Available online at https://ijikm.uitm.edu.my/

e-ISSN: 2289-5337

Journal of Information and Knowledge Management (2024) Vol. 14, No. 1

Journal of Information and Knowledge Management

Content Validity of Assessment Instrument for Information Security Culture in Relation to Digital Literacy

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

[1,4]Cybersecurity Malaysia, Level 4, Tower 1, Menara Cyber Axis, Jalan Impact, 63000 Cyberjaya, Selangor, Malaysia
[1,2]School of Information Science, College of Computing, Informatics and Media, Universiti Teknologi MARA Puncak Perdana Campus, Seksyen U10, 40150, Shah Alam, Selangor, Malaysia
[3]Universiti Teknologi MARA Cawangan Kelantan, Bukit Ilmu, 18500 Machang, Kelantan, 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

ARTICLE INFO

Article history:
Received 1 January 2024
Revised 14 February 2024
Accepted 1 March 2024
Online first
Published 1 April 2024

Keywords:
content validity
information security culture
digital literacy
information management
information science

ABSTRACT

This study intends to assess the content validity of an instrument intended to measure the relationship between digital literacy and information security culture among Malaysian administrative and diplomatic officers (ADO). Throughout the process of determining the content validity of the instrument, six specialists were contacted. The item content validity index (I-CVI) and scale content validity index (S-CVI) were established for assessing content validity. The two characteristics that were discovered were security risk and security awareness, and each of them had seven and six items, respectively. On the security risk and security awareness aspects of the information security culture, the scale content validity index (S-CVI/Ave) was 0.95 and 1.00 respectively, and the item content validity index (I-CVI) ranged from 0.95 to 1.00. Both indices were consistent with a high level of reliability. It has been determined that the instrument possesses a high level of content validity. In the future, research may be conducted to ensure that the instrument's reliability and other types of validity, such as face validity, concept validity, and criteria validity, are investigated to improve the instrument's applicability.

[2*] Corresponding author. *E-mail address*: shamila@uitm.edu.my

INTRODUCTION

In recent decades, Malaysia, along with the rest of the world, has progressively become a part of the digital age due to the explosive and unprecedented growth of information and communication technologies (ICT). The Malaysians have come a long way since their first Internet adoption in 1995. For Malaysian enterprises, services, and people relevant to the Fourth Industrial Revolution, internet access is now a must for advancement (Industry 4.0). Nobody or anything is beyond the reach of internet. Companies rely extensively on democratised technologies, such as social, mobile, the Internet of Things (IoT), Big Data, hypercloud, and Artificial Intelligence (AI), which are all based on and centred on connectivity (Aziz, Norhashim, & Halim, 2011). Due to the ever-evolving nature of digital technology, however, anything connected to the Internet poses information security threats. Even internal factors, according to Shamsudin et al 2019's study, can pose a threat. The risk has the potential to bring about the demise of businesses. Security risks and attacks, such as threats arising from external aspects or recognised as external threats associated with an outsider who violates the security of the organization's information, can contribute to a decrease in the organization's efficiency and productivity. Even management and staff members can be subject to internal dangers.

Technology is an integral component of our everyday life. Technology has become so pervasive that everything we do, whether at work or at home, requires interaction with technology. To enjoy the benefits or ease of utilising such technology while maintaining the privacy and security of one's data, the usage of technology has brought about additional responsibilities. Then, the subject of digital literacy arises. The use of technology was restricted to experts in the past, but this has changed dramatically over time. Indeed, technological interaction has become an integral element of our daily lives. To be effective and efficient in the workplace, individuals must possess or obtain a minimum level of skills. Organizations should view digital literacy as an ongoing process that can be viewed in terms of employees' personal development (depending on their working environment) and technology advancement. One of the most significant assets of any organisation is its information or data. Thus, its handling and security are essential.

In this regard, Malaysia Planning has already integrated a practical cyber security policy; directed by Majlis Keselamatan Negara (MKN), the Malaysia Cyber Security Strategy 2020-2024 aims to ensure information security while fostering economic progress and public well-being. Security and cyber risk information exchange networks, channels, and avenues for government agencies, enterprises, and the public should be reinforced (Majlis Keselamatan Negara (MKN) 2020). Understanding of the situation, teamwork, and the ability to reduce risks must also be improved. This research might also highlight the necessity to not only focus on security at the national level, but also to implement a top-down approach with the participation of all Malaysian inhabitants in terms of information security. With globalisation accelerating at an alarming rate because of digitization, this was or is done to help businesses gain a competitive advantage. This necessitates a set of technical, professional, and specialised ICT abilities. Employers must guarantee that policymakers involve all stakeholders in participating in and learning new skills in an increasingly digitised society. This study examines the influence of Information Security Behaviour (ISB) exhibited by administrative and diplomatic officers (ADO) on the relationship between Digital Literacy and Information Security Culture (ISC), particularly in the context of remote work (which has become the prevailing norm for online meetings and tasks). This research is consistent with and supports the MYDigital economy blueprint for all civil servants to be digitally literate by 2025 as mentioned in:

> Thrust 1: to drive digital transformation in the public sector with the objective of educating all levels of government employees on digital literacy; and

Thrust 6: to build trusted, secure, ethical digital environments with the objective of raising cyber security awareness and guarantee that all Malaysians have the skills and information necessary to fight cyber-attacks and cybercrimes.

This research will also further bolsters Malaysia's efforts to uphold its ranking and contribute to The Global Cybersecurity Index (GCI), an initiative led by the International Telecommunication Union (ITU), the specialised UN agency for ICTs with aims to enhance cybersecurity worldwide through the collaboration of experts and contributors from various countries and international organisations.

In a changing society and labour market where information is a crucial resource, knowledge and skills in information security, privacy, and copyright/intellectual property rights and protection are essential for organisational and individual success. One of the most serious issues with the security of an organization's information is an employee's lack of knowledge, awareness, and commitment to information security (da Veiga et al., 2020). Users have developed ‘security blindness' because of their frequent interactions with information assets, according to Dhillon and Backhouse (2000). Individual attitudes, beliefs, and core values, on the other hand, can be modified to ensure a secure environment for an organization's information assets and successful information security management. Thomson et al. hypothesised that well-trained and conscientious employees might be the most secure link in any organization's security architecture. As a response to the risks posed by insiders, many firms have implemented a variety of administrative and technological controls within an overall information security management system based on policies, processes, and practises (Alhogail, 2015). Unfortunately, there is a scarcity of organised frameworks that provide practitioners with a reference guide for the human components that must be addressed when dealing with the insider threat.

Companies require informed and trained personnel who understand the risks and responsibilities connected with information privacy, information security, and intellectual property management. Professionals with this expertise can help organisations ensure that they and their employees comply with privacy and security requirements for information under their care and control, as well as that the organisation and its employees do not violate copyright provisions in their use of information (Burkell, 2015). Individual employees' inadequate or inappropriate information management practises are at the root of organisational issues relating to information privacy, security, and ownership. Users exhibit insufficient skills and knowledge, as well as inappropriate behaviours, and equivalent gaps occur at the organisational level as well. National and international regulatory frameworks governing data privacy, data security, and intellectual property are complex and ever-changing, increasing the burden on organisations to stay current on essential regulatory and legal responsibilities.

Information privacy governance and risk management are critical to the performance of a wide range of job categories, including the emerging disciplines of information and knowledge management. There is an increasing demand for competent and knowledgeable people to undertake organisational duties related to information management, with growth in these industries being especially visible over the previous decade. Organizations must have significant expertise in these areas of digital literacy in order to ensure that they and their employees comply with privacy and security requirements for information in their care and control, as well as that neither the organisation nor its employees violate copyright provisions in their use of information. Failing to fulfil any of these responsibilities may result in reputational harm, legal action, and/or financial loss for the company.

According to Burkell's 2015 research, many users, including those with significant relevant educational backgrounds, do not follow basic security updates measures such as confirming the source of an email before downloading an attachment, running anti-virus software, and applying software promptly (Rajivan et al., 2020). Users fail to fully protect even the most private and significant of technological gadgets, the cell phone (Alsaleh et al., 2017; Jones & Heinrichs, 2012; Jones, Chin & Aiken, 2014; Tan & Sagala, 2012). In general, security systems do not pay enough attention to usability, making them difficult for consumers to utilise effectively (Furnell, 2006). User security complacency (Mylonas, Kastania, and Gritzalis 2013) is another issue, with many individuals depending on application repositories to ensure that programmes are safe to install rather than carefully reading security alerts, notices, and terms of service. If users are confidence in their abilities to use the tools, security features and rules are more likely to be applied and followed. An often-debated attribute that has potential significance in cybersecurity recruitment and education is the concept of a "security mindset": a cognitive approach that is believed by some security experts to provide distinct advantages in their field (Schoenmakers et al., 2023). Those with basic security awareness are more likely to implement security measures (Tan & Sagala, 2012), as are those who have received training in information and cybersecurity. There are a few demographic groups that are more cognizant of security knowledge and behaviours than others. For example, older persons are less aware of the need of information security and are less likely to practise it effectively than their younger colleagues (Grimes, Hough, Mazur, & Signorella, 2010). Males are more likely than women to engage in risky behaviour (e.g., clicking on a link from an unknown source) and use more technological security measures (e.g., encryption, password protection); Jones & Heinrichs, 2012; Mensch & Wilkie, 2011. There is now substantial evidence that at least some users take insufficient security measures in their personal lives, and their attitude towards security and level of digital literacy, such as knowledge and skill gaps, are likely to influence their behaviour inside an organisation, leading them to be lax in adopting security in their online environment.

LITERATURE REVIEW

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 (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).

To reduce the likelihood of security breaches, businesses should place a larger emphasis on employee conduct. By fostering a culture of information security awareness, the risk to information assets will be diminished (Da Veiga and Eloff, 2010). Employees have the potential to be a substantial asset in reducing the risk to information assets notwithstanding this potential risk. Employee adherence to security policies and procedures is essential for strengthening information security (Bulgurcu et al., 2010). Employees with the proper training have the potential to be the strongest link in an organization's architecture (Osborne & Hammoud, 2017). Employees of organisations should have the necessary level of digital literacy to ensure that they are adequately prepared to comply with information security rules and legislation, hence fostering a healthy information security culture (Bulgurcu et al., 2010). Employees should view information security as second nature and an intrinsic part of their daily routine. This supports the incorporation of information security into the culture of the organisation. The corporate culture of an organisation should shape the security behaviours of its employees (Karlsson et al., 2021).

Security Risks

When assessing an organization's information security culture, security risk is the first component to analyse. To increase the effectiveness of an organization's ISC, the decision is made to equip employees with cutting-edge technology (strategic component). In order to reduce any associated risk, a risk assessment (a component of risk management) is conducted to identify security concerns and develop the necessary processes to mitigate the identified risks. ADOs engage directly with the wireless network and mobile devices on the individual layer of the information security culture structure proposed by Da Veiga and Eloff (2010). As such, they must be informed of the needs of the information security policy and any security concerns. They must utilise strong passwords and ensure that Bluetooth-enabled devices like PDAs are set to "non-detectable." A culture of information security can be observed in its artefacts (e.g., peripherals, web-based training, email, and telephones) and underlying attitudes and ideas. According to Masrek et al., 2018, when personnel have the knowledge and skills necessary for information security, they are also familiar with the processes and procedures that ensure information security.

Information technology's (IT) rapid expansion has exacerbated security threats in both the industrial and financial sectors. Human action is currently regarded as the most important aspect in the management of information security. Human activity-related information security hazards are observed in large and medium-sized firms where employees breach company security regulations or personally commit security theft. These challenges are caused by multiple sources, including a lack of information security awareness among employees, inadequate information security training for employees, and poorly managed teams. These elements pose significant risks to an organization's information security. Compliance with an organization's security policy and periodic information security training for employees can have a favourable effect on the human factors of security.

The exponential growth of the IT industry has increased the technological requirements of businesses. With the increased use and availability of World Wide Web services, security has become the most important factor for many enterprises. Several academics have presented solutions to these problems; yet the quantification of security measures remains a hurdle according to numerous studies. Employee illiteracy increases data breaches and data security vulnerabilities, according to Yeniman et al. (2011). In an empirical study conducted by Jaeger (2013) on the causes of data breaches, 38% of data breaches are due to the loss of paper files, 27% are due to human carelessness (such as the loss of data storage devices), and 11% are due to hackers. Employees have a significant impact on information security risk and data breaches, according to these findings. It has been reported that noncompliance with regard to information security and access policy violations. Vance et al. (2013) suggested that lack of information security training and policy infractions are the result of incompetent or inept management.

Security Awareness

The second component of ISC is security awareness, which is defined as an understanding of security threats, their negative ramifications, and the cost of security failures. In the context of information security, "security culture" refers to the understanding of security issues and rules (Pfleeger et al.,2015). As information security has become an organisational function, a culture of information security may be assumed to exist within an organisation. It is a subculture that emphasises integrating information security into the daily lives of workers (AlHogail and Mirza, 2014). Awareness of security is a crucial component of any efficient security plan. Employers must ensure that all personnel are aware of security threats, rules, and procedures (McCormac et. Al, 2017). The National Institute of Standards and Technology (NIST) (2003) asserts that information security awareness and training programmes are essential for developing an effective information security programme. As corporations learn to comprehend the position of end-users as a security barrier, they reevaluate security awareness and the most effective means of addressing security awareness challenges. According to Hadlington and Parsons (2017), ISA is essential for protecting organisations from security threats. Information Security Awareness (ISA), according to Alzahrani and

Alomar (2016), is the information one possesses regarding security dangers, procedures, and protocols. Information security awareness, according to McCormac et al. (2017), is the degree to which an end-user comprehends information security policies and procedures and their compliance with security regulations. According to Sebescen and Vitak (2017), businesses must recognise the significance of security investments, including technology solutions and security education. According to Tasevski (2016), security awareness is the most important protection mechanism for information security. Effective risk management requires outlined processes, policies, and procedures based on identified threats and dangers (Croitoru & Neacsu, 2019). Mckeown (2019) maintains that security is still in its infancy; it must transition from a belief- and value-based foundation to one based on established procedures and industry standards. According to the study by Oyinloye et al. (2020), the delivery strategy for security awareness training and education has a direct impact on the outcome. In addition, Oyinloye et al. (2020) found that end-user security training enhanced end-user understanding for the significance of security awareness.

Culture and information security have not been combined historically (Mekeown, 2019). Positive security behaviour is enforced by security awareness education, according to Sebescen and Vitak (2017). Understanding the motivations underlying user behaviour can aid in defining security education and mitigating deviant behaviour (Sebescen & Vitak, 2017). Alotaibi et al. (2019) assert that end-user unwillingness to comply with security standards renders traditional policy-based security methods unsuitable. IT policies are the basis of a security programme, giving a means of minimising hazards posed by employees' exploitation of information assets (Alotaibi et al., 2019). Organizations must recognise that while humans are the first line of defence for IT security, they are also the weakest link (Alotaibi et al., 2019; Tsohou et al., 2015). To effectively exploit people as a security barrier, Tsohou et al. (2015) assert that the significance of security awareness cannot be overlooked. Croitoru and Neacsu (2019) believe that a successful security programme will help establish a culture of security awareness aimed at mitigating risk via company-wide participation in risk detection, prevention, and mitigation. Mckeown (2019) argues that organisations must recognise the significance of incorporating security into the company culture. Understanding the importance of end-users in the protection of corporate information assets, firms have increased their emphasis on information security awareness campaigns, according to Aldawood and Skinner (2019). However, Aldawood and Skinner (2019) stress that cost constraints can restrict the sorts of training that are accessible. Insider threats and end-user indifference owing to a lack of security understanding contribute to the success of malware attacks, according to Valiente (2017). According to Rahim et al. (2015), information security awareness must be inclusive of all ages and demographics to be the most effective. Researchers have raised the alert to emphasise the significance of cybersecurity knowledge (Rahim et al., 2015). Stanciu and Tinca (2016) noted that organisations' haste to adopt new technologies exceeds their capacity to safeguard information assets. The reliance of enterprises on technology alone for safety has left them vulnerable to dangers (Stanciu & Tinca, 2016).

METHODOLOGY

An exhaustive examination of the relevant literature was performed with the purpose of determining the dimensions for information security culture in respect to the components of digital literacy. The researchers were able to uncover numerous study gaps in the foundation of the construct with the assistance of the literature. It was clear that there was a lack of conceptual clarity because there were many different definitions of information security culture in relation to digital literacy. These definitions were often inconsistent. There was a significant gap observed between the academic view and the industry perspective on the topic of employee engagement (Nasir, 2020). It was determined to be vital to build the construct with contributions from both academicians and practitioners to fill the research void that had been identified. In order to accomplish this goal, the researcher reached out to six information security industry professionals with whom the preliminary field study would be carried out. The selection of the subject matter experts who should take part was based on a set of criteria, and those criteria included specialists and experts in their respective fields who had prior experience working in information security. It was determined that six different subject matter experts, including a head of department, a specialist, a professor, manager, and a senior lecturer, were eligible to participate and were granted authorization to do so as subject matter experts.

The results of the literature research and the thoughts that were prompted by the working environment of the ADOs at the workplace were used to develop a series of questionnaires, which were distributed to the participants. According to Hyman, Michael, and Sierra (2016) open-ended questions have the potential to give crucial insights not just into the substantive answers that respondents provide, but also into how respondents comprehend the questions that the researcher poses to them and how they arrive at an answer. The researcher also made a concerted effort to put respondents at ease by speaking to them in everyday language and avoiding technical terms that could lead to misunderstandings. As a result of the researcher's involvement in the industry, the researcher's job of conducting the session with the respondents was made easier by the researcher's gathered experiences. Table 1 presents the results of a combination of items used in previous research, responses from preliminary study, and items developed specifically for this study. The items developed specifically for this study were adapted and derived from an existing questionnaire found in DaVeiga (2010), Martins & Elofe, 2002 and Da Veiga & Martins, 2017). In the context of this study, the researcher made some adjustments to the measures in terms of the number of items, the wording of sentences, and the scaling for the items so that they would better reflect the culture of the ADO and the type of the job that they do.

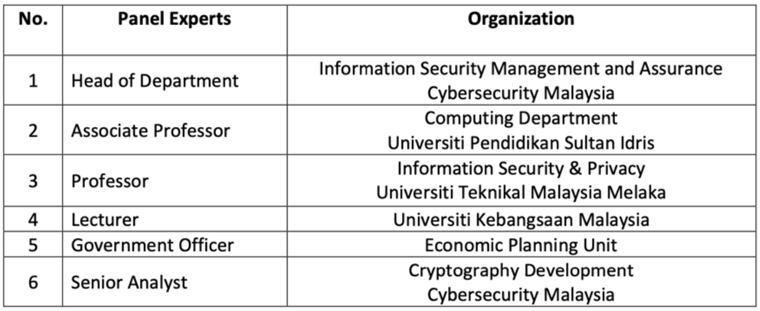
Table 1 : Items for Each Dimensions

Security Risks
My workplace has implemented a risk assessment program that is supported and adhered to at all levels
My workplace provides a system or platform whereby all employees may report security problems and incidents
My workplace, password protocol is enforced and tested **My workplace routinely reviews and revises the information security programme, particularly after incidents and threats**
Hackers do not target me because my computer has no value to them
I logged into work accounts using public network, such as from a library, cyber café or hotel lobby
I use the same passwords for my work accounts as I do for my personal accounts at home, such as Facebook, Twitter or my personal email accounts
Security Awareness
I feel I have been sufficiently trained in information security at my workplace to do my job online
When I learn things about information security aspects in the office, I implement them at home
I am confident that I could recognize a cyber-attack or cyber incident if I saw one **I am interested in increasing my own cyber security knowledge and skills**
Management and the security division routinely share with all employee's information security regarding security evaluations and issues
I know where to access internal resources to help me make good security decisions

PRE TESTING

The following step was to have a certain number of experts confirm the items to guarantee the evaluation instrument's content validity. When choosing domain experts, it's important to look for things like in-depth familiarity with the topic, formal education in the field, and relevant work experience. In order to ensure the reliability and validity of the questionnaire, Sekaran and Bougie (2016) recommend assessing it for three forms of validity: content validity, criterion-related validity, and construct validity. Content validity was used in this research to make sure the questionnaire was reliable. To what extent does the instrument contain a representative sample of items for the concept of interest? (Polit & Beck, 2006). That is the definition of content validity. The content validity of a new instrument is seen as equally relevant to the criterion-related and construct validity when making inferences about the measure's quality. Although she recommended at least three, Lynn (1986) hinted that having more than ten might be excessive. The instruments in this study were reviewed by a panel of six specialists. The questionnaire was pre-tested by an information security and privacy specialist from Universiti Teknikal Melaka, as well as associate professors from the computing department of the Faculty of Art, Computing, and Creative Industries at Universiti Pendidikan Sultan Idris. These scholars possessed extensive expertise and qualifications in the domains of information security management and research methodology for the Social Sciences. In addition, two experts in cyber security from the Information Security Management and Assurance and Cryptography Development department at Cybersecurity Malaysia, as well as two other potential respondents, were involved in the pre-testing. These included a manager who is also a lecturer at Universiti Kebangsaan Malaysia and specialises in cyber security awareness, and an officer from the Prime Minister's Department, Economic Planning Unit. The list of panels who contributed to this study is presented in Table 2.

Table 2 : List of Panel Experts during the Questionnaires Pre-Testing



No.	Panel Experts	Organization
1	Head of Department	Information Security Management and Assurance Cybersecurity Malaysia
2	Associate Professor	Computing Department Universiti Pendidikan Sultan Idris
3	Professor	Information Security & Privacy Universiti Teknikal Malaysia Melaka
4	Lecturer	Universiti Kebangsaan Malaysia
5	Government Officer	Economic Planning Unit
6	Senior Analyst	Cryptography Development Cybersecurity Malaysia

FINDINGS

According to Lynn (1986), researchers calculate two varieties of CVIs. The first kind is concerned with the content validity of individual items, whereas the second type is concerned with the content validity of the entire scale. By custom and on the guidance of early researchers such as Lynn (1986), and Waltz (1981), these item evaluations are ordinarily measured on a 4-point ordinal scale. Lynn (1986) admitted that 3- or 5-point rating systems may be explored, but she pushed for a 4-point scale in order to avoid a neutral and ambiguous midway. In the context of this study, the labels for the four points are as follows: 1 = No relevance whatsoever, 2 = Item need correction, 3 = Relevant but requires minor revision, and 4 = Extremely relevant. Then, for each item, the content validity index for items (I-CVI) is calculated by dividing the number of experts who gave a rating of 3 or 4 (thereby dichotomizing the ordinal scale into relevant and irrelevant) by the total number of experts. Lynn (1986) recommended I- CVIs no lower than 0.83 if there are a total of six experts. The content validity index for scales (S-CVI) was used to measure the content validity of the total scale, which comprises Universal Agreement (UA) and Ave (Average). The findings for content validity are presented in Tables 3 and 4, with a summary in Table 5.

Table 3 : *I-CVI and S-CVI/Ave for Security Risks (SR)*

Item	**Expert 1**	**Expert 2**	**Expert 3**	**Expert 4**	**Expert 5**	**Expert 6**	**Number of Agreement**	**Item CVI**
SR1	✓	✓	✓	✓	✓	✓	6	1.00
SR2	✓	✓	✓	✓	✓	✓	6	1.00
SR3	✓	✓	✓	✓	✓	✓	6	1.00
SR4	✓	✓	✓	✓	✓	✓	6	1.00
SR5	✓	✓	✓	✓		✓	4	0.83
SR6	✓	✓	✓	✓		✓	5	0.83
SR7	✓	✓	✓	✓	✓	✓	5	1.00
Proportion Relevant:	1.00	1.00	1.00	1.00	0.71	1.00	Mean I-CVI:	0.95
							S-CVI/UA:	0.71
							S-CVI/AVE:	0.95

Note: ✓ = Item is relevant; I-CVI = Item Content Validity Index; S-CVI/UA = Scale Content Validity Index/Universal Agreement

S-CVI/AVE = Scale Content Validity Index/Average Proportion; Minimum I-CVI is 0.83 and S-CVI/AVE is 0.90 for 6 experts

Table 4 : *I-CVI and S-CVI/Ave for Security Awareness (SA)*

Item	**Expert 1**	**Expert 2**	**Expert 3**	**Expert 4**	**Expert 5**	**Expert 6**	**Number of Agreement**	**Item CVI**
SA1	✓	✓	✓	✓	✓	✓	6	1.00
SA2	✓	✓	✓	✓	✓	✓	6	1.00
SA3	✓	✓	✓	✓	✓	✓	6	1.00
SA4	✓	✓	✓	✓	✓	✓	6	1.00
SA5	✓	✓	✓	✓	✓	✓	6	1.00
SA6	✓	✓	✓	✓	✓	✓	6	1.00
Proportion Relevant:	1.00	1.00	1.00	1.00	1.00	1.00	Mean I-CVI:	1.00
							S-CVI/UA:	1.00
							S-CVI/AVE:	1.00

Note: ✓ = Item is relevant; I-CVI = Item Content Validity Index; S-CVI/UA = Scale Content Validity Index/Universal Agreement

S-CVI/AVE = Scale Content Validity Index/Average Proportion; Minimum I-CVI is 0.83 and S-CVI/AVE is 0.90 for 6 experts

Table 5: Summary of content validity

Construct	**No. of Items**	**I-CVI (>=0.83)**	**S-CVI/ Ave (>=0.90)**
Security Risks (SR)	7	0.95	0.95
Security Awareness (SA)	6	1.00	1.00

I-CVI for all the items of the two dimensions are 0.95 and 1.00. The S-CVI (Average) for security risks and security awareness of information security culture was 0.95 (Table 3) and 1.00 (Table 4), respectively. The overall SCVI for the 13-items scale was above 0.90 which indicated high content validity of the items for the construct of information security culture.

CONCLUSION

The next step in the research process is to conduct a content validity assessment to make sure the research instrument is reliable. In this case, a questionnaire is being used to collect data. Identifying issues, reducing measurement error, reducing respondent burden, ascertaining whether respondents are correctly interpreting questions, and making sure that question order does not affect responses all depend on the content validity of the instrument. Whilst it's nearly impossible to craft a perfect instrument, there are still many considerations that must be given priority if you want to construct something worthwhile. Thirteen items were generated as part of the evaluation instrument for information security culture; these included items from prior research, replies from a pilot study, and new items adapted and derived from an existing questionnaire for this investigation. Following that, six professionals in the field were polled about how important they felt the items were. In conclusion, all the constructions are maintained, as there is a fair amount of agreement among the specialists over their use. Hence, future studies can guarantee that the instrument's reliability and various forms of validity, such face, construct, and criterion validity, are checked to enhance the assessment tool's usefulness. Face validity, construct validity, and criteria validity are all types of this validity.

REFERENCES

Al Hogail, A. and Mirza, M. (2015), “Organizational information security culture assessment”, paper presented at The 2015 International Conference on Security and Management (SAM’15), 27-30 July, Las Vegas, available at: http://worldcomp-proceedings.com/proc/p2015/SAM_contents. html

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. Future Internet, 11(3), 73. https://doi.org/10.3390/fi11030073

Alotaibi, A., Edum-Fotwe, F., & Price, A. D. F. (2019). Critical barriers to social responsibility implementation within mega-construction projects: The case of the kingdom of saudi arabia. Sustainability, 11(6), 1755. https://doi.org/10.3390/su11061755

Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. PLOS ONE, 12(3). https://doi.org/10.1371/journal.pone.0173284

Alzahrani, A., & Alomar, K. (2016). Information security issues and threats in Saudi Arabia: A research survey. International Journal of Computer Science Issues, 13(6), 129–135. https://doi.org/10.20943/01201606.129135

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

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

Croitoru, I., & Neacsu, V. (2019). RISK MANAGEMENT – BETWEEN NECESSITY AND OBLIGATION. Internal Auditing & Risk Management, (1), 23–32.

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

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020a). Defining organisational information security culture—perspectives from academia and industry. Computers &amp; Security, 92, 101713. https://doi.org/10.1016/j.cose.2020.101713

G. Dhillon and J. Backhouse, “Technical opinion: Information system security management in the new millennium,” Commun. ACM, vol. 43, no. 7, pp. 125–128, Jul. 2000.

Hadlington, L., & Parsons, K. (2017). Can cyberloafing and internet addiction affect organizational information security? Cyberpsychology, Behavior, and Social Networking, 20(9), 567–571. https://doi.org/10.1089/cyber.2017.0239

Hyman, Michael & Sierra, Jeremy. (2016). Open- versus close-ended survey questions. NMSU Business Outlook. 14. [47]

Jaeger, J. (2013, February 5). Human error, not hackers cause most data breaches. Compliance Week. https://www.complianceweek.com/human-error-not-hackers-cause-most-data-breaches/4048.article

Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? Journal of Computer Information Systems, 53(2), 22–30.

Jones, B. H., Chin, A. G., & Aiken, P. (2014). Risky business: Students and smartphones. TechTrends, 58(6), 73–83. https://doi.org/10.1007/s11528-014-0806-x

Karlsson, M., Karlsson, F., Åström, J., & Denk, T. (2021). The effect of perceived organizational culture on employees' information security compliance. Information &amp; Computer Security, 30(3), 382–401. https://doi.org/10.1108/ics-06-2021-0073

Majlis Keselamatan Negara (MKN). (n.d.). https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

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

Masrek, M. N. (2018). Assessing information security culture: The case of Malaysia public organization. 1–1. https://doi.org/10.1109/icitacee.2017.8257663

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. Australasian Journal of Information Systems, 21. https://doi.org/10.3127/ajis.v21i0.1697

McKeown, D. A. (2019). Building a risk-based information security culture. ISSA Journal, 17(4), 14–21.

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. Academy of Information and Management Sciences Journal, 14(2), 91–116.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. Computers & Security, 34, 47–66.

Nasir, A. (2020). Information security culture model for malaysian organizations: A Review. International Journal of Advanced Trends in Computer Science and Engineering, 9(1.3), 117–121. https://doi.org/10.30534/ijatcse/2020/1691.32020

Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. Information and Computer Security, 27(2), 146–164. https://doi.org/10.1108/ICS-12-2016-0095

Osborne, S., & Hammoud, M. S. (2017). Effective employee engagement in the Workplace. International Journal of Applied Management and Technology, 16(1). https://doi.org/10.5590/ijamt.2017.16.1.04

Oyinloye, T., Eze, T., & Speakman, L., (2020). Towards cyber-user awareness: Design and Evaluation. Reading, Academic Conferences International Limited: 577-588, XVI.

Polit, D. F., & Beck, C. T. (2006). The content validity index: Are you sure you know what's being reported? critique and recommendations. Research in Nursing & Health, 29(5), 489–497. https://doi.org/10.1002/nur.20147

Rahim, N. H. A., Hamid, S., Mat Kiah, M. L., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, 44(4), 606-622. doi: http://dx.doi.org.proxy.cecybrary.com/10.1108/K-12-2014-0283

Rajivan, P., Aharonov-Majar, E., & Gonzalez, C. (2020). Update now or later? effects of experience, cost, and risk preference on update decisions. Journal of Cybersecurity, 6(1). https://doi.org/10.1093/cybsec/tyaa002

Rubenstein, S., & Francis, T. (2008). Are your medical records at risk? Wall Street Journal - Eastern Edition, 251(100), D1-D2.

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

Sebescen, N., & Vitak, J. (2017). Securing the human: Employee security vulnerability risk in organizational settings. Journal of the Association for Information Science and Technology, 68(9), 2237–2247. https://doi.org/10.1002/asi.23851

Shamsudin, N. N. A., Yatin, S. F. M., Nazim, N. F. M., Talib, A. W., Sopiee, M. A. M., & Shaari, F. N. (2019). Information Security Behaviors among Employees. International Journal of Academic Research in Business and Social Sciences, 9(6). https://doi.org/10.6007/ijarbss/v9-i6/5972

Sierra, J. J. (2016). Open-versus close-ended survey questions. https://www.researchgate.net/publication/282249876 @report{Sierra2016, author = {Jeremy J Sierra}, title = {Open-versus close-ended survey questions}, url = {https://www.researchgate.net/publication/282249876}, year = {2016}, }

Singh, N., Gupta, A.M. and Ojha, A. (2014), "Identifying factors of organizational information security management'", Journal of Enterprise Information Management, Vol. 27 No. 5, pp. 644-667.

Stanciu, V., & Tinca, A. (2016). Students' awareness on information security between own perception and reality – an empirical study. Accounting & Management Information Systems, 15(1), 112–130.

Tan, M., & Sagala Aguilar, K. (2012). An investigation of students' perception of Bluetooth security. Information Management & Computer Security, 20(5), 364–381

Tasevski, P. (2016). It and cyber security awareness – raising campaigns. Information & Security: An International Journal, 34, 7–22. https://doi.org/10.11610/isij.3401

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems, 24(1), 38-58. doi: http://dx.doi.org.proxy.cecybrary.com/10.1057/ejis.2013.27

U. Sekaran, & R. Bougie, Research methods for business: A Skill-Building Approach, 2016.

Valiente Jr, C. (2017). Addressing malware with cybersecurity awareness. ISSA Journal, 15(10), 16-22.

Van Niekerk, J.F. and Von Solms, R. (2010), "Information security culture: a management perspective", Computers and Security, Vol. 29 No. 4, pp. 476-486, doi: 10.1016/j.cose.2009.10.005

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in Information Systems. Journal of Management Information Systems, 29(4), 263–290. https://doi.org/10.2753/mis0742-1222290410

Yeniman Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. International Journal of Information Management, 31(4), 360–365. https://doi.org/10.1016/j.ijinfomgt.2010.10.006

Z. Musanni1Xp, E. Siregar, E. Ahman, & S. H. Senen, ―Factors Influencing Innovative Work Behavior: An Individual Factors Perspective‖, International Journal of Scientific & Technology Research, vol. 8, no. 9, 324–327, 2019.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. Information Management & Computer Security, 17(4), 330–340. https://doi.org/10.1108/09685220910993980