Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q)

Agata Mccormac
Defence Science and Technology Group, Agata.McCormac@dsto.defence.gov.au

Dragana Calic
Defence Science and Technology Group, Dragana.Calic@dsto.defence.gov.au

Kathryn Parsons
Defence Science and Technology Group, kathryn.parsons@dsto.defence.gov.au

Tara Zwaans
The University of Adelaide, taradzwaans@gmail.com

Marcus Butavicius
Defence Science and Technology Group, Marcus.Butavicius@dsto.defence.gov.au

See next page for additional authors

Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q)

Agata McCormac
Defence Science and Technology Group
Edinburgh, South Australia
Email: agata.mccormac@dsto.defence.gov.au

Dragana Calic
Defence Science and Technology Group
Edinburgh, South Australia
Email: dragana.calic@dsto.defence.gov.au

Kathryn Parsons
Defence Science and Technology Group
Edinburgh, South Australia
Email: kathryn.parsons@dsto.defence.gov.au

Tara Zwaans
School of Psychology
The University of Adelaide
Adelaide, South Australia
Email: tara.zwaans@student.adelaide.edu.au

Marcus Butavicius
Defence Science and Technology Group
Edinburgh, South Australia
Email: marcus.butavicius@dsto.defence.gov.au

Malcolm Pattinson
Business School
The University of Adelaide
Adelaide, South Australia
Email: malcolm.pattinson@adelaide.edu.au

Abstract

This paper reports on an evaluation of the test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q), a measure designed to capture an individual's knowledge, attitude and self-reported behaviour towards information security in the workplace. The analyses focused on responses from 197 working Australians, who completed two iterations of the HAIS-Q, approximately four weeks apart. The HAIS-Q showed significant test-retest correlations and has high internal reliability levels. The results of this study demonstrated that the HAIS-Q possesses both external reliability and internal consistency, and can therefore be used as a reliable measure of information security awareness. The HAIS-Q can be used within organisations to measure the effectiveness and impacts of training interventions, information security awareness programs and to determine the impact of security incidents and cultural changes.

Keywords Information security, Information Security Awareness, Cyber security, Reliability, Questionnaire design.

1 Introduction

Computer users form an integral part of the overall information technology (IT) system, and are often considered to be the weakest link in the overarching system (e.g., Furnell & Clarke, 2012; Pattinson & Anderson, 2007; Schneier, 2004). Human error plays a significant role in information security breaches, with employees identified as the largest source of compromise (Pricewaterhouse Coopers (PWC), 2015). The latest Global State of Information Security Survey suggests that, in 2015, security incidents increased by 38%, and during the 2014-2015 financial year, organisations reported an average loss of $2.5 million, directly linked to security incidents (Pricewaterhouse Coopers (PWC), 2015). Globally, some estimates suggest the loss is as high as $1 trillion every year (Lewis & Baker, 2013).

It is increasingly acknowledged that security incidents cannot be fixed through the implementation of solely technical solutions (Parsons et al., 2010; Parsons, McCormac, Butavicius, Pattinson & Jerram, 2014). Previous research has shown that employee information security awareness (ISA) is vital in mitigating the risks associated with information security breaches (Arachchilage & Love, 2014; Safa, Von Solms, & Furnell, 2016). Therefore, it is crucial for organisations to be able to measure the ISA of their employees. Through understanding employees' ISA, organisations can identify areas of strength and weakness, and use this information to tailor their training and awareness programmes to improve ISA within their organisation.

In this paper, we report on the appropriateness of using the Human Aspects of Information Security Questionnaire (HAIS-Q), as a reliable measure of ISA, with an examination of its test-retest reliability and internal consistency. Previous research has validated the HAIS-Q as a measure of ISA and has demonstrated its internal consistency (e.g., Parsons et al., 2016; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). However, the test-retest reliability of the HAIS-Q has not been previously assessed. It is important to evaluate test-retest reliability to provide evidence about the extent to which a measure is reliable and stable. Demonstrating that the HAIS-Q is a reliable and stable measure can enable organisations to confidently assess the effectiveness of information security training and intervention strategies, in conjunction with organisational changes.

The scope of this paper is to determine if the HAIS-Q has both external reliability and internal consistency. Specifically, the aim of this paper is to measure the reliability of the HAIS-Q through:

- Assessment of internal consistency through Cronbach's alpha
- Assessment of external reliability through test-retest correlation

1.1 Reliability

Reliability is a term that is used to describe the consistency of a measure. Essentially, if findings are able to be replicated consistently, they are considered to be reliable (Portney & Watkins, 2015). It is important to understand that although reliability does not imply validity of a measure, without reliability, the validity of a measure is compromised (Streiner, 2003).

There are two overarching types of reliability, internal reliability and external reliability. External reliability is the extent to which a measurement tool or test varies from one administration to another. External reliability can be captured by assessing the test-retest of a measurement tool. Test-retest requires the same participants to complete a test at two different times (Portney & Watkins, 2015). To determine if the HAIS-Q is a reliable measure of ISA, an individual should obtain a similar score if they are tested twice. If test-retest reliability can be demonstrated, it shows that the HAIS-Q could also be used to assess the effectiveness of intervention strategies. There are a number of factors that may affect an individual's results across multiple completions (Allen & Yen, 2001). For example, factors such as the completion of intervening information security training or changes in work or personal lives can influence responses. However, scores on a reliable test should still correlate highly. The time interval between the initial and the retest should be long enough to minimise practice effects, carry over effects and recall (Allen & Yen, 2001). Other test-retest studies employed in organisational environments have used a two to eight week time interval period, therefore, a three to four week time delay between T1 and T2 was deemed to be sufficient (Burch & Anderson, 2004; Griffiths, Cox, Karanika, Khan, & Tomas, 2006; Traynor & Wade, 1993). A measurement tool should have a test-retest coefficient of greater than .70 to illustrate external reliability (van Saane, Sluiter, Verbeek, & Frings-Dresen, 2003).

Internal reliability is also referred to as internal consistency. It is the extent to which a measure is consistent within itself. Cronbach's alpha is used to measure the consistency of results, across items and within a measure (Cronbach, 1951). An acceptable Cronbach's alpha should be over .70 (DeVellis, 2011).

1.2 Information Security Awareness (ISA): Previous HAIS-Q Research

ISA centres on the extent to which an individual understands the importance and implications of information security policies, rules and guidelines, and, the extent to which they behave in accordance with these policies, rules and guidelines (Kruger & Kearney, 2006; Siponen, 2000). This definition is consistent with the Knowledge-Attitude-Behaviour (KAB) model that the HAIS-Q is founded upon. Based on the KAB model, as an employee's level of knowledge of information security policy and procedures increases, their attitude towards information security policy and procedures improves, and this results in better information security behaviour (Parsons, McCormac, Butavicius, et al., 2014).

The HAIS-Q is a measure of ISA. It comprises 63 items that assess seven focus areas, namely, *Password management*, *Email use*, *Internet use*, *Social media use*, *Mobile devices*, *Information handling* and *Incident reporting*. The initial development of the HAIS-Q was motivated by the need to obtain a holistic understanding of the level of ISA of Australian government employees (Parsons, McCormac, Pattinson, Butavicius, & Jerram, 2013, 2014). Interviews with senior managers from Australian government revealed that they believed that security breaches were primarily related to human error and employee naivety. This motivated the focus of the initial information security survey which formed the basis of the HAIS-Q (Parsons et al., 2013; Parsons, McCormac, Pattinson, et al., 2014).

As part of the development and use of the HAIS-Q, it has been tested on diverse samples, using different methodologies. For example, content validity was assessed by Pattinson, Butavicius, Parsons, McCormac, and Jerram (2015) who used the Repertory Grid Technique (RGT) interviews to obtain an in-depth understanding of students' attitudes about the information security behaviours evaluated as part of the HAIS-Q. Content validity focuses on the extent to which the questions in an instrument really assess the construct of interest (Burton & Mazerolle, 2011; Straub, Boudreau, & Gefen, 2004). Most recently, Parsons et al. (2016) report two further studies to establish construct validity of the instrument. Construct validity is demonstrated when a measure correlates with other theoretically-related measures (Westen & Rosenthal, 2003).

Previous research has also demonstrated that the HAIS-Q has high internal consistency. For example, Parsons, McCormac, Butavicius, et al. (2014) reported Cronbach's alphas of above .80 for both a pilot survey, as well as the main survey. Parsons et al. (2015) used the HAIS-Q to explore the relationship between information security and organisational security culture, and reported similarly high Cronbach's alphas of above .80. Most recently, Zwaans et al. (2016) evaluated the extent to which individual differences (e.g., personality, age, gender) may be associated with HAIS-Q scores, and also reported consistently high Cronbach's scores.

These evaluations and findings demonstrate the viability and internal consistency of the HAIS-Q as a useful measure, and have helped shape the current version of the HAIS-Q. To date a total of 1,631 Australians have completed the HAIS-Q (Parsons et al., 2016). This paper adds reliability evaluations and explores test-retest reliability and internal consistency.

1.3 Other Information Security Surveys

There are a limited number of alternative questionnaires or surveys that have been used to assess the level of ISA of employees within organisations. Historically, measures would focus on limited aspects of ISA, or only one component of ISA, and rely on responses to broad and general statements, rather than specific behaviours. For example, Siponen, Pahnila, and Mahmood (2010), assessed individuals' information security related behaviour by asking participants the extent to which *"[they] comply with information security policies"*. Similarly, a questionnaire developed by Martins and Eloff (2002) included items such as: *"I know what the term information security implies"* and *"I am trained in the information security controls I am supposed to use"*. These types of basic statements are more prone to bias; therefore, contributing to an underestimation of security issues (Anderson et al., 2012). Tools measuring ISA in a more concise and empirical manner have only recently been cited in the literature, however, these measures still require further validation and reliability testing.

For example, a team of researchers have developed the Users' Information Security Awareness Questionnaire (UISAQ). This is a 37 item questionnaire which is divided into four parts as follows: 20 items assessing risk behaviour, 6 items measuring level of ISA, 5 items measuring beliefs about information security and 6 questions examining the quality and security of passwords (Solic, Velki, &

Galba, 2015; Velki, Solic, & Ocevcic, 2014). This measure is in the early stages of development, to date no validity and reliability testing has been reported.

Four scales have also been developed by Öğütçü, Testik, and Chouseinoglou (2016) to measure information security behaviour and awareness of users. These four scales include: Risky Behaviour Scale (RBS), Conservative Behaviour Scale (CBS), Exposure to Offence Scale (EOS) and Risk Perception Scale (RPS). Students (n =395), academics (n = 163) and administrative (n = 323) staff from a university environment participated in the study. They determined that the more participants perceived threats, the more protective their behaviours became. It was found that the higher a participant's education level, the more information security aware they were. Also, the most at risk group was identified as students aged between 18 and 30. Although a total of 881 participants completed the four scales, they were all from the one university environment, which may not be generalisable to other workplace settings. The authors plan to conduct further research with larger sample sizes among different population groups.

Egelman and Peer (2015) developed the Security Behavior Intentions Scale (SeBIS), which was completed by 3,619 computer users. This 16-item scale consists of four sub-scales measuring: attitudes towards choosing passwords; device securement; staying up-to-date; and, proactive awareness. This scale measures an individuals' self-reported adherence to computer security advice or an individual's intention to comply with computer security advice. The internal reliability of the (SeBIS) was found to be high with a Cronbach's alpha of .83, and test-retest evaluations also demonstrated scale reliability. However, a subsequent study, conducted by Tischer et al. (2016) found the internal reliability of the SeBIS to be much lower. They used the measure in two studies, a USB survey and an email survey; they found the Cronbach's alpha value to be below the required .70 for both surveys, with results at .57 and .62, respectively. Further analysis revealed that the internal consistency of many of the subscale values reported were below .70. Therefore, subsequent testing is required to determine the reliability of the measure.

All of these instruments, including the HAIS-Q, measure ISA. At this point the HAIS-Q has undergone more extensive validity and reliability testing. The measure has been completed by a large and representative sample of working Australians, covering a broad range of employment sectors, educational backgrounds and ages. Various qualitative and quantitative methodologies have been used to test and further develop the measure (Parsons et al., 2016).

2 Methodology

The present study involved the completion of two surveys using the same participant sample. This enabled a comparison of results obtained from the initial test (referred to as T1) and retest (referred to as T2). Data collection involved an online survey, administered through the web-based survey platform, Qualtrics. To take part in the survey, participants were required to meet the following inclusion criteria: they had to be currently employed and working within Australia; be at least 18 years of age; spend at least 20% of their work time using a computer; and, work for an organisation with a formal or informal information security policy. Also, upon completion of T2, participants were asked if they had completed any intervening information security training, if completing T1 had changed the way they use computers for work, and, if there were any other changes in their work or personal life that might have affected the way they use computers for work. These questions were asked as these aspects may have affected the participants' survey responses.

A total of 531 participants completed the HAIS-Q, and, following a three to four week period, 207 of the participants in the initial sample completed the survey for a second time. Ten outliers were identified from analysis. These participants had *z* scores more than two standard deviations from the mean. Following recommendations made by Meade and Craig (2012), the data gathered from these 10 participants were further examined to determine the quality of responses (e.g., whether they responded appropriately to questions or if there were signs of non-responsivity and careless responses, such as, only selecting the one response option). Following this process, data from these 10 participants was excluded from analysis, leaving 197 participants who completed the online survey at both T1 and T2.

All analyses reported in this paper focus on the 197 participants who completed the online survey at both T1 and T2. The 197 (105 females and 92 males) participants represented all age categories (12 between 18 and 29 years of age, 52 between 30 to 39, 49 between 40 to 49, 43 between 50 and 59, and 41 aged 60 and above), with most participants (94%) over the age of 30. Level of completed education was also well represented among participants, with most participants having completed a bachelor degree (34%) or further post-graduate qualifications (20%). Many participants had completed year 12 equivalent (14%) or had some post-secondary education (25%). Participants represented over 13 employment sectors and eight job areas, including sales, labourers, professionals, management and technician/trade workers.

2.1 Measures

The online survey collected general demographic details and computer use information, including; gender, age, employment status, and the percentage of time at work spent using a computer. In addition to these questions, the participants completed the following measure:

The **Human Aspects of Information Security Questionnaire (HAIS-Q)** is a 63-item measure of ISA (Parsons, McCormac, Butavicius, et al., 2014). It examines knowledge of information security policies and procedures, attitude towards policies and procedures, and self-reported information security behaviours. As mentioned previously, the HAIS-Q focusses on seven areas of ISA. Respondents are asked to respond on a five-point Likert-type scale, ranging from “Strongly Agree” to “Strongly Disagree”.

3 Results

3.1 Internal Consistency

To measure the internal consistency of the HAIS-Q, the Cronbach’s alpha coefficient scores at T1 and T2 were compared. To assess the level of internal consistency, the Cronbach’s alpha coefficient should be over .70 (DeVellis, 2011). Table 3 presents Cronbach’s alpha scores for knowledge, attitude, self-reported behaviour and overall ISA at T1 and T2. It reveals minimal variation in estimated internal consistency between the two time intervals.

	T1 Cronbach’s	T2 Cronbach’s
Knowledge	.84	.86
Attitude	.93	.92
Behaviour	.90	.91
ISA	.96	.96

Table 3. Cronbach’s Alpha Scores for Knowledge, Attitude, Behaviour and ISA at T1 and T2

Table 4, shows the Cronbach’s alpha scores for the seven focus areas at T1 and T2, once again a similar pattern is observed, with little variation between T1 and T2 scores. These reported Cronbach’s alpha coefficient scores reveal that the HAIS-Q has high internal consistency as an overall measure of ISA and also good internal consistency within its focus areas.

Focus Area	T1 Cronbach’s	T2 Cronbach’s
Password Management	.83	.84
Email Use	.77	.81
Internet Use	.79	.80
Social Media Use	.75	.78
Mobile Devices	.83	.82
Information Handling	.76	.79
Incident Reporting	.78	.78

Table 4. Cronbach’s Alpha Scores for Focus Areas at T1 and T2

3.2 Test-Retest Reliability

To evaluate the test-retest reliability of the HAIS-Q, first we focussed on the comparison of the knowledge, attitude and behaviour sub-scales, and the overall ISA scores. Table 1 shows the test (T1) and retest (T2) means, standard deviations and test-retest (T1/T2) correlations. The test-retest correlations for knowledge, attitude, self-reported behaviour and overall ISA were all statistically significant, and were greater than .70 in all instances. It is generally accepted that a test-retest coefficient greater than .70 is required to illustrate external reliability (van Saane et al., 2003). However, as shown in Table 1, the scores for knowledge, attitude, self-reported behaviour and overall ISA all increased from T1 to T2. To further assess this difference, raw scores were examined to identify the amount of variation between T1 and T2. For 93% of participants, there was less than 10% variation between T1 and T2.

Paired Samples t-tests revealed that there were significant differences in T1 and T2 scores for knowledge, $t(196) = -3.74$, $p = .000$, $d = .19$, behaviour, $t(196) = -2.73$, $p = .007$, $d = .11$, and overall ISA, $t(196) = -3.44$, $p = .001$, $d = .12$. However, as shown by Cohen's d, the small effect size, of below .20, demonstrates that these differences are not meaningful (Cohen, 1992a, 1992b). The findings for attitude were non-significant, $t(196) = -9.95$, $p = .341$, $d = .04$. This suggests that, overall, there was a high level of stability in HAIS-Q scores.

	T1 Mean(SD)	T2 Mean(SD)	T1/T2 *r* correlation
Knowledge	80.64 (11.57)	82.84 (11.52)	.75*
Attitude	86.54 (12.67)	87.09 (12.00)	.79*
Behaviour	84.31 (12.31)	85.31 (11.66)	.84*
ISA	251.50 (33.27)	255.55 (32.98)	.88*

*Table 1. Correlations for Knowledge, Attitude, Behaviour and ISA at T1 and T2 (*p < .01, two-tailed)*

In Table 2, we present the test-retest reliability of the seven focus areas, which provides further evidence of the stability of the HAIS-Q. The correlations between T1 and T2 were all significant, and, as shown in the table, the differences in means were very small. Although four focus areas had statistically significant differences (i.e., email use, internet use, social media use and mobile devices), as the effect size was below .20, these differences were not meaningful (Cohen, 1992a, 1992b).

Focus Area	T1 Mean(SD)	T2 Mean(SD)	T1/T2 *r* correlation
Password Management	37.20 (5.82)	37.34 (5.76)	.78*
Email Use	34.50 (5.67)	35.56 (5.61)	.73*
Internet Use	33.86 (5.77)	34.50 (5.59)	.72*
Social Media Use	36.08 (5.35)	36.76 (5.16)	.74*
Mobile Devices	36.88 (5.72)	37.72 (5.41)	.77*
Information Handling	36.84 (5.74)	37.10 (5.88)	.82*
Incident Reporting	36.13 (5.27)	36.56 (5.03)	.75*

*Table 2. Correlations for Focus Areas at T1 and T2 (*p < .01, two-tailed)*

Although these results provide sufficient evidence that the HAIS-Q is a stable measure, we explored a number of other variables that may have affected the way people responded. For example, only two participants indicated that they had received information security training in the intervening period, and a very small minority discussed any changes in their work or personal life that might have affected the way they use computers for work.

When asked *'Did completing the initial survey change the way you use computers for work?'*, approximately 40 participants commented on how completing T1 affected their awareness of information security risks. A minority of respondents commented that they did not change their behaviour, for example, *"have been following all the security rules for a long time"*, and *"I knew this already"*. However, participants most commonly reported being more cautious in the use of computers. For example, *"I thought more about it"*, *"I am more cautious"*, and *"It made me more aware of security risks both with information sources and my surroundings"*. Some reported being more cautious in relation to specific areas, such as password management, *"I am more mindful of passwords being the same for personal and work-related accounts"*, and email use, *"more careful with email links and attachments"*. A small number of participants reported having taken more specific actions following T1, such as *"[changing] their passwords"* and *"always [being] careful leaving things around"*. These comments may account for the small increase in mean scores, between T1 and T2.

4 Discussion

In this study, we examined the test-retest reliability and internal consistency of the HAIS-Q. By showing that the HAIS-Q is stable and reliable, it demonstrates that the HAIS-Q provides accurate measurements of ISA, and, can be confidently used to assess interventions and training strategies. Results show that the HAIS-Q possesses both high internal and external reliability. There were small increases in scores between T1 and T2, which suggests that completing the HAIS-Q may have prompted some participants to think more actively about information security. This is demonstrated in the qualitative responses. However, statistical analysis revealed that overall, these differences were not meaningful. Test-retest coefficient values were over .70 across the overall measure and the three components that make up ISA, namely, knowledge, attitude and self-reported behaviour. The seven focus areas of the HAIS-Q followed the same pattern. Similarly, the results of this study show the HAIS-Q to be internally consistent, with Cronbach's alpha scores across all dimensions and focus areas above .70. This means that the HAIS-Q is likely to be a reliable measurement tool.

These findings have a number of practical implications. A reliable and valid tool that measures various aspects of ISA is undoubtedly a valuable asset to any organisation. It provides an opportunity to reliably measure ISA of individuals, and to potentially determine individual and organisational strengths and weaknesses. By administrating the HAIS-Q to employees, an organisation can determine if, for example, password management is more of a weakness than social media use or mobile computing within their current work environment.

The qualitative responses, although only a small component of the study, revealed that completing the HAIS-Q affected user awareness and made some individuals more cautious. In fact, some participants revealed that completing the HAIS-Q, at T1, altered their behaviour in the intervening period. Conversely, some participants reported no behavioural changes. These findings suggest that completing the HAIS-Q, for certain individuals, may provide some training benefit.

Furthermore, both researchers and organisations can use the HAIS-Q to measure the impact and effectiveness of interventions including training, ISA programs, cultural changes and the impact of security incidents. For example, an organisation may initially administer the HAIS-Q to their employees in order to gather baseline data about their ISA. Using this information, they may identify certain areas of information security that require further targeted training campaigns. After this training is completed, the HAIS-Q can be administered again to determine the success of the training intervention. If the training intervention was successful, improvements in scores across the knowledge, attitude and behaviour components of the HAIS-Q, along with improvements in specific focus areas, should be evident.

4.1 Limitations and Future Research

While in this study, we establish the test-retest reliability and internal consistency of the HAIS-Q, we note some limitations. For example, some authors recommend sample sizes between 200 to 400 participants for a test-retest reliability study (Charter, 2003; Kline, 1986). This increases statistical precision, and improves generalisability of the findings. The sample size used in our reliability study (n = 197) is close to the minimum recommendation. While we do not envisage that a larger sample size would radically change the results, this study could be replicated with more participants.

The qualitative responses provided insights that warrant further investigation into individual differences. It would be beneficial to explore why certain participants changed their behaviour after completing the HAIS-Q and why others did not. It would undoubtedly help if we also knew more about participants, not only from an individual perspective, but also from an organisational one. Participants in this study were all from unknown organisations. By completing the test-retest study using a known organisation, we would be better able to assess what happens between T1 and T2. Any intervening training sessions or organisational changes could be controlled and accounted for.

Another limitation is the generalisability of these results to other cultural settings and environments. The HAIS-Q has been completed by a representative sample of working Australians, and we have demonstrated that it is reliable within this Australian context. However, further validity and reliability assessments of the HAIS-Q should be conducted in different countries to measure the effects of any cultural differences.

5 Conclusion

This study has demonstrated that the HAIS-Q, a measure of ISA, is externally reliable and internally consistent. In the current cyber environment, the ability to measure ISA of employees, and having confidence in those results, is a valuable asset to organisations. The HAIS-Q, as a reliable measure of ISA, enables organisations to assess the effectiveness of any information security intervention strategies or other changes over time. Therefore, research on the HAIS-Q provides a unique contribution to the information security literature and research field, as well a practical contribution to organisations.

6 References

Allen, M. J., & Yen, W. M. (2001). *Introduction to Measurement Theory*. Long Grove, Illinois: Waveland Press.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., . . . Savage, S. (2012, 25-26 June). *Measuring the cost of cybercrime*. Paper presented at the 11th Annual Workshop on the Economics of Information Security, Berlin, Germany.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304-312.

Burch, G., & Anderson, N. (2004). Measuring person-team fit: Development and validation of the team selection inventory. *Journal of Managerial Psychology, 19*(4), 406-426.

Burton, L. J., & Mazerolle, S. M. (2011). Survey instrument validity part I: Principles of survey instrument development and validation in athletic training education research. *Athletic Training Education Journal, 6*(1), 27-35.

Charter, R. A. (2003). Study samples are too small to produce sufficiently precise reliability coefficients. *Journal of General Psychology, 130*(117-129).

Cohen, J. (1992a). A Power Primer. *Psychological bulletin, 112*(1), 155.

Cohen, J. (1992b). Statistical Power Analysis. *Current Directions in Psychological Science, 1*(3), 98-101.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297-334.

DeVellis, R. F. (2011). *Scale Development: Theory and Applications* (3rd ed.): SAGE Publications.

Egelman, S., & Peer, E. (2015). *Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)*. Paper presented at the Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea.

Furnell, S., & Clarke, C. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*, 983-988.

Griffiths, A., Cox, T., Karanika, M., Khan, S., & Tomas, J. M. (2006). Work design and management in the manufacturing sector: development and validation of the Work Organisation Assessment Questionnaire. *Occupational and Environmental Medicine, 63*(10), 669-675.

Kline, P. (1986). *A Handbook of Test Construction: Introduction to Psychometric Design. NY: Methuen.* : Routledge.

Kruger, H., & Kearney, W. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

Lewis, J., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage *Center for Strategic and International Studies, Washington, DC.*

Martins, A., & Eloff, J. H. P. (2002). Information security culture *Security in the Information Society* (pp. 203-214). Boston: MA: Kluwer Academic Publishers.

Meade, A. W., & Craig, S. D. (2012). Identifying careless responses in survey data. *Psychological Methods, 17*(3), 437-455.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2016). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Manuscript submitted for publication*.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013, May). *An Analysis of Information Security Vulnerabilities at Three Australian Government Organisations*. Paper presented at the Proceedings of the European Information Security Multi-Conference (EISMC 2013), Lisbon, Portugal.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). A study of information security awareness in Australian government organisations. *Information Management & Computer Security, 22*(4), 334-345.

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M., & Jerram, C. (2015). The Influence of Organisational Information Security Culture on Cybersecurity Decision Making. *Journal of Cognitive Engineering and Decision Making: Special Issue on Cybersecurity Decision Making, 9*(2), 117-129.

Pattinson, M., & Anderson, G. (2007, April). *End-user risk-taking behaviour: An application of the IMB model*. Paper presented at the Proceedings of the 6th Annual Security Conference, Las Vegas, Nevada, USA.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Jerram, C. (2015). *Examining attitudes toward information security behaviour using mixed methods*. Paper presented at the Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), Mytilene, Greece.

Portney, L. G., & Watkins, M. P. (2015). *Foundations of Clinical Research: Applications to Practice* (3rd ed.). Philadelphia: FA Davis.

Pricewaterhouse Coopers (PWC). (2015). Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

Schneier, B. (2004). *Secrets and lies: digital security in a networked world*: Wiley.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Siponen, M. T., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71.

Solic, K., Velki, T., & Galba, T. (2015). *Empirical study on ICT system's users' risky behavior and security awareness*. Paper presented at the Information and Communication Technology, Electronics and Microelectronics (MIPRO).

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *The Communications of the Association for Information Systems, 13*(1), 380-427.

Streiner, D. L. (2003). Starting at the beginning: An introduction to coefficient alpha and internal consistency. *Journal of personality assessment, 80*(1), 99-103.

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). *Users Really Do Plug in USB Drives They Find*. Paper presented at the 37th IEEE Symposium on Security and Privacy, San Jose, California.

Traynor, M., & Wade, B. (1993). The development of a measure of job satisfaction for use in monitoring the morale of community nurses in four trusts. *Journal of Advanced Nursing, 18*, 127-136.

van Saane, N., Sluiter, J. K., Verbeek, J. H. A. M., & Frings-Dresen, M. H. W. (2003). Reliability and validity of instruments measuring job satisfaction—a systematic review. *Occupational Medicine, 53*(3), 191-200.

Velki, T., Solic, K., & Ocevcic, H. (2014). *Development of Users' Information Security Awareness Questionnaire (UISAQ) — Ongoing work*. Paper presented at the Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija.

Westen, D., & Rosenthal, R. (2003). Quantifying construct validity: two simple measures. *Journal of personality and social psychology, 84*(3), 608.

Zwaans, T., McCormac, A., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2016). Individual Differences and Information Security Awareness. *Manuscript submitted for publication.*

Acknowledgements

This project was supported by a Premier's Research and Industry Fund granted by the South Australian Government of State Development.

Copyright