A Reliable Measure of Information Security Awareness and the Identification of Bias in Responses

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

Dragana Calic
Defence Science and Technology Group
Edinburgh, South Australia

Marcus Butavicius
Defence Science and Technology Group
Edinburgh, South Australia

Kathryn Parsons
Defence Science and Technology Group
Edinburgh, South Australia

Tara Zwaans
School of Psychology
The University of Adelaide
Adelaide, South Australia

Malcolm Pattinson
Adelaide Business School
The University of Adelaide
Adelaide, South Australia

Abstract

The Human Aspects of Information Security Questionnaire (HAIS-Q) is designed to measure Information Security Awareness. More specifically, the tool measures an individual's knowledge, attitude, and self-reported behaviour relating to information security in the workplace. This paper reports on the reliability of the HAIS-Q, including test-retest reliability and internal consistency. The paper also assesses the reliability of three preliminary over-claiming items, designed specifically to complement the HAIS-Q, and identify those individuals who provide socially desirable responses. A total of 197 working Australians completed two iterations of the HAIS-Q and the over-claiming items, approximately 4 weeks apart. Results of the analysis showed that the HAIS-Q was externally reliable and internally consistent. Therefore, the HAIS-Q can be used to reliably measure information security awareness. Reliability testing on the preliminary over-claiming items was not as robust and further development is required and recommended. The implications of these findings mean that organisations can confidently use the HAIS-Q to not only measure the current state of employee information security awareness within their organisation, but they can also measure the effectiveness and impacts of training interventions, information security awareness programs and campaigns. The influence of cultural changes and the effect of security incidents can also be assessed.

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

1 Introduction

Employee Information Security Awareness (ISA) is critical in mitigating the risks associated with cyber security incidents (Arachchilage & Love, 2014; Safa, Von Solms, & Furnell, 2016). Therefore, it is crucial for organisations to be able to measure their employees' ISA. Through

understanding employee ISA, organisations can identify areas of strength and weakness, and use this information to tailor their training and awareness programs to improve their ISA.

It is increasingly acknowledged that security incidents cannot be mitigated through solely technical solutions (Parsons et al., 2010; Parsons, McCormac, Butavicius, Pattinson & Jerram, 2014). Human error plays a major role in information security breaches, with employees consistently identified as the main source of compromise (Pricewaterhouse Coopers (PWC), 2015; 2017). Consequently, the consideration of the human element of information security has become increasingly important for organisations around the world.

In this paper, we examine the test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q) and report on the appropriateness of using the HAIS-Q as a reliable measure of ISA. Previous research has validated the HAIS-Q as a measure of ISA and has demonstrated its internal consistency (Parsons et al., 2017; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). In this paper we evaluate test-retest reliability to provide evidence about the extent to which the HAIS-Q is reliable and stable. Demonstrating that the HAIS-Q is a reliable and stable measure of ISA can enable organisations to confidently assess the effectiveness of information security training and intervention strategies, in conjunction with organisational changes.

When developing any security assessment instrument it is important to consider the extent to which the results may be affected by social desirability bias. This form of bias can affect the reliability and validity of survey findings. Hence, in this study participants also provided responses to three preliminary over-claiming items designed to ascertain if participants were responding in a socially desirable manner. The reliability of the HAIS-Q over-claiming questions will also be assessed using test-retest correlations and Cronbach's alpha.

1.1 Reliability

Reliability can be described as reputability of findings, and it serves to demonstrate the consistency of a measure or an instrument. Essentially, if findings are able to be replicated consistently, they are considered to be reliable (Portney & Watkins, 2015). Although reliability does not imply validity of a measure, without reliability, the validity of a measure is compromised (Streiner, 2003). There are two types of reliability, internal reliability and external reliability.

External reliability refers to the extent to which an instrument or a test varies from one administration to another. External reliability can be captured by assessing the test-retest of an instrument. 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 test (i.e., T1) and the retest (i.e., T2) should be sufficiently long 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).

Interpretation of alpha scores is important; this is because a high alpha level does not always reflect high internal consistency. When items within a measure are highly correlated, then the alpha level will also be high. Lower alpha levels can be associated with low number of questions, poor correlations between items or heterogeneous constructs. These issues are important to keep in mind when interpreting findings and reliability assessments (Tavakol & Dennick, 2011).

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

ISA can be defined as the extent to which a person understands the importance and implications of information security policies, rules and guidelines, as well as, the extent to which they are committed to and 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 measures ISA by examining seven focus areas, namely, *Password management, Email use, Internet use, Social media use, Mobile devices, Information handling* and *Incident reporting*. The HAIS-Q 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 student 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). Also, more recently, Parsons et al. (2017) 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 et al. (2015) used the HAIS-Q to explore the relationship between information security and organisational security culture, and reported high Cronbach's alphas of above .80. Most recently, McCormac et al. (2017) 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 alpha 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., 2017). This paper adds reliability evaluations and explores test-retest reliability and internal consistency.

1.3 Social Desirability Bias

Social desirability bias is described as a form of response bias or cognitive bias, and it refers to the tendency of participants to respond to questions in a way that presents them in the best possible manner (Fisher, 1993). When participants respond to survey questions in this way they are not providing truthful responses and this may lead to incorrect results that skew findings. Therefore, surveys should incorporate questions to identify participants who are more likely to respond in a socially desirable way (Grimm, 2010). Essentially, when it comes to measures of ISA, researchers need to be cognizant of individuals who may be assessed at higher levels of ISA than they actually possess. Such participants may be trying to present themselves as having greater knowledge; a more positive attitude; and report more secure behaviours than they actually exhibit in their workplace.

Experimental designs can incorporate several processes and techniques to minimise the effect of social desirability bias. For example, ensuring anonymity and confidentiality of respondents, has been shown to reduce bias (Bowling, 2005). Research has found that this assurance contributes to participants providing more truthful responses (Szolnoki & Hoffmann, 2013).

Allowing participants to complete a survey online also increases the likelihood of truthful answers because it is considered a neutral administration of the survey. Participants are less likely to be affected by bias when providing responses online, as they may be less likely to feel judged (Duffy, Smith, Terhanian, & Bremer, 2005). Researchers are also encouraged to include questions that can be used to determine if someone is providing socially desirable responses (Nederhof, 1985). These are specifically constructed questions used for the sole purpose of separating credible responses from those who are providing socially biased answers.

By incorporating these techniques into the experimental design it is expected that the impact of the social desirability bias could be reduced and also captured. For the purposes of our study, we designed a preliminary set of over-claiming questions for use within the HAIS-Q. In this paper, we focus on an assessment of the reliability of the over-claiming items, as a measure of response bias.

2 Method

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. Participants were required to meet the following inclusion criteria: they had to be currently employed and working in 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 ten 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 were 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, participants completed the Human Aspects of Information Security Questionnaire (HAIS-Q), a 63-item measure of ISA (Parsons, McCormac, Butavicius, et al., 2014). The HAIS-Q 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".

Three over-claiming items were developed, one a knowledge question, one an attitude question and one a behaviour related question. These questions were incorporated into the HAIS-Q. The purpose of these questions was to identify individuals who were responding in a socially desirable manner. As with the HAIS-Q, participants responded on a five-point Likert scale. An example item was: "*Safe passwords must include the letter 'v'*".

3 Results

3.1 Internal Consistency of the HAIS-Q

To measure the internal consistency of the HAIS-Q, the Cronbach's alpha coefficients 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 1 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 1. Cronbach's Alpha Scores for Knowledge, Attitude, Behaviour and ISA at T1 and T2

Table 2, 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 coefficients 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 2. Cronbach's Alpha Scores for Focus Areas at T1 and T2

3.2 Test-Retest Reliability of the HAIS-Q

To evaluate the test-retest reliability of the HAIS-Q, first we compared the knowledge, attitude and behaviour sub-scales, and the overall ISA scores. Table 3 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 evident by the Cohen's d measures, these differences are all small sized effects (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 3. Correlations for Knowledge, Attitude, Behaviour and ISA at T1 and T2 (*p < .01, two-tailed)*

In Table 4, we present the test-retest reliability of the seven focus areas, which provides evidence of the stability of the HAIS-Q at the sub-scale level as well. 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 small (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 4. 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 responses. 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 stated that completing T1 affected their awareness of information security risks. A minority of respondents stated 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 for the focus area of email use one participant said they were, "*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.

3.3 Internal consistency and test-retest of the over-claiming items

The same statistical analysis, conducted on the HAIS-Q, was repeated using participants' responses to the three over-claiming items to assess both internal consistency and test-retest reliability. To evaluate the internal consistency of the over-claiming questions the Cronbach's

alpha coefficient scores at T1 and T2 were calculated. At T1 the Cronbach's Alpha score was .53 and at T2 the score was .55 Cronbach's alpha scores were below the .70 mark used to determine internal consistency.

Table 5, summarises the test (T1) and retest (T2) means, standard deviations and test-retest (T1/T2) correlations for the individual knowledge, attitude and behaviour over-claiming items and the total over-claiming score. Mean scores and standard deviations were stable from T1 and T2. All reported correlations were significant; however, they were below .70 for individual over-claiming items. Given that there are only three items we correlated the total over-claiming score, between T1 and T2. This figure is .66, indicating that the scale is approaching the .70 cut off, which is indicative of test-retest reliability (van Saane et al., 2003).

	T1 Mean(SD)	T2 Mean(SD)	T1/T2 r correlation
Knowledge Over-Claiming Item	3.21 (1.16)	3.21 (1.16)	.55*
Attitude Over-Claiming Item	4.03 (1.00)	4.06 (.92)	.51*
Behaviour Over-Claiming Item	2.98 (1.29)	3.02 (1.27)	.50*
Total Over-Claiming Score	10.22 (2.49)	10.29 (2.45)	.66*

*Table 5. Correlations, means and SD scores for the over –claiming individual Knowledge, Attitude, Behaviour items and total over-claiming score at T1 and T2 (*p < .01, two-tailed)*

A paired samples t-test revealed that there were no significant differences in T1 and T2 scores for the total over claiming score which combined the three over-claiming items, $t(196) = -.45$, $p = .65$, $d = -.03$, suggesting stability.

These results show that the preliminary over-claiming items are approaching test-retest reliability, and are stable; however, the items are not internally consistent. Implications of these reliability findings are discussed in the following section.

4 Discussion

In this study, we examined the test-retest reliability and internal consistency of the HAIS-Q, a measure of ISA, and three preliminary over-claiming items, designed to measure response bias.

Current findings serve to further demonstrate that the HAIS-Q is an accurate measure 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, and this was demonstrated in participants' 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 a valuable asset to any organisation. It provides an opportunity to reliably measure employee ISA, 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 may have affected employee 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.

The three preliminary over-claiming items were designed to complement the HAIS-Q, and their purpose was to identify individuals who were responding in a socially desirable manner. Having the ability to identify these individuals gives organisations the opportunity to more rigorously understand the nature of ISA in their environment. Not only would they be able to assess if employees were being truthful in their responses but they would also be able to use this knowledge to investigate why this was occurring. For example, it may be the case that a high rate of socially desirable responses correlates with a lack of training opportunities. Alternatively, in a work environment that is perceived as punitive, employees may be more likely to respond in a socially desirable manner to avoid the potential negative consequences associated with low information security behaviour that may potentially incur a penalty.

Although current findings indicate that the three preliminary over-claiming items were not internally consistent, they approached the test-retest reliability cut-off. These results are promising and it is suggested that the low alpha level could be due to the low number of questions used to assess bias which meant the measure lacked precision (Tavakol & Dennick, 2011). It is proposed that adding additional over-claiming items could improve both internal and test-retest reliability. An improved version would give organisations greater confidence in the over-claiming questions. Assessing these responses in conjunction with HAIS-Q findings may provide organisations with valuable information about their employees' ISA and the security culture in their workplace. Specific suggestions as to how this can be achieved are provided in the following section.

4.1 Limitations and Future Research

In this study, we establish the test-retest reliability and internal consistency of the HAIS-Q and measured the reliability of the over-claiming items. However, there are 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 of this research 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. The over-claiming items are still in early stages of development but the effect of social desirability bias may certainly differ across cultural settings. Once an improved reliable and validated measure has been developed it should also be further assessed in a variety of cultures and work settings.

The findings relating to the over-claiming items were encouraging. However, its reliability may have been limited by the small number of questions, therefore, it would be prudent to increase the number of items in future research. It is recommended that rather than having a knowledge, attitude and behaviour over-claiming item there should be an over-claiming item for each of the focus areas. This would expand the number of items from three to seven. Following the addition of five new items the reliability of the over-claiming questions would need to be re-assessed.

This paper also only focused on the reliability of the HAIS-Q and the preliminary over-claiming items, however, a measure needs to be both reliable and valid. Validity testing and assessments have been conducted on the HAIS-Q (Parsons et al., 2017). However, further validation testing is recommended following the development of a more robust version of the over-claiming items.

5 Conclusion

This study has demonstrated that the HAIS-Q, a measure of ISA, is externally reliable and internally consistent. The reliability of the over-claiming items, used to measure social desirability bias, although encouraging require further development. 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. By supplementing HAIS-Q findings with reliable data on response bias, organisations will have greater insight into the state of ISA in their organisation and a richer understanding of their organisational culture. Therefore, research on the HAIS-Q and over-claiming items provides a unique contribution to the information security literature and research field, as well a practical contribution to organisations.

References

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

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

Bowling, A. (2005). Mode of questionnaire administration can have serious effects on data quality. *Journal of public health, 27*(3), 281-291.

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.

Duffy, B., Smith, K., Terhanian, G., & Bremer, J. (2005). Comparing data from online and face-to-face surveys. *International Journal of Market Research, 47*(6), 615.

Fisher, R. (1993). Social Desirability Bias and the Validity of Indirect Questioning. *Journal of Consumer Research, 20*(2), 303-315.

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.

Grimm, P. (2010). Social desirability bias. *Wiley International Encyclopedia of Marketing*.

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*. Retrieved from http://www.mcafee.com/au/resources/reports/rp-economic-impact-cybercrime.pdf

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

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual Differences and Information Security Awareness. *Computers in Human Behavior, 69*, 151-156.

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

Nederhof, A. J. (1985). Methods of coping with social desirability bias: A review. *European Journal of Social Psychology, 15*(3), 263-280.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40-51.

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). An Analysis of Information Security Vulnerabilities at Three Australian Government Organisations *Proceedings of the European Information Security Multi-Conference (EISMC 2013)* (pp. 34-44). 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., Butavicius, M., Parsons, K., McCormac, A., & Jerram, C. (2015). Examining attitudes toward information security behaviour using mixed methods. In S. Furnell & N. Clarke (Eds.), *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)* (pp. 57 - 70). Mytilene, Greece: Centre for Security, Communications & Network Research.

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*. Retrieved from www.pwc.com/giss

Pricewaterhouse Coopers (PWC). (2017). *The Global State of Information Security® Survey 2018*. Retrieved from https://www.pwc.com/us/en/cybersecurity/information-security-survey.html

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

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.

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.

Szolnoki, G., & Hoffmann, D. (2013). Online, face-to-face and telephone surveys—Comparing different sampling methods in wine consumer research. *Wine Economics and Policy, 2*(2), 57-66.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International journal of medical education, 2*, 53.

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.

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

Acknowledgements

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