J. Sci. Inform. Soc. 2023, Vol. 1, No. 2
ISSN 3024-9074

Research Review on Measuring Information Security Awareness

Ariana Yunita[1*], Deden Ade Nurdeni[2]

[1]Department of Computer Science, Universitas Pertamina, Jakarta 12220, Indonesia
[2]Faculty of Computer Science, Universitas Indonesia, Depok, Indonesia
*Corresponding Author: ariana.yunita@universitaspertamina.ac.id

Received: 20 Oktober 2023
Accepted: 14 November 2023

Abstracts

One of the factors that contributes to unauthorized parties releasing confidential company information, including employee personal information, is a lack of awareness of employee information security. This is a critical concern that needs to be addressed immediately by strengthening the company's information security culture and raising employee awareness of security. To enhance the clarity and emphasis of the reform policy, it is crucial to evaluate employee awareness of information security. This paper discusses several approaches that have been employed, either as models or frameworks, to evaluate an organization's level of information security awareness. With the aid of inclusion and exclusion criteria, we chose papers out of the 842 that were included in the systematic literature review. Three components are commonly used to assess information security awareness: knowledge (what is already known), attitude (what is thought to be appropriate to do), and habit (what is usually done). Measurements that encompass these three aspects employ the Knowledge, Attitude, and Behavior (KAB) paradigm. This study might be a reference for organizations to measure their employees' security awareness. Several findings are also discussed in this paper.

Keywords: Systematic Review, Information Security Awareness, Cyber Security, KAB framework

Introduction

Currently, technological advances make it easy for people to access information with various existing tools. This can have both positive and negative impacts on all parties. On the one hand, information can spread to all levels of society quickly. On the other hand, with the ease and sophistication of technology, everything could be data [1] and data can then be transformed into valuable information [2] that is prone to spread. Information is a critical asset, especially for companies. Some data and information about a company can be highly confidential.

In 2022, Indonesia was surprised by the presence of Bjorka who was stealing and selling governments and companies' data on the internet. Data from the State Electricity Company, IndiHome, data registration for 1.3 billion SIM cards, 105 million voter data, and presidential letters were allegedly leaked. Therefore, organizations or companies should be vigilant and consider the importance of information security [3]. Furthermore, the management of a company's information security also becomes important.

Information security, commonly, contains three things, namely the information is not spread to other parties who are not entitled (confidentiality), the integrity of the information (integrity) and the availability of the information when it is needed (availability). However, the standard definition of information, the CIA definition, was encountered by an Appropriate Access definition [4]. Despite the new definition of information security, from the point of view of information security management, a company's information can be leaked due to various factors, such as the weakness of the system against attacks and internal factors. These two things are the focus for the company in implementing information security management.

From an external perspective, according to data from the Ministry of Communication and Information, Indonesia received 1.225 billion cyber-attacks per day in 2018 [5]. Furthermore, according to a report from IBM X-Force, during the Covid-19 pandemic, cybercriminals strategically adopted methods and approaches to successfully enter companies all over the world by taking advantage of a shifting environment [6]. Therefore, companies should be wary of attacks from outside.

From an internal perspective, [7] stated that although 45% of attacks were carried out by outsiders, 55% were also caused by internal parties, namely those who have access to an organization. Insiders can mean that an attack is carried out by entering an organization or employee who lacks information security awareness so that they make mistakes that result in information security incidents. Common user mistakes include clicking on pages that could potentially record important information, sharing passwords with unauthorized people, leaving work on computers unattended and connecting personal devices to untrusted public networks. Furthermore, phishing overtook vulnerability exploitation as the most common infection vector in 2021, overtaking it in 2020. However, there is currently no one technology or solution that will stop all phishing assaults, and threat actors are always improving social engineering and anti-malware detection methods to get beyond security measures. To overcome this, it is necessary to socialize employees regarding information awareness. The first step before socializing information security awareness is measuring the level of information security awareness.

Another study has attempted to review how to measure information security awareness [8]. However, they did not list what areas and sub areas that should be measured. This study aims to review methods for evaluating the level of information security awareness in an organization as well as detail the areas and sub areas as the baseline for designing the questionnaire. The next section explains how this research is conducted. Section three discusses the results, and then the final section shows the conclusion.

Material and Methods

This study employed the Systematic Literature Review (SLR) method proposed by Kitchenham [9]. Several stages in the SLR are: 1) Defining research questions, 2) Determining research databases and keywords, 3) Formulating selection criteria/ inclusion and exclusion. The following are research questions that are used as the basis for conducting SLR:

1. What research methodologies and methods have been used in evaluating the level of information security awareness in an organization?
2. What are the frameworks or models used to measure information security awareness?

The database used to perform the search was the Scopus database. The Scopus database was used in this study because it contains peer-reviewed publications [10], [11]. The purpose of the search is to search for related literature according to the research questions above. Keywords that were used in this study were related to how to measure, evaluate, and investigate information security awareness. The word assess is often used interchangeably with measure or investigate. Therefore, the keyword to search is TITLE-ABS-KEY ((asses* OR measur* OR investigate* OR analy* or evaluat*) AND ("information security awareness" OR "cyber security awareness" OR "security awareness")). The initial search results, as of March 18 2020, were 842 documents. Figure 1 shows how to select the literature for this review.

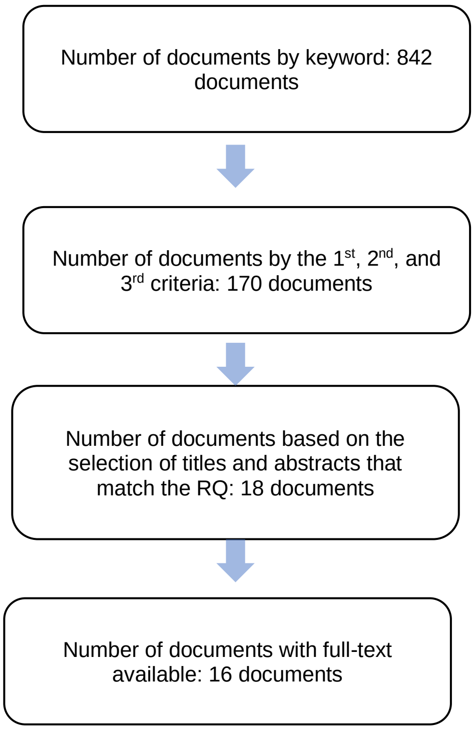
Number of documents by keyword: 842 documents
Number of documents by the 1st, 2nd, and 3rd criteria: 170 documents
Number of documents based on the selection of titles and abstracts that match the RQ: 18 documents
Number of documents with full-text available: 16 documents

Figure 1. Number of Documents in Each Systematic Review Stages

The following were the criteria for previous research that will be included and not included.

1. Publications within the last 3 years.
2. Publication in English.
3. Publications are in the form of journals or proceedings, not in the form of textbooks, lecture notes or book chapters.
4. Peer-reviewed publications.
5. Publications must be complete and can be downloaded (full text).

Furthermore, a selection of criteria is carried out according to the first to third criteria. The search results became 170 documents. Furthermore, the selection of titles and abstracts from 170 documents that can answer research questions in this Systematic Literature Review, from this stage obtained 18 documents. Then search for complete documents (full text) on the 18 documents, the result is that 16 documents have full text and two documents do not have full text. Finally, we selected 8 papers that can address our research questions. The following section discusses the results of measuring information security awareness.

Results and Discussion

Data is valuable for a company and data that has been processed can become information. Information of a company or organization is an asset and should not be accessed by unauthorized parties. Employees in a company or organization can unknowingly or unconsciously divulge company secrets [12]–[14]. Therefore, there should be decent data management and information security management by a company. Information security is defined as the protection of the confidentiality, integrity, and availability of information assets in the storage, processing, or transmission of information [15]. Information security is implemented through the application of policies, knowledge, awareness training, and technology. Information security covers a broad area of information security management, data security, and network security. The Triangle model of CIA has become a standard for information security in industry or government, this standard is based on three characteristics of information that give value to organizations, namely confidentiality, integrity, and availability.

Information security awareness is a practice carried out to make people aware of issues related to information security. The goal is to encourage them to act in a way that is appropriate to the value of information as part of their work activities. Information security awareness is a fundamental element of effective security management. An organization can make concrete changes by increasing awareness of information security.

Thus, information security awareness seen from the 'person' side includes cognitive and behavioral aspects. Meanwhile, from an organizational perspective, it covers process aspects. From the cognitive aspect, information security awareness is about users knowing and understanding about information security and its threats. From the behavioral aspect, information security awareness is that users can provide appropriate responses when there is a threat to information security or take preventive action against information security threats. Meanwhile, from the process aspect, it is about continuous efforts to increase user awareness according to their roles and responsibilities in managing information security.

Measurement of information security awareness aims to obtain a baseline about the status of an organization's information security, this is fundamental in information security awareness program initiatives [16]. Awareness programs are designed to improve the security of information assets by providing knowledge, skills, and guidance to individuals targeted by the organization. Furthermore, to be able to measure information security awareness, it is necessary to determine what is being measured (information security area) and how to measure it (awareness measurement method) [17].

There are several methods for measuring information security awareness such as questionnaire surveys, scenario-based, experiments or interviews. The questionnaire survey method is used to capture user knowledge, attitudes, or behavior according to what the user perceives, this method can be combined with interviews to enrich the results of the analysis [18]. Qualitative research methods such as Focus Group Discussion (FGD) can also be used to validate and enrich survey materials or research results. Comparison of information security awareness measurement methods is presented in Table 1. Table 1 shows eight studies [12]–[14], [19]–[23] that have been summarized to determine the target type of organization and the method used. Most methods use a questionnaire survey aimed at correspondence in government, business, and education.

Table 1. Information Security Awareness Measurement Method

No	Author (Year)	Ref	Organization			Method				
			Government	Business	Education	FGD	Questionnaire	Scenario Based	Experiment	Interview
1	Galba et al. (2018)	[20]		V			V			
2	Ndiege and Okello (2018)	[23]			V		V	V		
3	Tarmizi et al. (2019)	[14]	V			V	V			
4	Filippidis et al. (2018)	[19]			V		V			
5	Kusumawati (2018)	[22]	V				V			
6	Normandia et al. (2019)	[12]	V				V			V
7	Puspitaningrum et al. (2018)	[13]	V				V			V
8	Ikhsan and Ramli (2019)	[21]	V					V	V	

Measurement of information security awareness generally uses three dimensions, namely the knowledge dimension (what is already known), the attitude dimension (what is perceived/should be done) and the habit dimension (what is usually done). Measurements that use these three dimensions use the Knowledge, Attitude, Behavior model which is abbreviated as KAB [17]. This KAB model adopts psychologist theory and forms the basis for several studies on the evaluation of information security awareness. The basis of the KAB model is that each of the three dimensions is measured by the focus area [17].

The advantage of using the questionnaire survey method is that the research target is a large population, and limited research resources, so the questionnaire survey method makes sense to apply. This method can be implemented with the approach of [17], which proposes a prototype/model to measure the level of information security awareness. In addition, the measurement results are converted to a scale as in Table 2.

Table 2. Category of Awareness Based on Evaluation Score. Source: [17]

Level of Awareness	Score
Good	>80
Average	60-79
Poor	<60

The results of measuring the level of information awareness in an organization will be a recommendation for information management. This is a dynamic process, where information security awareness training will be conducted to increase employee awareness. In terms of training, users will be changed to become aware (become aware), then stay aware (stay aware) and end up being fully aware (be aware) which will change the conscious culture by definition [17].

Evaluation of information security awareness requires a focused area as a reference to the aspect being measured. For example, Kruger and Kearner [17], use 6 focus areas and divide them into several factors/sub areas. Meanwhile Parsons et al. [18] use 21 sub areas in 7 focus areas of information security. Based on the literature review, Table 3 summarizes the 8 focus areas and 24 sub areas that will be used for further study.

The measurement on the knowledge, attitude and behavior model of Kruger and Kearney [17] above, focuses on 6 areas, namely compliance with rules, confidentiality of passwords, use of email and internet, mobile devices, reporting of security incidents, and areas of consequence. However, these areas can be tailored to the needs of the organization. Previous research evaluated 11 focus areas for information security awareness in their organizations, for example in the Ministry of Communication and Information Technology [13], BATAN [14], and the Ministry of Foreign Affairs [12]. The following is a list of focus areas for measuring information security awareness based on a literature study.

Table 3. Areas and Sub Areas of Information Security Awareness

No	Area	Sub Area		References
1	Computer Work Security	SA1	Installing a USB device	[12], [18]
		SA2	Install and update (update) antivirus programs	[12], [19], [20], [23]
		SA3	Make sure your computer is safe by locking it	[12], [22], [23]
		SA4	Updating computer operating system	[20]
2	Password Management	SA5	Choose a good password	[18], [22], [23]
		SA6	Don't use the same password	[13], [18], [19], [21]
		SA7	Don't share password	[12], [18], [21], [23]
3	Email usage	SA8	Don't click on malicious email links	[12], [18], [21]
		SA9	Don't open malicious email attachments	[12], [18], [20], [21]
		SA10	Ignoring requests for personal data via email	[20], [23]
		SA11	Beware of new correspondent opponents	[13], [19], [21]
4	Internet Usage	SA12	Don't download malicious files	[18], [21]
		SA13	Don't access dubious websites	[12], [13], [18], [19], [21], [23]
		SA14	Enter information online securely	[18], [19], [21], [23]
5	Use of Social Media	SA15	Check social media privacy settings	[18], [21]
		SA16	Don't post about sensitive/secret work	[12], [18], [21]–[23]
6	Mobile Device Usage	SA17	Physically secure the mobile device	[18], [21]
		SA18	Sending sensitive/confidential information over public wi-fi networks	[13], [18], [21]

No	Area	Sub Area		References
7	Handling of Data and Information	SA19	Ensure surrounding safety when accessing work	[18], [21], [23]
		SA20	Storing sensitive/confidential documents	[18], [21], [23]
		SA21	Discard/destroy sensitive/confidential documents	[12], [18], [21], [22]
		SA22	Always backup sensitive/confidential data	[12], [19], [23]
8	Information Security Incident Reporting	SA23	Report individual harmful behavior	[12], [18], [21]
		SA24	Reporting information security incidents	[12], [18], [21], [22]

The explanation of each area and sub-area of information security in the table above is as follows.

1. Work Computer Security Area
Computer devices or workstations are media used by employees (end-users) to work. Devices that are often used to exchange data today are USB flash drives. Therefore, it is necessary to pay attention to a safe attitude to transfer data using USB [SA1] and always update the latest antivirus to protect computers from virus threats [SA2]. Locking the computer device with a password [SA3], is also important in preventing unauthorized user access to data/information on the computer. Furthermore, when the operating system is continuously updated, these fixes help keep the system protected, so updating the security patch [SA4] is a way to keep data/information secure.

2. Password Management
Password (password) is a secret word / character that serves as an identifier in a system. To prevent unauthorized user access to the system, setting a strong password is significant. Attacks such as brute force, dictionary passwords, rainbow tables are methods aimed at breaking passwords [24]. The recommended password strength for organizations is a minimum of 10 characters and contains one uppercase letter, one lowercase letter, one number, and one symbol. Thus, [SA5] can be used as an information security awareness area. One of the security practices that must be considered is not sharing passwords with anyone because the possibility of data theft is very high [SA7] and not using the same password for multiple accounts, both for internal organization accounts and accounts on the internet or social media [SA6].

3. Email usage
This form of social engineering is a type of attack that is usually carried out via email, this technique is a major security threat for organizations [24]. Social engineers compromise target accounts by manipulating users into installing malware/spyware on their computers or revealing their passwords unknowingly. Often phishing emails occur in organizational email accounts, it is intended for employees to click on email links [SA8] or open attachments which is actually a trap to install malware/spyware [SA9]. Social engineering can also ask for employee data including username and password information for a personal or organizational account [SA10], therefore employees must be careful when getting emails from correspondents who are unfamiliar or newly known [SA11].

4. Internet Usage
In the area of internet use, an example of unintentional user error is downloading files or malicious software from the internet [SA12]. Files or software downloaded for free from the internet may be spyware that can steal information on the computer [25]. These malicious files are usually found on sites or web pages that contain lots of advertisements, are not trusted or do not use good security [SA13]. Therefore, users are expected to be careful in registering or providing personal or confidential information on untrusted websites [SA14].

5. Use of Social Media
Social media is a medium of social interaction that can be visited by anyone in various parts of the world online. On social media, users should

make privacy settings by protecting personal data or information in it [SA15]. Within the scope of the organization, some organizational information assets may be very sensitive and pose a risk to the image or reputation of the organization if disseminated, so it is necessary to know the level of employee awareness about not posting sensitive/job secret information on social media sites [SA16].

6. Use of Mobile Devices
In this sub area, security and user behavior in using mobile devices should be of concern to organizations, especially for organizations that provide mobile devices for work or employees who access email or company materials via mobile devices [SA17]. Extra security must be a priority for employees when accessing mobile devices using public wi-fi [SA18], because public wi-fi networks are at risk of being infiltrated by people who want to take advantage of the negligence of wi-fi users for actions that are not their right. Therefore, users must ensure the security of the wi-fi by validating to the wi-fi provider and ensuring the surrounding environment is safe when starting to work using mobile devices in public places [SA19].

7. Handling of Data and Information
Data and information security are also maintained by managing the organization's physical documents. The employee's concern in practicing information security is to keep sensitive/confidential documents neatly [SA20]. Leaving confidential information in an unprotected area is as big a threat as someone attempting to exploit the information, as it can create vulnerabilities. If the confidential documents are no longer used, it is better to secure them by destroying the documents to avoid misuse when found by irresponsible people [SA21]. Confidential and sensitive data stored in electronic form can be backed up for data to provide double security on the document, if the data is accidentally lost, we still have backup data that can be used [SA22].

8. Information Security Incident Reporting
Reporting incidents in an information security threat is very important because this will increase the vigilance of the organization's security managers. If an employee sees unsafe behavior or actions from a coworker [SA23], it is strongly recommended to report it to the designated party in the organization [SA24]. It is important to note here that knowledge and behavior is highly connected [26]. In other words, the higher levels of cyber knowledge, the higher levels of cyber awareness. This is in line with the result of our study that the KAB model is the most common framework to be applied to measure security awareness for companies.

.

Conclusion

This paper reviews several previous studies that measure information security awareness. Most previous studies used questionnaires to assess their employee’s security awareness. Furthermore, most previous studies adopt the KAB (Knowledge, Attitude, Behavior) model to evaluate information security awareness. This paper explains eight areas and twenty-four sub areas of the KAB model that can be tailored to the needs of the organization. As measuring information security awareness is important for organizations, organizations might refer to this study for tailoring the areas and sub areas that are needed to be included in the questionnaire.

References

[1] A. Yunita, H. B. Santoso, and Z. A. Hasibuan, "‘Everything is Data’: Towards one big data ecosystem using multiple sources of data on Higher Education in Indonesia," *Journal of Big Data*, vol. 9, pp. 1–22, 2022. https://doi.org/10.1186/s40537-022-00639-7

[2] Z. A. Hasibuan, "Towards using universal big data in artificial intelligence research and development to gain meaningful insights and automation systems," in *2020 International Workshop on Big Data and Information Security, IWBIS 2020*, IEEE, 2020, pp. 9–15. https://doi.org/10.1109/IWBIS50925.2020.9255497

[3] Safitri, "Hacker Bjorka Terus Umumkan ‘Dapur’ Pemerintahan Indonesia," *RadarJember*, 2022. https://radarjember.jawapos.com/nasional/12/09/2022/hacker-bjorka-terus-umumkan-dapur-pemerintahan-indonesia/

[4] B. Lundgren and N. Möller, "Defining Information Security," *Sci. Eng. Ethics*, vol. 25, no. 2, pp. 419–441, Apr. 2019.

[5] A. Yuliani, “Indonesia Diserang Hacker Miliaran Kali Tiap Hari,” 2018. https://kominfo.go.id/content/detail/11956/indonesia-diserang-hacker-miliaran-kali-tiap-hari/0/sorotan_media

[6] Ibm, “X-Force Threat Intelligence Index 2022,” 2022. [Online]. Available: https://www.ibm.com/downloads/cas/ADLMYLAZ

[7] Ibm, “IBM Security Services 2014 Cyber Security Intelligence Index,” 2014. [Online]. Available: https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF

[8] T. Fertig and A. E. Schütz, “About the Measuring of Information Security Awareness: A Systematic,” *core.ac.uk*, [Online]. Available: https://core.ac.uk/download/pdf/286030852.pdf

[9] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering - A systematic literature review,” *Information and Software Technology*, vol. 51, no. 1, pp. 7–15, 2009. https://doi.org/10.1016/j.infsof.2008.09.009

[10] A. Martín-Martín, E. Orduna-Malea, M. Thelwall, and E. Delgado López-Cózar, “Google Scholar, Web of Science, and Scopus: A systematic comparison of citations in 252 subject categories,” *J. Informetr.*, vol. 12, no. 4, pp. 1160–1177, 2018. https://doi.org/10.1016/j.joi.2018.09.002

[11] A. Yunita, H. B. Santoso, and Z. A. Hasibuan, “Research review on big data usage for learning analytics and educational data mining: A way forward to develop an intelligent automation system,” *J. Phys. Conf. Ser.*, vol. 1898, no. 1, pp. 0–13, 2021. https://doi.org/10.1088/1742-6596/1898/1/012044

[12] Y. Normandia, L. Kumaralalita, A. N. Hidayanto, W. S. Nugroho, and M. R. Shihab, “Measurement of employee information security awareness using analytic hierarchy process (AHP): A case study of foreign affairs ministry,” in *Proceedings - 2018 4th International Conference on Computing, Engineering, and Design, ICCED 2018*, Institute of Electrical and Electronics Engineers Inc., 2019, pp. 52–56. https://doi.org/10.1109/ICCED.2018.00020

[13] E. A. Puspitaningrum, F. T. Devani, V. Q. Putri, A. N. Hidayanto, Solikin, and I. C. Hapsari, “Measurement of employee information security awareness: Case study at a government institution,” in *Proceedings of the 3rd International Conference on Informatics and Computing, ICIC 2018*, Institute of Electrical and Electronics Engineers Inc., 2018. https://doi.org/10.1109/IAC.2018.8780571

[14] A. Tarmizi, I. C. Hapsari, A. N. Hidayanto, L. Y. Adhi Yuniarto, and Herkules, “Information security awareness national nuclear energy agency of Indonesia (BATAN),” in *Proceedings - 2018 4th International Conference on Computing, Engineering, and Design, ICCED 2018*, Institute of Electrical and Electronics Engineers Inc., 2019, pp. 35–39. https://doi.org/10.1109/ICCED.2018.00017

[15] C. K. Yee and M. F. Zolkipli, “Review on Confidentiality, Integrity and Availability in Information Security,” *Journal of ICT in Education*, vol. 8, no. 2, pp. 34–42, 2021. http://dx.doi.org/10.37134/jictie.vol8.2.4.2021

[16] A. McIlwraith, *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge, 2021.

[17] H. A. Kruger and W. D. Kearney, “A prototype for assessing information security awareness,” *Computers and Security*, vol. 25, no. 4, pp. 289–296, 2006. https://doi.org/10.1016/j.cose.2006.02.008

[18] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, “The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies,” *Computers and Security*, vol. 66, pp. 40–51, 2017. https://doi.org/10.1016/j.cose.2017.01.004

[19] A. P. Filippidis, C. S. Hilas, G. Filippidis, and A. Politis, “Information security awareness of Greek higher education students - Preliminary findings,” in *2018 7th International Conference on Modern Circuits and Systems Technologies, MOCAST 2018*, Institute of Electrical and Electronics Engineers Inc., 2018, pp. 1–4. https://doi.org/10.1109/MOCAST.2018.8376578

[20] T. Galba, K. Solic, and K. Nenadic, “Evidential reasoning approach to behavioural analysis of ICT users’ security awareness,” *Tehnicki Vjesnik*, vol. 25, no. 2, pp. 309–315, 2018. https://doi.org/10.17559/TV-20150513123751

[21] M. G. Ikhsan and K. Ramli, “Measuring the Information Security Awareness Level of Government Employees Through Phishing Assessment,” in *34th International Technical Conference on Circuits/Systems, Computers and Communications, ITC-CSCC 2019*, Institute of Electrical and Electronics Engineers Inc., 2019. doi: 10.1109/ITC-CSCC.2019.8793292. https://doi.org/10.1109/ITC-CSCC.2019.8793292

[22] A. Kusumawati, “Information Security Awareness: Study on a Government Agency,” in *3rd International Conference on Sustainable Information Engineering and Technology, SIET 2018 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2018, pp. 224–229. https://doi.org/10.1109/SIET.2018.8693168

[23] J. R. Ndiege and G. Okello, “Towards information security savvy students in institutions of higher learning in Africa: A case of a university in Kenya,” in *2018 IST-Africa Week Conference, IST-Africa 2018*, Institute of Electrical and Electronics Engineers Inc., 2018. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85051193072&partnerID=40&md5=7c2301781380803e30bdf5e8bd7ed086

[24] M. E. Whitman and H. J. Mattord, *Principles of information security*. Cengage learning, 2021.

[25] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, “Information security conscious care behaviour formation in organizations,” *Comput. Secur.*, vol. 53, pp. 65–78, 2015. https://doi.org/10.1016/j.cose.2015.05.012

[26] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, “Cyber Security Awareness, Knowledge and Behavior: A Comparative Study,” *Journal of Computer Information Systems*, 2020. https://doi.org /10.1080/08874417.2020.1712269