The Development of Cybersecurity Awareness Measurement Model in the Water Sector

Bryan S. Mufor, Annlizé Marnewick and Suné von Solms
Postgraduate School of Engineering Management, Department of Electrical Engineering Science, University of Johannesburg, South Africa
amarnewick@uj.ac.za
svonsolms@uj.ac.za

Abstract: Cyber-attacks are one of the main threats to information systems, and humans have been identified as the weakest link with regards to information security. This study aims to develop a measurement instrument to evaluate the level of cyber security awareness (CSA) in the water sector in South Africa. There are lots of synergies with regards to cyber system usage across industries, and as a result this study will take a broad base approach in configuring an instrument that can be used to adequately assess the sample space in question. Having a reliable instrument to measure cyber security awareness helps mitigate the failed attempts at preparing employees for imminent cyber disruptions by pin-pointing areas where the training is needed before campaigns can be organised. This study will show that the psychology of employees with respect to cyber security awareness is compartmentalised into three traits: knowledge, attitude, and behaviour. These three traits were assessed under the following eight focus areas to check employee resilience to cyber security: IS policy adherence, Password management, Email use, Internet use, social media use, mobile devices, information handling, and incident reporting. In practice, employees will be required to answer questions formulated under these focus areas to the evaluate their cyber security awareness (CSA) level. The model proposed in this paper was developed to test cybersecurity awareness in the water sector, but can be utilised in other sectors for cybersecurity awareness testing.

Keywords: Cybersecurity; Awareness; Critical Infrastructure

1. Introduction

The age of digitalisation has brought with it an improved level of connectivity and automation. Organisations across the globe have taken full advantage of the digitisation in many ways including, but not limited to, improved access to communication, efficient scaling of operations, and overall cost reduction (Hasan *et al.*, 2021). However, this expansion unfortunately increased the risk and level of exposure of users of interconnected web information systems (Rantapelkonen and Salminen, 2013; Strupczewski, 2021). This rapid growth accentuated the need for innovative methods to protect information systems from malware attacks (Rantapelkonen and Salminen, 2013). Information technology (IT) security is not only an imperative tool for modern organisations, but also a means to retain competitive advantage over the competition in industry (Kong, Kim and Kim, 2012), and improving awareness and readiness to handle cyber-attacks across organisations can have positive effects on the performance of organisations in financial, non-financial and security sectors (Hasan *et al.*, 2021).

Cyber security awareness is an important aspect to evaluate by organisations to fortify cyber security protocols and configurations. This study aims to develop a comprehensive instrument to measure cyber security awareness in the water sector using previously studies psychological inclinations of employees.

2. Cyber security considerations for water sector

This study looks in the CSA levels of employees in the water sector because this sector is among the main targets of cyber-attacks (The White House, 2013). Traditional water systems generally operate on the SCADA system, which monitors a variety of processes along the value creation chain, including raw water extraction and/or collection, transport of water, monitoring and control of purification process, treated water distribution, and control of pressure boost pumps (Luiijf, 2008).

SCADA systems have largely been dependent on customised operational technology—technology which requires in-person operation (Hassanzadeh *et al.*, 2020). However, according to Hassanzadeh et al. (2020), these SCADA infrastructure are increasingly overlapping operational technology with information technology systems, essentially exposing them remote or cyber tampering. SCADA systems that integrate IT into their operations tend to increase vulnerabilities in the system. However, due to the dispersed nature of water systems, employees have little choice but to access these system remotely to perform operational tasks (Hassanzadeh *et al.*, 2020), and if these individuals are compromised, the entire system becomes vulnerable to pending attack.

Third party personnel such as SCADA manufacturers, who are allowed to perform maintenance on SCADA systems, and who are usually given full access to these system are another source of risk. Luiijf, Ali and Zielstra (2011) indicate that managers in the water sector have raised this as an area of vulnerabilities. There exists many incidents where a lack of CSA can leave critical infrastructure, including water, vulnerable to cyber attacks. In many of the cases, the areas of vulnerability are simple issues, such as are password management, email use, internet use, and incident reporting.

3. Methodology

The purpose of this study is to develop a comprehensive measuring instrument to determine CSA of employees in the water industry. The study was conducted in four phases. A systematic literature review was conducted on publications by experts in the field to assess the tools that they have developed in the past, and how these tools were applied to study CSA levels (phase 1 and 2). The data from the identified literature was extracted and assessed (phase 3). This information was utilised to develop a measurement model based on other CSA tools previously tested in industry (phase 4). The following steps were followed in the development of the CSA measurement tool:

- Phase 1: Literature wide scope search, which included the initial search for publications from databases, application of exclusion criteria, screening by title and removal of duplicates and restricted content.
- Phase 2: Literature final content selection, which included validation of publication via abstract, full text quality appraisal process and backward referencing to identify additional content.
- Phase 3: Comparison of measurement theories, which included the identification of model base theory, selection of focus areas and measurement traits, as well as the identification of organisation type and status considerations.
- Phase 4: CSA model design, which included the selection of base theory, focus areas and measurement traits. It also included the consideration of water specific aspects and the final model development.

The execution of these phases will be discussed in detail in the following sections.

4. Search strategy and selection of relevant material

To avoid a random and distorted search process, a comprehensive search strategy was employed, to assure the reader of the level of diligence applied to complete the work presented (Meades, 2015). Systematic literature reviews have strict requirements for implementation of search strategies and the selection of relevant material (Snyder, 2019).

4.1 Phase 1: Literature wide scope search

To identify academic material that is considered relevant to the research objective, targeted searches were conducted using key terms often applied in the field of cyber security. The key terms were identified using a variation of the PICO (People, Intervention, Comparators, Outcome) model (Purssell and McCrae, 2020). This variation entails exposure (E) in place of intervention and the removal of Comparators - PEO. The question to be answered was: *What are the current instruments available to measure CSA in industry in general?* In accordance with the PEO model, the following answers were used to determine the search terms, where the final terms are shown in **Table 1**:

- **People** (representing the sample space under investigation): industry.
- **Exposure** (representing the level of exposure of people): cybersecurity awareness.
- **Outcome** (represents the outcome required): instrument to measure awareness levels.

Table 1: Key search terms and synonyms

Population	**Exposure**	**Outcome**		
Industry(ies)	*Cybersecurity*	*Awareness*	*Measurement*	*Instrument*
Organisation(s) Company(s) Employee Worker(s) Human Factor	Information security	Education Culture	Assessment Evaluation	Model Mechanism Tool Framework Questionnaire Study

For this study, six academic databases were explored to find all relevant publications that could assist in the development of a CSA measurement tool, which included Association for Computing Machinery Digital Library (ACMDL), Emerald, IEEE Xplore, ScienceDirect, SpringerLink and Taylor & Francis Online.

The initial search recorded a total of **24596** titles. After every search, a set of exclusion criteria was applied, which included: papers not published in English, papers not peer-reviewed, magazine and newspaper articles, papers not in used subscription lists, and papers published before 2011. After the exclusion of papers not adhering to the abovementioned criteria, a total of **5928** papers were retained. These papers were screened via titles, removing any papers which do not focus on CSA. After the removal of duplicates and papers which could not be accessed, a total of **120** papers were retained for full content selection.

4.2 Phase 2: Literature final content selection

After the completion of Phase 1 of the search process **120** publications were retained. The retained publications were screened by abstract. All publications that did not specifically discuss the development of a measurement instrument for CSA in the abstract were excluded. A total of **25** papers were retained after the abstract validation step.

For the full text analysis, the following research analysis question was used for the full text quality appraisal process: *Did the author develop an instrument to measure CSA levels*? This quality appraisal was used to determine to what degree the selected studies meet the criteria of the current study—the degree to which the studies answer each predefined research analysis questions were scored on a 5-point scale, ranging from irrelevant (1) to inch-perfect (5). A further 7 publications were excluded, leaving a total of **18** publications. Backward referencing was utilised to identify relevant content. Four articles were refenced in most of the studies analysed, and these articles were included in the current research, bringing the total number of papers to **22**, shown in **Table 2,** retained for further analysed to develop the measurement tool for CSA.

Table 2: List of publications for CSA model development

N°	Publication	Reference
1	Improving Security Awareness in the Government Sector	(Amjad *et al.*, 2016)
2	Securing Our Digital Natives: A Study of Commonly Experience Internet Safety Issues and a One-Stop Solution	(Agarwal and Singhal, 2017)
3	Cybersecurity workforce in railway: its maturity and awareness	(Kour and Karim, 2020)
4	Information security awareness and behavior: a theory-based literature review	(Lebek *et al.*, 2014)
5	Measurement of Employee Information Security Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case Study at PT. PQS	(Zulfia *et al.*, 2019)
6	Measuring the Information Security Awareness Level of Government Employees Through Phishing Assessment	(Ikhsan and Ramli, 2019)
7	Measurement of Employee Information Security Awareness: Case Study at A Government Institution	(Puspitaningrum *et al.*, 2018)
8	A quick cybersecurity wellness evaluation framework for critical organizations	(Jazri and Jat, 2017)
9	Measuring Information Security Awareness on Employee Using HAIS-Q: Case Study at XYZ Firm	(Cindana and Ruldeviyani, 2019)
10	Measurement of Employee Information Security Awareness Using Analytic Hierarchy Process (AHP): A Case Study of Foreign Affairs Ministry	(Normandia *et al.*, 2019)
11	A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument	(Da Veiga, 2016)
12	Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)	(Parsons, McCormac, Butavicius, *et al.*, 2014)
13	The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies	(Parsons *et al.*, 2017)
14	Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions	(Nunes, Antunes and Silva, 2021)
15	Information Security Behavior: Development of a Measurement Instrument Based on the Self-determination Theory	(Gangire, Da Veiga and Herselman, 2020)

N°	Publication	Reference
16	Semi-automated Information Security Risk Assessment Framework for Analyzing Enterprises Security Maturity Level	(Abazi and Kő, 2019)
17	Cyber Security Awareness, Knowledge and Behavior: A Comparative Study	(Zwilling *et al.*, 2020)
18	A Model of Information Security Awareness for Assessing Information Security Risk for Emerging Technologies	(Mejias and Balthazard, 2014)
19	A prototype for assessing information security awareness	(Kruger and Kearney, 2006)
20	A study of information security awareness in Australian government organisations	(Parsons, McCormac, Pattinson, *et al.*, 2014)
21	Analysis of personal information security behaviour	(Öɬütçü *et al.*, 2016)
22	Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours.	(Hadlington, 2017)

5. Development of CSA Measurement Instrument

This section details the analysis of the articles selected to construct an inclusive CSA measurement tool for the assessment of CSA levels in organisations of interest. Existing models were analysed for similarities, differences, advantages and disadvantages, and a coherent model is proposed based on the analysis.

5.1 Phase 3: Comparison of measurement theories

In phase 3, the selected articles were analysed to identify which base theory was utilised to measure the CSA of the employees in the study. **Table 3** summarises the top base theories used in the selected studies.

Table 3: Summary of recurrence of base theory

N°	Base theory	Utilised in selected articles
1	Knowledge, Attitude, Behaviour model (KAB)	10
2	Human Aspect of Information Security-Questionnaire (HAIS-Q)	8
3	Risky cybersecurity behaviour scale (RScB)	2
4	Attitude Towards Cybersecurity and Cybercrime in Business (ATC-IB)	2
5	ISO 27001	2
6	General deterrence theory (GDT)	2

One of the most popular models on which ten of CSA measurement models in the retained literature were developed was borrowed from the field of social psychology (Kruger and Kearney, 2006). This model is called the Knowledge, Attitude, Behaviour (KAB) Model. Parsons, McCormac, Butavicius et al. (2014), Parsons, McCormac, Pattinson et al. (2014) and Parsons et al. (2017) developed the Human Aspect of Information Security-Questionnaire (HAIS-Q) which was based on the KAB Model discussed by Kearney and Kruger (2006). The HAIS-Q model itself appeared in eight different studies. Other models that appeared in the publications included: Risky cybersecurity behaviour scale (RScB), Attitude Towards Cybersecurity and Cybercrime in Business (ATC-IB), ISO 27001 and General deterrence theory (GDT). Each model had varying areas on which they focused with regards to measuring the CSA of employees. The focus areas for each model were counted and the top recurring focus areas throughout the analysed studies determined. **Table 4** shows a summary of how many times each entry was measured in the selected publications.

Table 4: Summary of number of articles that measured this focus area

N°	Focus area	Times measured in selected articles
1	Internet use	15
2	Password management	14
3	Mobile devices	14
4	Email use	13
5	Social media use	13
6	Incident reporting	12
7	Information handling	10
8	IS policy adherence	6

The selected studies also focused on measurement certain traits possessed by the subjects for which CSA had to assessed. The authors focused on different traits in order to determine what the level of CSA was for a given set of employees in each organisation evaluated. The most recurring traits were the knowledge, attitude, and

behaviour of the employees. The selected studies focused mainly on 3 types of institutions: public organisations, private organisations and academic institutions.

5.2 Phase 4: CSA Model design

Based on the comparison of the different models, the most popular method relied upon by the majority of the authors the HAIS-Q model, which is based on the KAB model, developed by Kruger and Kearney (2006). They developed a measurement model pegged to three dimensions pertaining to human cognition: knowledge (what you know), attitude (what you think), and behaviour (what you do) (KAB), which each had varying importance levels according to the study. The model developed by Kruger and Kearney (2006) followed strict guidelines of sustainability, ease of use, use of scientific methods, and compliance to the organisation of interest's unique requirement. The approach used by Parsons et al. (2017) in each publication was slightly improved with each iteration. Parsons, McCormac, Butavicius, et al. (2014) outlined the development of HAIS-Q and its connection to the KAB model in their 2014 publication after running a test trial with 500 Australian Employees. The model identified seven focus areas : password management, email use, internet use, social networking sites, mobile computing, information handling, and incident reporting—as opposed to the six proposed by Kruger and Kearney (2006) with social media not being an area of interest at the time. The wide use of HAIS-Q which has also been referenced in numerous publications geared towards measuring the CSA levels in a myriad of organisations makes HAIS-Q a reliable model for further study. Puspitaningrum et al. (2018), Normandia et al., (2019), Cindana and Ruldeviyani (2019), (Zulfia *et al.*, 2019) all based their measurement instruments on the HAIS-Q model. They assessed varying areas and types of organisations from government to private sector employees. The KAB and HAIS-Q models were therefore selected based on popularity with other authors.

5.2.1 Focus areas selection

The selection of the focus areas was done by popularity (see **Table 5**). These focus areas were selected because of how many times they were measured by previous authors. **Table 5** shows which focus arears are common to the different studies and how the current study was developed based on the focus areas previously studied by the experts.

Table 5: Similarities of focus areas in KAB, HAIS-Q and current study

KAB Model	HAIS-Q model	Current study
	Focus areas	
Adhere to policies	-	Adhere to policies
Action -› Consequences	-	-
Password management	Password management	Password management
Email use	Email use	Email use
Internet use	Internet use	Internet use
Mobile computing	Mobile computing	Mobile computing
Incident reporting	Incident reporting	Incident reporting
-	Information handling	Information handling
-	Social networking sites	Social networking sites

5.2.2 Key measurement traits selection

Similar to the selection of focus areas, the measurement traits were also selected based on popularity with previous academic publications by authors in the field of interest. The most popular measurement traits after the data extraction process were: Knowledge, Attitude, and Behaviour.

5.3 Model development

The knowledge and attitude aspects of the questionnaire remained generally unaltered, following the traditional methodology of the HAIS-Q model. For this section, respondents will rate the items from 1-5 (where 1 = Strongly Disagree and Strongly Agree) However, items under the behavioural segment of the questionnaire followed the methodology applied in the RScB model, where respondents answered the questions based on retrospective behaviour in the 6 months that precede the evaluation. This was done because the author considers retrospective behaviour more indicative of the respondent's level of awareness than simply having to agree or disagree on what the right behaviour should be in the different instances. The behavioural aspect of the HAIS-Q model was modified to fit RScB model and focus more on retrospective behaviour. The respondents will rate on a scale of 1-5 (where 1 = Never and 5 = Daily or almost daily), how often they engaged in a particular behaviour 6 month prior to the evaluation. The model covers all aspects discussed in the present study and can be used to assess the CSA levels of employees in the water sector by collecting data based on the response of each

individual. A total of 22 questions in 8 focus areas (shown in **Table 5**) forms the final measurement model. A summary of the measurement model, with selected questions from each focus area, can be seen in **Appendix A**).

6. Conclusion

This study documents the process of the development of a model to test cybersecurity awareness in the water sector. This study was based on generic measurement instruments which were not specific to the water sector (although an effort was made to draw parallels between both test cases). Future work includes the utilisation of this measurement model to determine the CSA levels of employees in this sector.

Considering how important CSA is in the water industry, a reliable CSA measurement tool can greatly assist in determining the level of CSA of employees in the sector and assist in the improvement of the security of the systems in this sector. From this study, it can be recommended organisations should invest more resources into evaluating the level of CSA of their employees, especially in the water sector because employees can prove to be the point of entry for some of the most disastrous attack as demonstrated by Hassanzadeh *et al.* (2020). This study also recommends that after performing a diagnostic on the level of CSA of employees, training programs focusing on all areas of weakness should be organised to improve the general level of CSA amongst employees and management.

References

Abazi, B. and Kő, A. (2019) Semi-automated Information Security Risk Assessment Framework for Analyzing Enterprises Security Maturity Level, Lecture Notes in Business Information Processing. Springer International Publishing. doi: 10.1007/978-3-030-37632-1_13.

Agarwal, C. and Singhal, A. (2017) 'Securing our digital natives: A study of commonly experience internet safety issues and a one-stop solution', ACM International Conference Proceeding Series, Part F1280, pp. 178–186. doi: 10.1145/3047273.3047303.

Amjad, H. A. R., Zaffar, M. F., Naeem, U., Choo, K. K. R. and Zaffar, M. A. (2016) 'Improving security awareness in the government sector', ACM International Conference Proceeding Series, 08-10-June, pp. 1–7. doi: 10.1145/2912160.2912186.

Cindana, A. and Ruldeviyani, Y. (2019) 'Measuring information security awareness on employee using HAIS-Q: Case study at XYZ firm', in 2018 International Conference on Advanced Computer Science and Information Systems, ICACSIS 2018. Institute of Electrical and Electronics Engineers Inc., pp. 289–294. doi: 10.1109/ICACSIS.2018.8618219.

Gangire, Y., Da Veiga, A. and Herselman, M. (2020) Information Security Behavior: Development of a Measurement Instrument Based on the Self-determination Theory, IFIP Advances in Information and Communication Technology. Springer International Publishing. doi: 10.1007/978-3-030-57404-8_12.

Hadlington, L. (2017) 'Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours.', Heliyon, 3. Available at: https://reader.elsevier.com/reader/sd/pii/S2405844017309982?token=825F4D5FD0127B0A8C8C470FC3E81D1ABB4BC845138F39113801012ACC189AF4CB663406D5E4486B841DB671AD4F3925.

Hasan, S., Ali, M., Kurnia, S. and Thurasamy, R. (2021) 'Evaluating the cyber security readiness of organizations and its influence on performance', Journal of Information Security and Applications, 58, p. 102726. doi: 10.1016/j.jisa.2020.102726.

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A. and Banks, M. K. (2020) 'A review of cybersecurity incidents in the water sector', Journal of Environmental Engineering, 146. doi: 10.1061/(asce)ee.1943-7870.0001686.

Ikhsan, M. G. and Ramli, K. (2019) 'Measuring the Information Security Awareness Level of Government Employees Through Phishing Assessment', 34th International Technical Conference on Circuits/Systems, Computers and Communications, ITC-CSCC 2019, pp. 16–19. doi: 10.1109/ITC-CSCC.2019.8793292.

Jazri, H. and Jat, D. S. (2017) 'A quick cybersecurity wellness evaluation framework for critical organizations', Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016. doi: 10.1109/ICTBIG.2016.7892725.

Kong, H. K., Kim, T. S. and Kim, J. (2012) 'An analysis on effects of information security investments: A BSC perspective', Journal of Intelligent Manufacturing, pp. 941–953. doi: 10.1007/s10845-010-0402-7.

Kour, R. and Karim, R. (2020) 'Cybersecurity workforce in railway: its maturity and awareness', Journal of Quality in Maintenance Engineering. doi: 10.1108/JQME-07-2020-0059.

Kruger, H. A. and Kearney, W. D. (2006) 'A prototype for assessing information security awareness', Computers and Security, 25(4), pp. 289–296. doi: 10.1016/j.cose.2006.02.008.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and Breitner, H. M. (2014) 'Information security awareness and behavior: a theory-based literature review', Management Research Review, 37(12), pp. 1049–1092.

Luiijf, E. (2008) TNO report SCADA Security Good Practices for the Drinking Water Sector TNO | Knowledge for business SCADA Security Good Practices for.

Luiijf, E., Ali, M. and Zielstra, A. (2011) 'Assessing and improving SCADA security in the Dutch drinking water sector', International Journal of Critical Infrastructure Protection, 4(3–4), pp. 124–134. doi: 10.1016/j.ijcip.2011.08.002.

Meades, P. (2015) Doing a literature review in health and social care: a practical guide, British Journal of Guidance & Counselling. doi: 10.1080/03069885.2014.975101.

Mejias, R. J. and Balthazard, P. A. (2014) 'A Model of Information Security Awareness for Assessing Information Security Risk for Emerging Technologies', Journal of Information Privacy and Security, 10(4), pp. 160–185. doi: 10.1080/15536548.2014.974407.

Normandia, Y., Kumaralalita, L., Hidayanto, A. N., Nugroho, W. S. and Shihab, M. R. (2019) 'Measurement of employee information security awareness using analytic hierarchy process (AHP): A case study of foreign affairs ministry', Proceedings - 2018 4th International Conference on Computing, Engineering, and Design, ICCED 2018, pp. 52–56. doi: 10.1109/ICCED.2018.00020.

Nunes, P., Antunes, M. and Silva, C. (2021) 'Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions', Procedia Computer Science, 181(2019), pp. 173–181. doi: 10.1016/j.procs.2021.01.118.

Öɬütçü, G., Testik, Ö. M. and Chouseinoglou, O. (2016) 'Analysis of personal information security behavior and awareness', Computers and Security, 56, pp. 83–93. doi: 10.1016/j.cose.2015.10.002.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017) 'The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies', Computers and Security, 66, pp. 40–51. doi: 10.1016/j.cose.2017.01.004.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', Computers and Security, 42, pp. 165–176. doi: 10.1016/j.cose.2013.12.003.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. and Jerram, C. (2014) 'A study of information security awareness in Australian government organisations', Information Management and Computer Security, 22(4), pp. 334–345. doi: 10.1108/IMCS-10-2013-0078.

Puspitaningrum, E. A., Devani, F. T., Putri, V. Q., Hidayanto, A. N., Solikin and Hapsari, I. C. (2018) 'Measurement of employee information security awareness: Case study at a government institution', Proceedings of the 3rd International Conference on Informatics and Computing, ICIC 2018. doi: 10.1109/IAC.2018.8780571.

Rantapelkonen, J. and Salminen, M. (2013) 'The Fog of Cyber Defence', Department of Leadership and Military Pedagogy Publication, 2(10), p. 236. Available at: http://www.doria.fi/bitstream/handle/10024/88689/The Fog of Cyber Defence NDU 2013.pdf?sequence=1&isAllowed=y.

Snyder, H. (2019) 'Literature review as a research methodology: An overview and guidelines', Journal of Business Research, 104(August), pp. 333–339. doi: 10.1016/j.jbusres.2019.07.039.

Strupczewski, G. (2021) 'Defining cyber risk', Safety Science, 135. doi: 10.1016/j.ssci.2020.105143.

The White House (2013) 'Presidential Policy Directive Critical Infrastructure Security and Resilience.', Technical report.

Da Veiga, A. (2016) 'A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument', Proceedings of 2016 SAI Computing Conference, SAI 2016, pp. 1006–1015. doi: 10.1109/SAI.2016.7556102.

Zulfia, A., Adawiyah, R., Hidayanto, A. N. and Fitriah Ayuning Budi, N. (2019) 'Measurement of Employee Information Security Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case Study at PT. PQS', 5th International Conference on Computing Engineering and Design, ICCED 2019. doi: 10.1109/ICCED46541.2019.9161120.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H. N. (2020) 'Cyber Security Awareness, Knowledge and Behavior: A Comparative Study', Journal of Computer Information Systems, 00(00), pp. 1–16. doi: 10.1080/08874417.2020.1712269.

Appendix A: Summary of measurement model

Sub Focus Area	Knowledge	Attitude	Behaviour	Behaviour (RScB modification)
Focus Area: IS Policy adherence				
Adhering to IS Policy	It's acceptable to ignore IS protocol set out by management and IT department. *	No serious consequence can result from not following safety protocol at all times at work.	None	Ignores safety protocols because they are difficult or inconveniencing to follow at all times.
Focus Area: Password Management				
Using the same password	It's acceptable to use my social media password on my work accounts. *	It's safe to use same password for social media and work accounts. *	I use a different password for my social media and work accounts.	How often you use your social media password on your work accounts?
Focus Area: Email Use				
Clicking on links in emails from known senders	I am allowed to click on any links in the emails from people I know. *	It's always safe to click on links in emails from people I know. *	I don't always click on links in emails just because they come from someone just because they come from someone I know.	Clicked on a link in an email that came from someone you know without appropriate verification
Focus Area: Internet use				
Downloading files	I am allowed to download any files onto mu work computer if they help me to do my work. ^	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done. *	Downloaded files you considered necessary for work on your work computer.
Focus Area: Social media use				
SM Privacy settings	I must periodically review the privacy settings on mu social media accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings. *	Reviewed your social media privacy settings.
Focus Area: Mobile device				
Physically securing mobile device	When working in a public place, I have to keep my laptop with me at all times.	When working in a café, it's safe to leave my laptop unattended for a minute. *	When working in a public place, I leave my laptop unattended.	Left your laptop unattended in a public place.
Focus Area: Information handling				
Disposing of sensitive print-outs	Sensitive print-outs can be disposed of in the same way as non-sensitive ones. *	Disposing of sensitive print-outs by putting them in the rubbish bin is safe. *	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.	Shredded or destroyed sensitive print-outs before disposing of them.
Focus Area: Incident reporting				
Reporting suspicious behaviour	If I see someone acting suspiciously in my workplace, I should report it.	If I ignore someone acting suspiciously in my workplace, nothing bad can happen. *	If I saw someone acting suspiciously in my workplace, I would do something about it.	Intervened after noticing someone acting suspiciously at your work place.

(*Reverse scoring should be used for this item)