Information Security Behavior: Development of a Measurement Instrument Based on the Self-determination Theory

Yotamu Gangire, Adéle Da Veiga, Marlien Herselman

Information security behavior: Development of a measurement instrument based on the self-determination theory

Yotamu Gangire[1][0000-0001-8951-6211], Adéle Da Veiga[1] [0000-0001-9777-8721], Marlien Herselman [1,2] [0000-0003-1089-3925]

[1] School of Computing, College of Science, Engineering and Technology, University of South Africa (UNISA), Florida Campus, Johannesburg, South African [2] Next Generation Enterprises and Institutions, CSIR, Pretoria, South Africa
ygangire@gmail.com, dveiga@unisa.ac.za, mherselman@csir.co.za

Abstract. Employee information security behaviour is important in securing an organisation's information technology resources. Employees can act in a risky or secure manner. Improving employee information security behaviour is important for organisations and should follow an assessment of their behaviour. A robust measuring instrument is a necessity for effectively assessing information security behaviour. In this study, a questionnaire was developed based on the Human Aspects of Information Security Questionnaire and self-determination theory and validated statistically. Data obtained through a quantitative survey (N = 263) at a South African university was used to validate the questionnaire. The result is a questionnaire that has internally consistent items, as shown by the results of the reliability analysis. Universities can use the questionnaire to identify developmental areas to improve information security from a behaviour perspective.

Keywords: information security, information security behaviour, information security policy (ISP), compliance, self-determination theory (SDT)

1 Introduction

Employee information security behaviour is important in ensuring that information and other information technology (IT) resources are secure in the organisation [1, 2]. However, employees contribute significantly to the information security threats and breaches in the organisation [3, 4]. PricewaterhouseCoopers reports that insiders such as employees, suppliers, consultants and contractors, could be responsible for 30% of the reported incidents [5]. Security breaches can have unpleasant consequences, some of which are: loss of productivity, theft of information assets, system downtime, destruction of IT infrastructure, damage to the organisation's reputation, and the organisation may face lawsuits, fines and regulatory actions [6].

There is a need to understand what influences compliance with information security policies (ISPs) [7, 8]. Understanding employees' information security behaviour, is an

important step in the assessment and consequently the improvement of information security behaviour [9]. Hence there is a need to assess and evaluate employees' information security awareness [10].

Some studies on employee information security behaviour are based on theories for example, the study by Safa, et al. [1] was based on the protection motivation theory and the theory of planned behaviour (TPB); the study by Ifinedo [11] used the TPB, social bond theory and the social control theory and the study by Kranz and Haeussinger [12] used the TPB and the self-determination theory (SDT). These studies aimed to validate a particular theory, hence they only assessed the variables in the theory under investigation while other variables were not considered. However, employee information security behaviour is influenced by many factors besides variables from theories [13]. This study develops an instrument based on themes from the Human Aspects of Information Security Questionnaire (HAIS-Q) [13] and the information security compliant behaviour model based on the SDT ($ISCBM^{SDT}$) [14]. This not only contributes to the theory validation of the SDT variables, but combines these with the themes of the HAIS-Q, thereby including more variables in the assessment instrument.

The aim of this study is to develop and validate an information security behaviour questionnaire to assess the influence of perceived competence, perceived relatedness and perceived autonomy on information security behaviour. The study postulates that perceptions of competence, relatedness and autonomy influence efficacy and hence the intention to comply with ISPs. It is therefore, intended that a positive perception of competence, relatedness and autonomy will help mitigate the risk of ISP non-compliance and that developing a questionnaire can aid in measuring and determining this. It is also aimed at outlining the development of this instrument, including the validity and reliability testing of the questionnaire. The instrument could be used to assess employee information security behaviour from the perspective of the SDT. To achieve these aims, a survey was carried out at a South African university using the information security behaviour questionnaire. This paper is structured as follows: Section 2 gives an overview of the information security behaviour and Section 3 describes the research methodology. The results of the survey and statistical validation of the questionnaire are discussed in Section 4. This is followed by the limitations and future directions in Section 5 and the conclusion in Section 6.

2 Information security behaviour

Pattinson et al.[15] refer to information security behaviour as the behaviour performed by computer users, which can be either intentionally risky behaviour or intentionally secure behaviour. According to Guo [16] employee security behaviour can be desirable or undesirable. Desirable behaviour is ISP compliant whereas undesirable behaviour is not. Examples of secure behaviour include taking precautions and reporting security incidents [16]. Employees can also exhibit behaviour aimed at preventing security breaches by taking fewer risks. Other employees engage in inappropriate security behaviour, including using the default security password and relying on the computer to

auto-lock when they leave their desk. Employees can also engage in behaviour that aid business continuity and recovery; these employees back up their data and inform colleagues of security issues [17]. It is argued that when employees comply with the ISPs, information security threats are reduced [18].

Alfawaz, Nelson and Mohannak [19] propose security behaviour modes as the knowing-doing mode, knowing-not doing mode, not knowing-doing mode and not knowing-not doing mode. In the not knowing-not doing mode, employees violate information security rules, because they do not know the organisation's information security rules and do not have any security knowledge [19]. In the not knowing-doing mode, employees do not know the information security rules and do not have security knowledge but still exhibit the right security behaviour. These are employees who will ask their co-workers before taking certain actions. In the knowing-not doing mode, employees know the rules and have the necessary security knowledge and skills, but still violate the rules [19]. In the knowing-doing mode, employees know the rules, have the necessary security skills and comply with the rules [19].

Ahmad, Norhashim, Song, & Hui [20] group employees into four types on the basis of whether or not they know the security rules and whether or not they comply with the information security rules. They classify them as discerning, obedient, rebel and oblivious employees. Discerning individuals conform to the information security rules because they have the necessary knowledge; some employees conform to the information security rules not because they have the knowledge but because they follow organisational rules just because they are there; some employees choose not to conform to information security rules despite having the knowledge; and other employees compromise information security because they do not have the security knowledge [20].

Alfawaz et al.[19] and Ahmad et al. [20] propose classification of employees' information security behaviour that also explain why employees fail to comply with organisational ISPs. They postulate that employees fail to comply because they are ignorant of the regulations, they choose not to or they are not competent due to lack of security knowledge. Their classifications suggest that in order for employees to comply with the ISPs, they have to be equipped with the relevant security knowledge and skills. Employees will also have to actively think about the security implications of their actions when they do their work. Therefore, security awareness, knowledge and experience are important [1]. Users must also understand their responsibilities regarding information security because an employee who lacks information security awareness is more vulnerable to information security attacks [21].

2.1 Information Security Compliant Behaviour Model

The Information Security Compliance Behavior Model ($ISCBM^{SDT}$) is based on the three concepts of the SDT, which are the need for competence, the need for relatedness and the need for autonomy. The three basic psychological needs are regarded as some of the sources contributing to intrinsic motivation [22, 23]. The need for autonomy is the perception that one is acting out of one's own volition and that one's behaviour is

self-determined. The need for relatedness refers to the desire be attached to others. Competence is the belief of being capable and effective [22]. The ISCBM^{SDT} postulates that when perceived competence, perceived relatedness and perceived autonomy are fulfilled, the employees will comply with the ISP because it is their choice to do so [14]. The questionnaire developed for this study is based on the ISCBM^{SDT} and the questionnaire themes/focus areas are discussed next.

2.2 Information security behaviour themes

The focus areas from the HAIS-Q were mapped to the three concepts of the SDT resulting, in each focus area focusing on competence, relatedness and autonomy. The themes are as follows.

Password management
This involves understanding how to protect information system resources by using strong and secure passwords. This includes regularly changing passwords, choosing strong passwords and not sharing passwords [17, 24, 25]

Email usage
Employees have to understand safe email use. This includes not downloading unsafe attachments, clicking on links in email from known or unknown senders and opening attachments in emails from unknown senders [1, 15, 17, 21, 24, 26].

Internet usage
Employees should know how to use the internet safely. This includes downloading files, accessing dubious websites and entering information online [15, 18, 26, 27].

Social media usage
Employees should understand safe usage of social media. This includes social media privacy settings, considering the consequences of posting information and acting responsibly regarding posting about work on social media [27].

Mobile devices usage
Employees should understand how to secure their mobile devices, which carry work information when working in a public area. This includes physically securing mobile devices, sending sensitive information via public Wi-Fi and guarding against shoulder surfing [27, 28].

Information handling
Employees have to understand how to handle sensitive information. This includes disposing of sensitive print-outs, inserting removable media in work computers and leaving sensitive material on work areas [17, 27, 29]

Privacy

Employees should understand how to handle personally identifiable information. This includes non-disclosure of sensitive information [1, 17], processing client information in a lawful manner [30], processing client information for the purpose for which it was collected[30, 31], and adhering to the organisation's privacy policy [32]. When employees adhere to the privacy policy they can uphold the privacy of student data they handle. Parsons et al. [33] propose that the link between information security awareness and privacy should be investigated. Table 1 shows an extract of items in the competence, relatedness and autonomy category.

Table 1. Questionnaire items extract

Focus Area	Competence	Relatedness	Autonomy
Password management	1. I have the necessary skills to use different passwords for social media and work accounts.	My colleagues support me to use different passwords for social media and work accounts.	I choose to use different passwords for social media and work accounts.
	2. I have the necessary skills to never share my work passwords with colleagues.	My colleagues support me never to share my work passwords with colleagues.	I choose never to share my work passwords with my colleagues.
	3. I have the necessary skills to use a combination of letters, numbers, and symbols in work passwords.	My colleagues support me to use a combination of letters, numbers, and symbols in work passwords.	I choose to use a combination of letters, numbers, and symbols in work passwords.
Email usage	4. I have the necessary skills to click only on links in emails from people I know.	My colleagues support me to click only on links in emails from people I know.	I choose to click only on links in emails from people I know.
	5. I have the necessary skills to avoid clicking on links in emails from people I do not know.	My colleagues support me to avoid clicking on links in emails from people I do not know.	I choose to avoid clicking on links in emails from people I do not know.
	6. I have the necessary skills to identify when it is risky to	My colleagues support me to identify when it is risky to	I choose to avoid opening attachments

Focus Area		Competence	Relatedness	Autonomy
		open attachments in emails from people I do not know.	open attachments in emails from people I do not know.	in emails from people I do not know.
Internet usage	7.	I have the necessary skills to identify when it is risky to download files onto my work computer.	My colleagues support me to identify when it is risky to download files onto my work computer.	I choose not to download risky files onto my work computer.
	8.	I have the necessary skills to avoid accessing websites that could be dubious (malicious).	My colleagues support me to avoid accessing websites that could be dubious (malicious).	I choose to avoid accessing websites that could be dubious (malicious).
	9.	I have the necessary skills to assess the safety of a website before entering information online.	My colleagues support me to assess the safety of a website before entering information online.	I choose to assess the safety of a website before entering information online.

3 Methodology

This study adopted the positivist research paradigm with a quantitative approach. In the positivist research paradigm researchers prefer to work with observable and measurable reality. Positivists use quantitative methods in their research and the research is based on the testing of theories [34, 35]. The survey strategy was chosen and the questionnaire was used for data collection at a university in South Africa. A non-probability purposive sampling method was used. With purposive sampling the researcher deliberately selects the sample for example because they are easy to reach or are available [34]. The selection of the expert panel was done using the purposive sampling method based on the following criteria: they had all done research work in information security and had experience in information security awareness. The pilot sample was selected using convenience sampling in one of the university's departments. The survey participants were selected using purposive sampling. The survey questionnaire was sent electronically to the entire population of administrative and academic staff. Ethical clearance was obtained from the university, adhering to the research ethics policy that focuses on aspects such as anonymity, voluntary participation, confidentiality and consent for participation.

The following statistical tests were performed: ANOVA, t-test and Pearson correlation analysis. ANOVA was carried out to determine if there were significant differences among the demographical groups for age, job level, level of education and length of service groups. The t-test were performed to determine if the mean scores among the gender groups had any significant differences. The correlation analysis was carried out to determine if there was any correlation among the resulting factors from the exploratory factor analysis.

3.1 Questionnaire

A Likert scale (strongly agree, agree, unsure, disagree and strongly disagree) was used to answer the statements. The questionnaire had two sections: Section 1 which was for biographical information and Section 2 which comprised the information security behaviour questions. The final questionnaire had 75 questions: 25 questions for each of the SDT categories.

3.2 Expert panel reviews

A panel of experts in the research area evaluated the questionnaire. This helped to refine and improve the questionnaire [35]. The questionnaire was reviewed by a panel of six experts, four of whom were from the field of psychology (human factors scientists) who had researched the human aspects of cyber security for 11 years and had developed the HAIS-Q. The other two were an academic in information security and an IT security consultant specialising in incident response and awareness. The reviewers had 10 to 20 years of working experience. They pointed out that some of questions were not clear and others addressed two different aspects in one question. The questionnaire was updated and sent for pilot testing.

3.3 Pilot testing

The pilot test was conducted among 12 staff members in one of the departments in the university. The questionnaire pilot test showed that some questions were not worded clearly and it was recommended that job level be added to the biographical section.

3.4 Main study

The updated questionnaire was prepared and administered using Google Forms over the internet and participants were notified by an email invitation sent by the ICT department of the university. The email contained information on the research and the links for completing the online questionnaire. The participants were required to read the information sheet and the consent form. If they consented to participate in the study, then they proceeded to complete the online questionnaire

4 Results

Two hundred and sixty-three (263) responses were received from the online survey. The sample consisted of 54.8% females, 44.1% males and 1.1% did not disclose their gender. Those born between 1977 and 1995 were the largest group of respondents (38.40%). The highest number of survey respondents (69.08%) was from the group with postgraduate qualifications. There were more respondents from the groups with higher qualifications (i.e. the higher the qualification the higher the number of respondents). This is consistent with a university environment. Those who had worked for six to ten years were the largest group (27.38%) and most of the respondents were administrative staff (51.53%). The results of the survey are reported next.

A cut-off of 4.0 for the means was set for the information security behaviour questions [36]. A mean score of 4.0 and above indicated a positive perception, while a mean score below 4.0 indicated a neutral or potentially negative perception.

For the competence questions, the top 10 questions all had means above 4.0. This suggests that the respondents had a positive perception of the competence questions. Of the bottom 10 questions, five had means above 4.0 and five had means below 4.0, indicating areas for which further improvement is required.

For the relatedness questions, the mean values for the top statements ranged from 3.05 to 3.51 and the mean values for the bottom statements ranged from 2.68 to 3.01. These mean values for both top questions and bottom questions show that all had means below 4.0. This suggests that the participants had neutral and potentially negative perceptions of the relatedness questions, indicating areas requiring further improvement.

For the autonomy questions, the mean values for the top statements ranged from 4.41 to 4.68 and the mean values for the bottom statements ranged from 3.91 to 4.27. The top questions all had means above 4.0, suggesting that the respondents had a positive perception of the autonomy questions. For the bottom 10 questions, eight questions had means above 4.0 and two had means below 4.0. The two questions with means below 4.0 indicate areas were further improvement is required.

The results of the Pearson correlation showed that the competence and autonomy factors had a statically significant positive correlation ($r >= .287$, $n=263$, $p < .05$), two tailed. The correlation for the competence and relatedness factors show that some factors had a positive correlation ($r >= .224$, $n=263$, $p < .05$), two tailed and other factors did not. The correlation results for the autonomy and relatedness factors showed that some factors had a positive correlation ($r >= .134$, $n=263$, $p < .05$), two tailed and others did not.

The results of the information security behaviour questions suggest that the respondents had a more positive perception of the competence and autonomy questions than of the relatedness questions. The Pearson correlation results show a positive correlation between competence and autonomy, suggesting that the respondents who perceive themselves to be competent also felt confident about their autonomy perception.

4.1 Validation of the instrument

Factor analysis

Exploratory factor analysis (EFA) was carried out to determine the underlying relationships between the variables [37], as well as the construct validity of the questionnaire [38]. O'Rourke and Hatcher [39] suggests that to achieve a sample size that is statistically adequate to carry out questionnaire validation, the responses or the collected data must be at least five times the number of questions in the questionnaire. The EFA was done for each category and new factors were determined per category. Since each category had 25 questions, a minimum of 125 responses were required per category. The recommendation of O'Rourke and Hatcher [39] and the received responses were sufficient to carry out the statistical validation of the questionnaire and the data was processed using SPSS Version 25.

Determining the number of factors

The Kaiser-Meyer-Olkin (KMO) test and the Bartlett sphericity tests were conducted for each of the three categories competence, relatedness and autonomy. Field [40] recommends a KMO value closer to 1 in order to produce distinct and reliable factors. For the Bartlett sphericity test, the probability should be less or equal to 0.05; this shows highly correlated variables [38]. The KMO for the competence statements was 0.915 and the Bartlett sphericity test result was statistically significant ($p = 0.000$). The KMO for the relatedness statements was 0.965 and the Bartlett sphericity test result was statistically significant ($p = 0.000$). The KMO for the autonomy statements was 0.885 and the Bartlett sphericity result was statistically significant ($p = 0.000$). As a result, all categories met the criteria for performing the EFA.

The factors were determined using the Eigenvalues, scree plots and cumulative percentages [41]. The item loading cut off was 0.4, as Stevens [42] suggests that item loading values should be greater than 0.4. The cumulative percentage had to be above 60% and the Eigenvalues had to be greater than 1. Competence statements resulted in four factors and these had Eigenvalues greater than 1 and a cumulative Eigenvalue of 62.38%. Relatedness statements resulted in two factors and these had Eigenvalues greater than 1 and a cumulative Eigenvalue of 70.74%. The autonomy statements resulted in six factors and these had Eigenvalues greater than 1 and a cumulative Eigenvalue of 63.68%.

Table 2 shows the resulting factors. For the competence statements, Factor 3 Statement 25 was removed as it had a factor cross-loading with a cross-loading difference of less than 0.2. Factor 4 was dropped as it had only one item, Statement 3 and factors for the competence category were reduced to 3. For the relatedness category, Questions 17 and 18 were dropped as they had cross-loading differences less than 0.2. For the autonomy category Statements 1, 2, 3, 14, 17 and 18 were dropped because they had loadings below 0.4.

Table 2. Resulting factors

Category	Factor	Statements
Competence	Factor 1	1, 10, 11, 12, 14, 15, 16, 18, 19, 20, 21
	Factor 2	4, 5, 6, 7, 8, 9, 17
	Factor 3	22, 23, 24
Relatedness	Factor 1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16
	Factor 2	19, 20, 21, 22, 23, 24, 25
Autonomy	Factor 1	8, 9, 10
	Factor 2	4, 5, 6, 7
	Factor 3	22, 23
	Factor 4	19, 20, 21
	Factor 5	24, 25
	Factor 6	11, 12, 13, 15, 16

Naming the factors

The factors shown in Table 2 were named to reflect the common themes of the statements grouped under that factor.

Competence

Factors in this category reflect the employee's competence/skills to carry out the information security actions. The employees are confident that they can protect the IT resources because they have necessary skills to do so. For the competence statements, Factor 1 (11 items) was named *employee skills for data safety awareness*, Factor 2 (seven items) was named *employee skills for email and website safety and* Factor 3 (four items) was named *employee skills for privacy awareness*.

Relatedness

Factors in this category reflect the employee's need for support from colleagues to carry out information security actions. The employees perceive that they can protect the IT resources if co-workers and superiors support them. For the relatedness statements, Factor 1 (16 items) was labelled *organisational support for employee device and information protection awareness* and Factor 2 (seven items) was named *organisational support for employee information and privacy protection awareness*.

Autonomy

Factors in this category reflect the employees' need to be in control of their information security behaviour. The employees perceive that when they are in control of their information security behaviour they can protect the IT resources of their organisation. For the autonomy statements, Factor 1 (three items) was named *employee choice*

on privacy awareness, Factor 2 (four items) was named *employee choice to avoid malicious emails and downloads*, Factor 3 (two items) was named *employee choice to keep privacy of student personal information*, Factor 4 (three items) was named *employee choice to report bad security behaviour*, Factor 5 (two items) was named *employee choice to adhere to information security and privacy policies* and Factor 6 (five items) was named *employee choice to keep devices and information secure*.

Two autonomy factors, *employee choice to keep privacy of student personal information* and *employee choice to adhere to information security and privacy policies*, had two statements each. They were retained because both factors had very good reliability as shown in Table 3.

4.2 Reliability analysis

The Cronbach alpha coefficient was calculated for each of the 11 factors. Reliability refers to how consistent or dependable the measuring instrument is, and whether under similar conditions the measuring instrument produces consistent results [43]. According to Gerber and Hall [41], the Cronbach alpha coefficient can be interpreted as follows: good for values greater than 0.8, acceptable for values between 0.6 and 0.8, unacceptable for values less than 0.6. Table 3 shows the results of the Cronbach alpha values for the 11 factors. All the Cronbach alpha results were above 0.7, suggesting high reliability.

Table 3. Cronbach alpha coefficient results for factors

Category	Factor	No. of items	Cronbach alpha	Comment
Competence	Employee skills for data safety awareness	11	0.906	Good
	Employee skills for email and website safety	7	0.905	Good
	Employee skills for privacy awareness	4	0.799	Good
Relatedness	Organisational support for employee device and information awareness	16	0.967	Good
	Organisational support for employee information and privacy protection awareness	7	0.945	Good
Autonomy	Employee choice on privacy awareness	3	0.775	Acceptable
	Employee choice to avoid malicious emails and downloads	4	0.836	Good
	Employee choice to keep the privacy of student personal information	2	0.904	Good
	Employee choice to report bad security behaviour	3	0.791	Acceptable
	Employee choice to adhere to information security and privacy policies	2	0.868	Good
	Employee choice to keep devices and information secure	5	0.793	Acceptable

The final questionnaire had 11 revised dimensions and the individual statements were not changed. The new dimensions were a result of the factor and reliability analysis hence the new questionnaire can be considered to have good internal consistency.

5 Limitations and future directions

The following are some of the study's limitations:

The purposive sampling method used in this study, an accepted method of collecting data, may not produce a sample that is representative of the population. Therefore, future research should consider a representative sample of the population and inclusion

of more organisations. The survey questionnaire had 75 questions, which may take some time to complete hence some respondents may not complete the survey. Future work will consider reducing the number of questions.

6 Conclusion

The aim of this study was to develop and validate the information security behaviour questionnaire based on the SDT. This questionnaire can be used to investigate how the perception of competence, relatedness and autonomy influence the intention to comply with ISPs. The results of the assessment can be used to design programs to assist employees to comply with ISPs.

The questions were developed by combining the variables from the SDT and the themes from the HAIS-Q as well as privacy to come up with a new questionnaire. Through a quantitative research, data were collected using the survey method. The collected data were used to validate the questionnaire resulting in a revised questionnaire with items with high internal consistency.

Generally, the results suggest that the survey participants were more confident about their competence and autonomy regarding their information security behaviour than they were about the relatedness questions.

The Pearson correlation results indicate a positive correlation between competence and autonomy, with a partial positive correlation between competence and relatedness, as well as a partial positive correlation between relatedness and autonomy. The results suggest, for example, that improving the competence of employees could result in an increased intention to comply with ISPs. In addition, how confident employees are about their information security skills, will influence their perception of autonomy in their information security behaviour. The participants had a neutral (M=3.08) or potentially negative perception of the relatedness questions, suggesting that area requires further development.

The practical implication of this study and this questionnaire is that it can be used by a university to assess individual employees' strengths and weaknesses in terms of their awareness of information security behaviour. The questionnaire could also be administered before and after information security awareness training to assess the effectiveness of the training.

7 Acknowledgment

This work is based on research supported by the University of South Africa's Women in Research Grant.

8 References

1. Safa NS, Sookhak M, Von Solms R, et al (2015) Information security conscious care behaviour formation in organizations. Comput Secur 53:65–78. https://doi.org/10.1016/j.cose.2015.05.012
2. Humaidi N, Balakrishnan V (2017) Indirect Effect of Management Support on Users' Compliance Behaviour Towards Information Security Policies. Heal Inf Manag J 47:17–27. https://doi.org/10.1177/1833358317700255
3. Pahnila S, Karjalainen M, Mikko S (2013) Information security behavior : Towards multi- stage models. In: Proceedings of the Pacific Asia Conference on Information Systems 2013 (PACIS 2013)
4. Mayer P, Kunz A, Volkamer M (2017) Reliable behavioural factors in the information security context. In: Proceedings of the 12th International Conference on Availability, Reliability and Security - (ARES '17). pp 1–10
5. PriceWaterhouseCoopers (2018) The Global State of Information Security Survey 2018: PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html
6. Ponemon Institute (2020) The third annual study on the state of endpoint security risk. https://www.morphisec.com/hubfs/2020 State of Endpoint Security Final.pdf
7. Huang H-W, Parolia N, Cheng K-T (2016) Willingness and ability to perform information security compliance behavior: Psychological ownership and self-efficacy perspective. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2016)
8. Iriqat YM, Ahlan AR, Nuha NMA (2019) Information security policy perceived compliance among Staff in palestine universities : An empirical pilot study. In: Proceedings of the Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT). IEEE, pp 580–585
9. Alaskar M, Vodanovich S, Shen KN (2015) Evolvement of information security research on employees' behavior: A systematic review and future direction. In: Proceedings of the 48th Hawaii International Conference on System Sciences. pp 4241–4250
10. Öłütçü G, Testik ÖM, Chouseinoglou O (2016) Analysis of personal information security behavior and awareness. Comput Secur 56:83–93. https://doi.org/10.1016/j.cose.2015.10.002
11. Ifinedo P (2013) Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. Inf Manag 51:69–79
12. Kranz JJ, Haeussinger FJ (2014) Why deterrence is not enough : The role of endogenous motivations on employees ' information security behavior. In: Proceedings of the 35th International Conference on Information Systems,. pp 1–14
13. Parsons K, McCormac A, Butavicius M, et al (2014) Determining employee

awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput Secur 42:165–176. https://doi.org/10.1016/j.cose.2013.12.003

14. Gangire Y, Da Veiga A, Herselman M (2019) A conceptual model of information security compliant behaviour based on the self-determination theory. In: Proceedings of the 2019 Conference on Information Communications Technology and Society, ICTAS 2019
15. Pattinson M, Butavicius M, Parsons K, et al (2015) Examining attitudes toward information security behaviour using mixed methods. In: Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015). pp 57–70
16. Guo KH (2013) Security-related behavior in using information systems in the workplace: A review and synthesis. Comput Secur 32:242–251. https://doi.org/10.1016/j.cose.2012.10.003
17. Blythe JM, Coventry L, Little L (2015) Unpacking security policy compliance : The motivators and barriers of employees ' security behaviors. In: Proceedings of the Symposium On Usable Privacy and Security (SOUPS) 2015. Ottawa, pp 103–122
18. Klein RH, Luciano EM (2016) What influences information security behavior? A study with brazilian users. J Inf Syst Technol Manag 13:479–496. https://doi.org/10.4301/S1807-17752016000300007
19. Alfawaz S, Nelson K, Mohannak K (2010) Information security culture : A behaviour compliance conceptual framework. In: Proceedings of the 8th Australasian Information Security Conference (AISC 2010). pp 47–55
20. Ahmad Z, Norhashim M, Song OT, Hui LT (2016) A typology of employees' information security behaviour. In: Proceedings of the 4th International Conference on Information and Communication Technology. pp 3–6
21. Alohali M, Clarke N, Furnell S, Albakri S (2017) Information security behavior: Recognizing the influencers. In: Proceedings of the Computing Conference. pp 844–853
22. Ryan MR, Deci LE (2000) Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. Am Psychol 55:68–78
23. Legault L (2017) Self determination theory. In: Zeigler-Hill V, Shackelford TK (eds) Encyclopedia of personality and individual differences. Springer, New York, pp 1–9
24. Shropshire J, Warkentin M, Sharma S (2015) Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Comput Secur 49:177–191. https://doi.org/10.1016/j.cose.2015.01.002
25. Calic D, Pattinson M, Parsons K, et al (2016) Naïve and accidental behaviours that compromise information security : What the experts think. In: Proceedings of the 10th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016). pp 12–21
26. Bélanger F, Collignon S, Enget K, Negangard E (2017) Determinants of early conformance with information security policies. Inf Manag 54:887–901.

https://doi.org/10.1016/j.im.2017.01.003
27. Bauer S, Bernroider EWN, Chudzikowski K (2017) Prevention is better than cure ! Designing information security awareness programs to overcome users ' non-compliance with information security policies in banks. Comput Secur 68:145–159. https://doi.org/10.1016/j.cose.2017.04.009
28. Curry M, Marshall B, Crossler RE, Correia J (2018) InfoSec Process Action Model (IPAM): Systematically addressing individual security behavior. Databse Adv Inf Syst 49:49–66. https://doi.org/10.1145/3210530.3210535
29. Aurigemma S, Mattson T (2017) Deterrence and punishment experience impacts on ISP compliance attitudes. Inf Comput Secur 25:421–436. https://doi.org/10.1108/ICS-11-2016-0089
30. Swartz P, Da Veiga A, Martins N (2019) A conceptual privacy governance framework. In: Proceeding of the 2019 Conference on Information Communications Technology and Society (ICTAS). pp 1–6
31. NIST (2017) Security and privacy controls for federal information systems and organizations: National Institute of Standards and Technology.
32. Dennedy MF, Fox J, Finneran TR (2014) Data and privacy governance concepts. In: The privacy engineer's manifesto. Apress, New York, pp 51–72
33. Parsons K, Calic D, Pattinson M, et al (2017) The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. Comput Secur 66:40–51. https://doi.org/10.1016/j.cose.2017.01.004
34. Oates BJ (2006) Researching information systems and computing. Sage, London
35. Saunders M, Lewis P, Thornhill A (2016) Research methods for business students, (7th ed.). Pearson Education Limited, Essex
36. Da Veiga A, Martins N (2015) Improving the information security culture through monitoring and implementation actions illustrated through a case study. Comput Secur 49:162–176. https://doi.org/10.1016/j.cose.2014.12.006
37. Yong AG, Pearce S (2013) A beginner ' s guide to factor analysis : Focusing on exploratory factor analysis. Tutor Quant Methods Psychol 9:79–94
38. Williams B, Onsman A, Brown T (2010) Exploratory factor analysis: A five-step guide for novices. J Emerg Prim Heal Care 8:1–13
39. O'Rourke N, Hatcher L (2013) A step-by-step approach to using SAS for factor analysis and structural equation. SAS Institute, Cary, NC
40. Field A (2009) Discovering statistics using SPSS, 3rd ed. Sage, London
41. Gerber H, Hall N (2017) Quantitative research design. In data acquisition - 1 day. HR Statistics, Pretoria
42. Stevens JP (2002) Applied multivariate statistics for the social sciences, 4th ed. NJ: Erlbaum, Hillsdale
43. Marczyk G, Fertinger D, DeMatteo D (2005) Essentials of research design and methodology. John Wiley, Hoboken, NJ