Exploring the Relationship Between Digital Literacy and Information Security Culture Toward IR 4.0 Among Administrative and Diplomatic Officers (ADO) in Malaysia

Mohd Sharulnizam Kamarulzaman[1], Shamila Mohamed Shuhidan[2*], Khalid Abdul Wahid[3], Amirudin Abdul Wahab[4], Abdul Jalil Tohara[5]

[1,2]School of Information Science, College of Computing, Informatics, and Mathematics, Al-Khawarizmi Building, Universiti Teknologi MARA, 40450 Shah Alam Selangor Darul Ehsan, Selangor, Malaysia
[3]Universiti Teknologi MARA Cawangan Kelantan, Bukit Ilmu, 18500 Machang, Kelantan, Malaysia
[4]Cybersecurity Malaysia, Level 4, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor, Malaysia
[5]Bahagian Pembangunan Kurikulum Kementerian Pendidikan Malaysia, Aras 4-8, Blok E9, Kompleks Kerajaan Parcel E, Pusat Pentadbiran Kerajaan Persekutuan, Presint 1, 62000 Putrajaya
shamila@uitm.edu.my

Abstract. The advent of Industry 4.0 (IR4.0) is significantly influencing employment sectors. Prior studies conducted in Malaysia indicate that the readiness of employees to embrace IR4.0 is affected by shifts in the environment, consumer behavior, and employee performance, while technological factors have lower compatibility. This stands in opposition to the process of transformation which demands a significant level of digital literacy from employees, as they must engage with and independently make decisions using these advanced technological tools. Therefore, the objective of this study is to investigate the correlation between digital literacy and information security culture among Administrative and Diplomatic Officers (ADO) in Malaysia. This study is also related to the goals of Thrusts 1 and 6 of the Malaysian Digital Economy Blueprint. These goals aim to improve the digital literacy of government employees at all levels, with the objective of creating reliable, secure, and ethically sound digital environments that promote a strong culture of information security. A survey questionnaire used to evaluate the correlation between the variables. Using SmartPLS for data analysis, it was found that three hypotheses were supported. Significant correlations are observed between information security culture and the technical (t-1.674, $p < 0.047$); cognitive (t-2.879, $p < 0.002$); and social emotional (t-5.300, $p < 0.000$) variables. The purpose of the research is to improve the digital literacy of organisation employees, thereby enhancing the organization's information security culture. Consequently, it will enhance the alignment between the DL competence framework and the information security culture of Malaysian employees.

N. A. S. Abdullah et al. (eds.),*Proceedings of the International Conference on Innovation & Entrepreneurship in Computing, Engineering & Science Education (InvENT 2024)*, Advances in Computer Science Research 117,
https://doi.org/10.2991/978-94-6463-589-8_57

Furthermore, this information will furnish the government, policymakers, and organisations with valuable insights regarding the deficiencies that hinder the realisation of the Mydigital Initiative's objective of equipping all civil servants with digital literacy by 2025.

Keywords: Information security culture, digital literacy skills, information security behavior, information management

1 Introduction

In recent decades, Malaysia has embraced the digital age through the growth of Information and Communication Technologies (ICT). The adoption of technologies like social media, mobile devices, Internet of Things (IoT), Big Data, cloud computing, and Artificial Intelligence (AI) has become crucial for Malaysian enterprises to advance in Industry 4.0 (Aziz, Norhashim, & Halim, 2011). However, with increased connectivity comes heightened information security risks from both internal and external threats, which can jeopardize businesses' efficiency and productivity.

As technology becomes more integrated into daily life, digital literacy has become essential for individuals to navigate technology effectively while safeguarding their data privacy and security. Organizations must view digital literacy as a continuous process to enhance employees' skills and adapt to technological advancements. Information and data handling are critical assets for any organization, emphasizing the importance of information security. To address cybersecurity challenges, Malaysia has implemented the Malaysia Cyber Security Strategy 2020-2024 to ensure information security, economic progress, and public well-being (Majlis Keselamatan Negara (MKN) 2020). Collaboration among government agencies, enterprises, and the public is essential to strengthen security measures and risk mitigation strategies. Moreover, there is a growing need for a top-down approach involving all Malaysian citizens to enhance national information security.

In the evolving digital landscape, individuals and organizations must prioritize knowledge and skills in information security, privacy, and intellectual property rights to achieve success. Employee awareness and commitment to information security are crucial, as individuals can be the weakest link in an organization's security architecture. (Alhogail, 2015). Companies need well-informed personnel to comply with privacy and security regulations and prevent insider threats effectively. Overall, a comprehensive approach to information security, including continuous training, policy enforcement, and regulatory compliance, is essential for organizations to navigate the complex and ever-changing landscape of data privacy, security, and intellectual property rights. (Burkell, 2015).

2 Literature Review

2.1 Information Security Culture

Information security is an integral part of our everyday life. Every aspect of our professional and private lives requires the use of information. Several organisations cannot survive without information; thus, they must take special precautions to protect their information assets (Van Niekerk and Von Solms, 2010). Every organisation must have an information security solution as a fundamental component (Nel & Drevin, 2019). Despite the emergence of technologically superior solutions, businesses continue to struggle to manage information security (Narain Singh et al., 2014). The success or failure of an organization's information system security initiatives depends on the online conduct of its personnel and the level of danger they pose. The human element is one of the most neglected parts of organisations' information system security (Nel & Drevin, 2019). Focusing on employee conduct can considerably improve the success of an organization's information system security initiatives (Da Veiga and Eloff, 2010).

2.2 Digital Literacy

Digital literacy refers to the ability to effectively use information and communication technologies (ICT) and the Internet for various purposes, such as innovation, creativity, entrepreneurship, acquiring essential information, and developing skills needed in the modern era. The Digital Competence Framework, developed by Calvani and refined by Ng, consists of three main components: cognitive, technical, and social-emotional, which collectively form the Digital Literacy Model.

Cognitive. The cognitive factor of Ng's (2012) digital literacy paradigm relates to the capacity to think critically throughout the search, assessment, and creative phases of working with digital information. Additionally, this skill involves analyzing and selecting the most appropriate applications for learning or carrying out specific tasks. This aspect of digital literacy demands familiarity with the ethical, moral, and legal difficulties involved with online commerce and content replication using digitally based resources, such as copyrights and plagiarism. The individual should understand multiliteracies (Reyna et al., 2018) and be able to decode text-based information as well as information from images, sounds, videos, maps, and models, as well as those involving multiliteracies' skills that are linguistic, audio, visual, gestural and spatial as captured in videos and multimodal as in multimedia resources. Cognitive in this research refers to an ADO's capacity to search, assess, select, and utilise suitable digital information to complete a certain work-related activity while adhering to the information security culture. Personality and cognitive differences may also impact the perception of (and propensity to take) risks. The Parsons, Kathryn, et al. (2010) research based on O'Neill (2004) argues that individuals may be categorised depending on how they cope with risk, from those who are very risk averse to those who actively seek out danger. These distinctions are expected to

impact how individuals interpret the information around them, which is likely to Influence security behaviour that reflects information security culture.

Technical. The technical aspect of digital literacy encompasses the abilities to effectively use information and communication technology (ICT) for learning and daily tasks. This includes understanding and utilizing various input and output devices like earphones, headsets, external speakers, and smartboards (Noh, 2016). Additionally, one must have knowledge of hardware components, file protection, and troubleshooting methods acquired from sources like manuals or online resources such as YouTube videos (Noh, 2016). Being digitally literate implies proficiency in technology, including tasks like understanding file structures, managing data transfers, downloading and installing apps, using mobile device connections, managing data charges, utilizing communication tools, updating user account information, and handling email communication. In the research context, the term "technical" refers to the ability of Administrative Officers (ADOs) to possess the necessary technical skills for utilizing digital tools in their work and daily activities, such as app management (Ng, 2012; Quaicoe & Pata, 2015). To thrive in the future, organizations need to adopt a comprehensive approach to information security that considers human, organizational, and technological aspects. Scholars like Yildrim (2016) emphasize that technology, people, and education are crucial components of a holistic approach, while Alhogail and Mirza (2014) highlight the importance of people, organizations, and technology in determining the success of Information Security Culture (ISC). It is essential to recognize that the effectiveness of technical security measures ultimately relies on human interaction, and employees can inadvertently pose security risks if not properly trained or guided (Kobis & Karyy, 2021). Consequently, fostering a security culture becomes vital for addressing human-related issues in information security, as highlighted by scholars like Van Niekerk and Von Solms (2010).

Social Emotional. The advent of the Internet and other digital communication platforms has created new dimensions and possibilities for collaborative learning via information-sharing and discussion groups, knowledge communities, and chat rooms, among many other forms (Johnson, 2016). However, to take advantage of these new possibilities, users require sociological and emotional abilities that allow them to "understand the rules of the game" and overcome the obstacles confronting them in the information and communication of cyberspace; by understanding the information security aspect of the cyberspace and for organizations to adapt proper information security culture. Socio-emotional literacy is a relatively new kind of digital literacy that users must learn, since it largely encompasses emotional and social components, the human aspects of functioning in information security culture. Users must possess a high level of critical thinking and analysis, along with a strong sense of maturity and proficiency in information, branching, and visual literacy (Vercruyssen et al., 2023).

3 Research Framework

This section discusses the framework that created for the study. The literature consulted to determine how the factors interacted in this study. The idea then developed to study the relationship between digital literacy toward information security culture. Digital literacy components; cognitive, technical, and social emotional constructed as independent variables (IVs) for this study. Information security culture is the attached dependent variable (DV). The structure displayed in Figure 1 below:

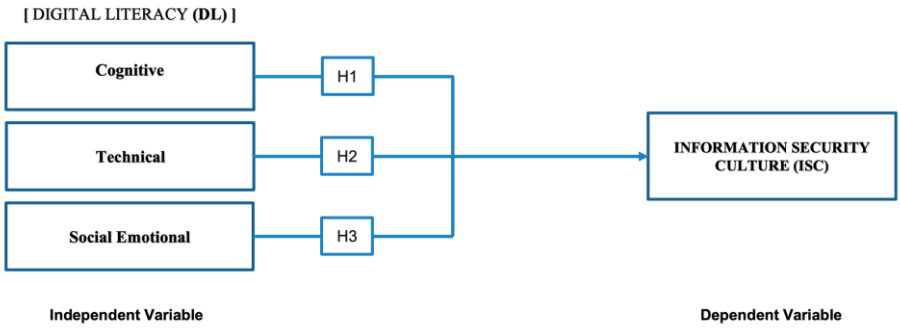

Fig. 1. Research Framework

4 Methodology

This study conducted research using quantitative methods to explore the relationship between digital literacy components and information security culture among Administrative and Diplomatic Officers (ADOs) in Malaysia. The study involved collecting data through a survey questionnaire from a sample of 405 ADOs from various government ministries to evaluate their digital literacy levels, characteristics, and attitudes towards enhancing information security culture within organizations. ADOs are crucial in managing information assets, including sensitive data, and are responsible for making important decisions related to government matters, making them vulnerable to cyber threats.

The study highlighted the lack of academic research on the influence of digital literacy on employees within organizations. The importance of leveraging real-time data during the COVID-19 pandemic to conduct research that can offer valuable insights, enhance existing policies, and better prepare for future crises was emphasized. The research employed purposive sampling to select administrative and diplomatic workers within specific grade ranges based on their cognitive abilities for survey participation. The Raosoft Calculator was used to determine a recommended sample size of 371 participants. Data collection was facilitated through Google Forms, and data preparation involved encoding, inputting data into SPSS, filtering,

and addressing missing responses. The survey data was analyzed using SPSS, with a total of 405 participants contributing responses. A thorough analysis was conducted to identify and address any missing or incorrect data. The data analysis utilized two software applications: SPSS version 29 and SmartPLS version 4 for Partial Least Squares Structural Equation Modelling.

5 Finding and Discussion

This part presents the study's conclusions regarding the demographic characteristics of the respondents, including age, gender, and the assessment of the relationship between the variables being studied.

5.1 Relationship between Digital Literacy Components – Cognitive, Technical and Social Emotional towards Information Security Culture

The relationship between variables: cognitive, technical, social emotional, and information security culture are shown in table 1. Findings of H1 show that cognitive and information security culture is supported as the cognitive aspect of digital literacy does encourage information security culture. The findings of the study have evidently show that digital literacy components which consist of critical thinking and problem-solving support information security culture. The significance of cognitive's influence on information security culture was shown in the results, where the t- values appeared to be reasonable for the relationship (t- 2.879, p = > 0.002).

Table 1. Hypothesis Testing for Direct Effect

Hypothesis	Relationship	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T - Values	P- Values	Decision
H1	Cognitive -> Information Security Culture	0.073	0.076	0.025	2.879	0.002	Supported
H2	Social Emotional -> Information Security Culture	0.195	0.203	0.037	5.300	0.000	Supported
H3	Technical -> Information Security Culture	0.039	0.041	0.023	1.674	0.047	Supported

The research conducted by Parsons, Kathryn, et al. (2010) builds upon the findings of O'Neill (2004) and suggests that individuals can be classified based on their approach to risk, ranging from extreme risk aversion to actively pursuing risky situations. These distinctions are anticipated to affect how individuals perceive the information in their surroundings, which is likely to influence their security behaviour that aligns with the culture of information security. In this research, the term "cognitive" refers to an individual's ability to effectively search for, evaluate, choose, and use appropriate

digital information to successfully carry out a certain work-related task, while also adhering to the culture of information security.

Findings of H2 show the relationship between technical and information security culture is supported. The findings of the study have evidently confirmed that technical which consist of technical skills and operational skills do influence information security culture. The significance of technical and information security culture was shown in the results, where the t- values appeared to have moderate values on the relationship (t- 1.674, $p = < 0.047$), making the topic worth to be discussed further.

An individual who possesses digital literacy is proficient at utilising technology. In this research, the term "technical" pertains to the ability of ADOs to possess the essential technical and operational skills to effectively use digital technologies for work and daily tasks, such as uploading, downloading, and installing applications (Ng, 2012; Quaicoe & Pata, 2015). Hence, in order to ensure their survival in the coming years, organisations must implement a comprehensive and all-encompassing approach to information security, which encompasses the human, organisational, and technological aspects According to Yildirim (2016), technology, people, and education are the three essential components of a comprehensive strategy. Alhogail and Mirza (2014) assert that the effectiveness of information security culture is contingent upon the significance of people, organisations, and technology. It is widely known that every technical measure, regardless of its design quality, must be utilised effectively and consistently by humans. Findings for social emotional represent the H3 naturally have a strong influence and impact on information security culture. The findings of the study have evidently confirmed that social-emotional which consists of communication and responsible does influence information security culture. The significance on information security culture was shown in the results where the t-values appeared to show strong values (t- 5.300, $p = < 0.000$).

Based on the study, social-emotional is shown as an important factor in information security culture in an organization. The emergence of the Internet and other digital communication platforms has opened new opportunities for collaborative learning through information-sharing and discussion groups, knowledge communities, and chat rooms, among other forms. However, in order to make the most of these new opportunities, users need sociological and emotional skills that enable them to comprehend the rules and overcome the challenges they face in the realm of information and communication in cyberspace. This includes understanding the importance of information security in cyberspace and organisations adopting a suitable information security culture. Eshet-Alkalai (2005) identified several skills necessary for effective digital communication. These skills encompass not only the capacity to exchange formal knowledge, but also the ability to convey emotions through digital means, discern insincere individuals in chat rooms, and navigate the internet safely by avoiding hoaxes and malicious viruses. Socio-emotional literacy is a recently developed sort of digital literacy that users need to acquire. Understanding and managing emotions and social interactions are crucial for effectively participating in information security culture. Eshet-Alkalai (2005) defines socio-emotional literacy

as the most advanced and refined form of digital literacy explored in this context. Users must possess a high level of critical thinking and analytical skills, as well as demonstrate exceptional maturity and proficiency in information processing, branching logic, and visual interpretation. (Vercruyssen et al., 2023). According to Eshet-Alkalai (2005), those who are "socio-emotionally literate" possess the ability to effectively communicate with others, analyse information, engage in abstract thinking, and generate new knowledge within the realm of information security.

6 Limitation and Future Research

The research's modest population included Malaysian ministry administrative and diplomatic officers. Extrapolating the research's findings to government servant, industries, or organizations is impractical. Since many variables might affect an employee's digital literacy, subsequent study should be undertaken in other industries, at different employee levels, in other environments, and according to social hierarchy. Previous research studies have focused on digital literacy skills, thus future study may examine online employees' security practices to improve information security. This study gives perspective for the skills and unskilled employees gap. According to the research's empirical findings, having significant skills isn't enough to guarantee better security behavior. This is supported by the survey. To dramatically raise security standards, other issues must be addressed. Building and sustaining a continuous information security culture in government departments may be a larger solution. This may help remote workers understand security issues better and encourage them to take charge of their security.

7 Conclusion

Based on the measured characteristics, this study can provide suitable recommendations for a healthy ISC. In the context of this study, it is well-established that a significant concern is the level of digital literacy skills among employees, namely in the areas of cognitive, technical, and social-emotional abilities (such as reading, writing, and arithmetic). Mastering digital literacy is crucial for all individuals, as it enables effective communication and the acquisition of reliable information. Hence, the primary suggestion is to improve the competences and skills of employees to make them cyber security ready. Martins and Eloff (2002) defined information security as a collection of characteristics that an organisation values, including acceptable and unacceptable behaviours related to information security, encouraged and discouraged behaviours, cognitive skills, adaptability to changing circumstances, and the ability to recognise and respond to threats based on technical skills and knowledge of technology (Al Hogail and Mirza, 2014). Masrek (2017) also stated that for a company to foster a subculture of information security, all their actions must align with the organization's established practices for sound information security. This is crucial for instilling the information security culture. It is anticipated that the government will improve the existing framework for remote working and online

management of private information assets in organisations in order to minimise the number of information breaches that could lead to substantial problems in the organization's culture.

Acknowledgments. I would like to express my sincere appreciation to Universiti Teknologi MARA (UiTM) especially College of Computing, Informatics and Mathematics and individuals whose contributions and support have greatly enhanced the quality and rigour of this research.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers and Security, 29(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002
2. Alhogail, A. (2015), "Design and validation of information security culture framework", Computers in Human Behavior, Vol. 49, pp. 567-575, doi: 10.1016/j.chb.2015.03.054.
3. AlHogail, A., & Mirza, A. (2014). A proposal of an Organizational Information Security Culture Framework. Proceedings of International Conference on Information, Communication Technology and System (ICTS) 2014. https://doi.org/10.1109/icts.2014.7010591
4. Aziz, K. A., Norhashim, M. B., & Halim, E. M. (2011). Information security and information technology governance: A Malaysian case study. International Journal of Management Practice, 4(4), 331–344. https://doi.org/10.1504/IJMP.2011.039204
5. Burkell, J. A., Fortier, A., Di Valentino, L., & Roberts, S. (2015). Enhancing Key Digital Literacy Skills: Information Privacy, Information Security, and Copyright / Intellectual Property. FIMS Publications, 35, 67. Retrieved from https://works.bepress.com/jacquelyn.burkell/2/%0Ahttps://www.researchgate.net/publication/283551425_Enhancing_Key_Digital_Literacy_Skills_Information_Privacy_Information_Security_and_CopyrightIntellectual_Property
6. Da Veiga, A., & Eloff, J. H. P. (2010). A framework and Assessment Instrument for Information Security Culture. Computers & Security, 29(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002
7. Eshet-Alkalai (2005). Thinking skills in the digital era. In: Haward, C., Bottcher, J. V., Justice, L., Schenk, K., Rogers, P. L., Berg, G, A. (eds.) (2005). Encyclopaedia of Distance Learning, Vol. I. London, Idea Group Inc., (pp. 1840-1845).
8. Johnson, N. F. (2016). The Multiplicities of Internet Addiction. https://doi.org/10.4324/9781315555430
9. Kobis, P., & Karyy, O. (2021). Impact of the human factor on the security of information resources of enterprises during the COVID-19 pandemic. Polish Journal of Management Studies, 24(2), 210–227. https://doi.org/10.17512/pjms.2021.24.2.13
10. Majlis Keselamatan Negara(MKN). (n.d.). https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf
11. Martins, A., & Elofe, J. (2002). Information security culture. IFIP Advances in Information and Communication Technology, 203–214. https://doi.org/10.1007/978-0-387-35586-3_16

12. Narain Singh, A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "Organizational Information Security Management." Journal of Enterprise Information Management, 27(5), 644–667. https://doi.org/10.1108/jeim-07-2013-0052
13. Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. Information & Computer Security, 27(2), 146–164. https://doi.org/10.1108/ics-12-2016-0095
14. Ng, W. (2012). Can we teach digital natives digital literacy? Computers & Education, 59(3), 1065–1078. https://doi.org/10.1016/j.compedu.2012.04.016
15. Noh, Y. (2016). A study on the effect of digital literacy on information use behavior. Journal of Librarianship and Information Science, 49(1), 26–56. https://doi.org/10.1177/0961000615624527
16. Parsons, K., Mccormac, A., Butavicius, M., & Ferguson, L. (2010). Human Factors and Information Security : Individual , Culture and Security Environment. Science And Technology, (DSTO-TR-2484), 45. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf
17. Quaicoe, J. S., & Pata, K. (2015). The teachers' Digital Literacy: Determining Digital Divide in public basic schools in Ghana. Communications in Computer and Information Science, 154–162. https://doi.org/10.1007/978-3-319-28197-1_16
18. Reyna, J., Hanham, J., & Meier, P. C. (2018). A framework for digital media literacies for teaching and learning in higher education. E-Learning and Digital Media, 15(4), 176–190. https://doi.org/10.1177/2042753018784952
19. Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & Security, 29(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005
20. Vercruyssen, A., Schirmer, W., Geerts, N., & Mortelmans, D. (2023). How "BASIC" is Basic Digital Literacy for older adults? insights from Digital Skills Instructors. Frontiers in Education, 8. https://doi.org/10.3389/feduc.2023.1231701
21. Yildirim, E. (2016), "The importance of information security awareness for the success of business enterprises", Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, Florida, USA, pp. 211-222.