's cultural dimensions, an aspect that has been largely overlooked in previous studies.

Still, our study has some limitations. First, the findings are based solely on qualitative interviews, which, while insightful, are inherently subjective and may introduce bias. Second, our interviewees were primarily drawn from specific regions, namely the German-speaking part of Switzerland and the English-speaking region of Cameroon, limiting broader generalisability.

For future research, we recommend exploring the same topic using a quantitative approach to validate our findings on a larger scale. Further studies could also focus on implicit organisational cultural elements that influence cybersecurity behaviour. Additionally, conducting quantitative surveys with participants from diverse regions across Cameroon and Switzerland would provide a more comprehensive perspective on the cultural factors affecting cybersecurity practices.

Acknowledgements. This study was carried out as part of a project funded by the Leading House (LH) Africa Consolidation Grant 2023.

References

1. SentinelOne, “Cybersecurity's Defining Moments: 7 lessons from History's ost Infamous Breaches,” 9 January 2024. [Online]. Available: https://www.sentinelone.com/blog/cybersecuritys-defining-moments-7-lessons-from-historys-most-infamous-breaches/. [Accessed 26 May 2024].
2. J. Hancock, “Psychology of Human ErrorUnderstand the mistakes that compromise your company’s cybersecurity," Tessian Research., 2020.
3. L. Hadlington, “Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours,” Heliyon, vol. 3, 2017.
4. N. H. Chowdhury, M. T. Adam and T. Teubner, “Time pressure in human cybersecurity behaviour: Theoretical framework and countermeasures,” Computers & Sceurity, 2020.
5. W. Delanoy, “What Is Culture?,” in The Cambridge Handbook of Interculsotural Communication. Cambridge Handbooks in Language and Linguistics, Cambrigde University Press, 2020, pp. 17-34.
6. J. A. Chatman and S. E. Cha, “Leading by Leveraging Culture,” California Review Management, vol. XLV, no. 4, 2003.
7. A. Wiley, A. McCormac and D. Calic, “More than the individual: Examining the relationship between culture and Information Security Awareness,” Computers & Security, vol. 88, 2020.
8. W. Yeoh, S. c. Wang, A. Popovi and N. H. Chowdhury, A Systematic Synthesis of Critical Success Factors for Cybersecurity, Computers & Security, 2022.
9. E. T. Hall, Beyong Culture, New York: Knopf Doubleday Publishing Group, 1976.
10. C. Barczyk, C. Rarick and G. Winter, “An Exploratory Study of the Cultural Values of Cameroon’s Young, Elite, Urban Population: Implications for Management and International Business,” Journal of Business Diversity, pp. 11-25, 2021.
11. R. Djamen, L. Georges and P. jean-louis, “Understanding the cultural values at the individual level in central africa: A test of the CVSCALE in cameroon," in *International Conference on Advanced Marketing*, 2017.The Culture Factor, “Country Comparison Tool,” 2024. [Online]. Available: https://www.hofstede-insights.com/country-comparison-tool?countries=switzerland. [Accessed 18 June 2024].
12. The Culture Factor, “Country Comparison Tool,” 2024. [Online]. Available: https://www.hofstede-insights.com/country-comparison-tool?countries=switzerland. [Accessed 18 June 2024].
13. G. Hofstede, G. J. Hofstede and M. Minkov, Cultures and Organisations: Software of the Mind, The McGraw Hill Companies, 2010.
14. A. Onumo, A. Cullen and I. Ullah-Awan, “An Empirical Study of Cultural Dimensions and Cybersecurity Development,” in IEEE 5th International Conference on Future Internet of Things and Cloud, 2017.
15. J. J. Jeong, M. Chamikara, M. Grobler and C. Rudolph, “Fuzzy Logic Application to Link National Culture and Cybersecurity Maturity,” in *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)* , 2019.
16. S. Creese, W. H. Dutton and P. Esteve-González, “The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions,” Personal and Ubiquitous Computing, pp. 941-955, 2021.
17. G. Crespos-Pérez, “Factors that influence the cybersecurity behaviour: A cross-cultural study, Gurabo, Puerto Rico: Universidad Ana G Méndez-Gurabo, 2021.

18. R. E. Crossler, F. Kofi, Andoh-Baidoo and P. Menard, “Espoused cultural values as antecedents of individuals’ threat and coping appraisal toward protective information technologies: Study of U.S. and Ghana,” Information & Management, pp. 754- 766, 2019.
19. T. Halevi, N. Memom, J. Lewis, P. Kumaraguru, S. Arora, N. Dagar, F. Aloul and J. Chen, “Cultural and Psychological Factors in Cyber-Security,” in Proceedings of the 18th International Conference on Information Integration and Web-based Application and Services, 2016.
20. S. Hasan, M. Ali, S. Kurnia and R. Thurasamy, “Evaluating the cyber security readiness of organizations and its influence on performance,” Jornal of Information Security and Applications, vol. LVIII, 2021.
21. A. Onumo, I. Ullah-Awan and A. Cullen, “Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures,” ACM Transactions on Management Information Systems, vol. 12, no. 2, pp. 1-29, 2021.
22. G. Solomon and I. Brown, “The influence of organisational culture and information security culture on employee compliance behaviour,” Journal of Enterprise Information Management, 2020.
23. E. Bell, A. Bryman and B. Harley, Business Research Methods, Oxford: Oxford University Press., 2022.
24. U. Flick, An Introduction to Qualitative Research, 6th ed., Sage Publications, 2018.
25. R. A. Mueller, “Episodic Narrative Interview: Capturing Stories of Experience with a Methods Fusion.,” International Journal of Qualitative Methods, pp. 1-11, 2019.
26. S. Dawson, L. Manderson and V. L. Tallo, “A Manual for the Use of Focus Groups. A Boston: International Nutrition Foundation for Developing Countries (INFDC).," in *A manual for the use of focus groups/Susan Dawson and Lenore Manderson and Veronica L. Tallo.*, 1993.
27. R. Barbour, “Introducing focus groups,” in Doing Focus Groups, SAGE Publications Ltd, 2018, pp. 1-14.
28. A. Bryman, Social Research Methods, 4th ed., New York: Oxford University Press, 2012.
29. M. Miles, A. M. Huberman and J. S. Saldana, Qualitative Data Analysis: A Methods Sourcebook, 3rd ed., London: Sage Publications Inc., 2014.
30. I. Alhasan, “Human Factors in Cybersecurity: A Cross-Cultural Study on Trust. Doctoral dissertation,” Purdue University Graduate School, 2023.