2013

The Development of the Human Aspects of Information Security Questionnaire (HAIS-Q)

Kathryn Parsons
Defence Science and Technology Organisation (DSTO), kathryn.parsons@dsto.defence.gov.au

Agata McCormac
Defence Science and Technology Organisation (DSTO), Agata.McCormac@dsto.defence.gov.au

Marcus Butavicius
efence Science and Technology Organisation (DSTO), Marcus.Butavicius@dsto.defence.gov.au

Malcolm Pattinson
The University of Adelaide, Malcolm.Pattinson@adelaide.edu.au

Cate Jerram
The University of Adelaide, cate.jerram@adelaide.edu.au

Recommended Citation

Parsons, Kathryn; McCormac, Agata; Butavicius, Marcus; Pattinson, Malcolm; and Jerram, Cate, "The Development of the Human Aspects of Information Security Questionnaire (HAIS-Q)" (2013). *ACIS 2013 Proceedings*. 31.
https://aisel.aisnet.org/acis2013/31

ACIS 2013
RMIT MELBOURNE

Information Systems: Transforming the Future

24th Australasian Conference on Information Systems, 4-6 December 2013, Melbourne

Proudly sponsored by

nab
ACIS 2013 Principal Sponsor

RMIT UNIVERSITY

CITRIX®

GS1® Australia

acs AUSTRALIAN COMPUTER SOCIETY

ACS Foundation
Advancing ICT through Education and Research

ACPHIS

AAIS
Australasian Association for Information Systems

The Development of the Human Aspects of Information Security Questionnaire (HAIS-Q)

Kathryn Parsons, Agata McCormac, Marcus Butavicius
Defence Science and Technology Organisation (DSTO)
South Australia
Email: kathryn.parsons; agata.mccormac; marcus.butavicius@dsto.defence.gov.au

Malcolm Pattinson, Cate Jerram
Business School
University of Adelaide
South Australia
Email: malcolm.pattinson; cate.jerram@adelaide.edu.au

Abstract

The Human Aspects of Information Security Questionnaire (HAIS-Q) is being developed using a hybrid inductive, exploratory approach, for the purpose of evaluating information security threats caused by employees within organisations. This study reports on the conceptual development and pre-testing of the HAIS-Q. Results from 500 Australian employees were then used to examine the reliability of the HAIS-Q, as well as the relationships between knowledge of policy and procedures, attitude towards policy and procedures and behaviour when using a work computer. Results indicate significant, positive relationships between all variables. However, both qualitative and quantitative results indicate the direct influence of knowledge of policy and procedure accounted for far less of the variance in self-reported behaviour than attitude towards policy and procedure. Implications for training and education campaigns and plans for future research to further develop this questionnaire are outlined.

Keywords

Information security; Security behaviours; Questionnaire design; Cyber security; Hybrid research

INTRODUCTION

There is a growing realisation that cyber security threats cannot be prevented, avoided, detected or eliminated by solely focusing on technological solutions. This is because many of the threats to an organisation's computer systems can be attributed to the behaviour of computer users. This includes behaviour such as inadvertently or deliberately divulging passwords to others, falling victim to phishing emails by clicking on embedded web site links, or inserting non-familiar media into work or home computers.

This paper reports on part of a larger project to produce an empirically validated instrument to assess the extent to which the organisation's information systems are vulnerable to threats caused by risk-taking behaviour of employees. This tool could then be used to measure levels of knowledge, attitude and behaviour to provide management with a benchmark. This instrument could also be used to evaluate the effectiveness of different information technology (IT) control strategies or to track the long-term security health of an organisation. The aim of this paper is to outline the development of the Human Aspects of Information Security Questionnaire (HAIS-Q) and to examine the relationships between knowledge of policy and procedures, attitude towards policy and procedures and behaviour when using a work computer.

THEORETICAL BACKGROUND

A comprehensive review of previous information security surveys has highlighted a gap in research. Although a number of organisations (see, for example, Deloitte, 2011; Ernst & Young, 2011; PricewaterhouseCoopers, 2013) conduct yearly information security surveys, these surveys traditionally collect information about security breaches and their impact and do not seek to establish what users think, know or do about information security issues. These surveys have also been criticised for flaws in their methodologies, the design of their questions, and their statistical reporting (Guillot & Kennedy, 2007; Walsh, 2006). For example, Anderson and colleagues (2012) suggest that these studies may suffer from response effects and sampling bias, which could result in an under-reporting of security issues. Furthermore, these surveys are often sponsored by vendors with an interest in providing specific solutions. This could cause conflicting motives, which could result in an over-reporting of certain security issues (Anderson, et al., 2012). Additionally, these surveys are usually conducted solely with information security professionals, and although this reveals important information regarding the technologies and other safeguards in place within an organisation, this does not necessarily represent the views or experiences of the majority of computer users (Herath & Rao, 2009).

There is a growing body of literature that attempts to apply existing behavioural models to the area of information security. For example, models such as the Theory of Planned Behaviour (Bulgurcu, 2008), the Health Belief Model (Ng, Kankanhalli, & Xu, 2009), the Protection Motivation Theory (Vance, 2010), the General Deterrence Theory (Fan & Zhang, 2011) and the Knowledge-Attitude-Behaviour (KAB) model (Kruger & Kearney, 2006) originally developed in fields including health, criminology and environmental psychology. According to Karjalainen (2011), many of these previous studies of information security behaviour are focused solely on theory-verification or validation, and therefore may present a biased viewpoint of the area of interest. In other words, because these studies only assess the variables in the theory under investigation, other potentially important variables are not considered.

Furthermore, there are many important differences between the field of information security and fields such as health, criminology or environmental psychology. These latter fields differ widely in regards to the ease of access and comprehension of information, the consequences for action or inaction, and the necessity to make decisions based on unclear or contradictory information. For example, topics like climate change and the health benefits or consequences of certain foods have been widely debated, which means people are faced with conflicting information, and the scientific legitimacy of this information is not always clear. In contrast, providing far less ambiguity, most organisations have an information security policy, either written or informal, which indicates what is expected from employees.

Although theories such as the Technology Acceptance Model (TAM) have been shown to predict intention to use security technologies (Davis, 1989; Mathieson, 1991) within an organisational setting, this finding may not capture the complexity of the problem. Essentially, much of the previous research has not adequately considered the unique nature of information security behaviour within an organisation. Employees work within a supported environment, where there are often multiple levels of protection and colleagues to provide assistance. The organisational setting is also generally supervisory, with potential monitoring of behaviour, and often demonstrable culpability. In most cases, there are also information technology (IT) personnel, who ensure that anti-virus software is installed and appropriately updated, firewalls are adequately implemented, and information is regularly backed-up. It is not necessary for most employees to have a comprehensive understanding of how these technologies work. Employee behaviours that are more likely to result in information security breaches, such as not choosing a strong password and opening suspicious email attachments, are not necessarily associated with the adoption of a specific technology (Ng, et al., 2009).

CONCEPTUAL MODEL DEVELOPMENT

In Parsons, McCormac, Pattinson, Butavicius and Jerram (2013), we reported on the results of an information security study with three Australian government organisations. Rather than focusing solely on theory-verification, we used a hybrid methodology, incorporating the inductive, exploratory approach recommended by Karjalainen (2011). We use the term 'hybrid' to denote a blend of qualitative and quantitative methods for gathering and analysing data. Interviews were conducted with senior management of each organisation (qualitative data), and the findings of the interviews assisted in developing the areas covered in our initial (predominantly quantitative) information security questionnaire. This questionnaire was then completed by 203 employees from the three government organisations. The resultant exploratory process eventually yielded the hypothesis that as computer users' level of knowledge of information security policy and procedures is raised, their attitude towards information security policy and procedures improves, which should translate into more risk-averse information security behaviour. This process of change is sometimes referred to as the KAB model (Baranowski, Cullen, Nicklas, Thompson, & Baranowski, 2003; Khan, Alghathbar, Nabi, & Khan, 2011; Kruger & Kearney, 2006), and a refined and specific version of this model is one component of the HAIS-Q.

There is disagreement in the literature regarding the usefulness or validity of the KAB model. For example, van der Linden (2012) examined previous research in the area of climate change and claimed there is "ample evidence" (p.13) in support of a significant relationship between environmental knowledge and attitudes and behaviours. Bettinghaus (1986) examined the model's relevance to health promotion, and concluded that there is a positive but small relationship between knowledge, attitude and behaviour. However, Kollmus and Agyeman (2002) criticised the model for being too rationalist, and Baranowski and colleagues (2003) examined its relevance in the health field, and concluded that "scientific support for the knowledge component of KAB models is weak" (p. 26S). However, according to McGuire (1969), the problem with the KAB model is not the theoretical model itself, but rather, the way the model is applied. In many cases, the concept of knowledge is not clearly specified (Baranowski, et al., 2003). For example, in regards to diet, knowledge could be assessed in respect to the health outcomes of certain foods, how to find nutritional information or how to best prepare food.

Individual responses in many of these areas would be strongly influenced by additional factors, such as self-efficacy (e.g., the ability to cook) (Baranowski, et al., 2003). Essentially, the variables of interest must be specified clearly and related to the other variables associated with the overall process of behavioural change for use of the KAB model to be evaluated with integrity.

THE HAIS MODEL AND QUESTIONNAIRE

Our model abides by McGuire's (1969) recommendation; knowledge was conceptualised first, and specifically, as 'knowledge of policy and procedures'. Within that refined context, we reviewed several information security policies and used the findings of our senior management interviews to develop specific focus areas. These were designed to represent the areas of an information security policy that are relevant to employers and computer users and most prone to non-compliance. From this process, we identified seven focus areas; these are internet use, email use, social networking site use, password management (including locking workstations), incident reporting, information handling and mobile computing.

For each focus area, we developed three representative areas, which can be seen in Table 1. These areas were developed to specifically represent common areas of risk-taking behaviour by computer users. For each of these representative areas, we developed one specific knowledge question, one specific attitude question and one specific behaviour question. For example, the following statements measure the sub-area *consequences of social networking sites* (within the *social networking site use* focus area):

- Knowledge: *"I can't be fired for something I have posted on a social networking web site."*
- Attitude: *"It is a bad idea to post things on social networking web sites about my work that I wouldn't say in a public place."*
- Behaviour: *"I would consider the negative consequences to my job before I post anything on social networking web sites."*

Three representative areas were chosen as this maintained a balance between the scientific need to obtain a specific measure of the most important areas and the practical need to limit the length of the questionnaire. This means the KAB component of the HAIS-Q consists of 63 specific statements. A five point Likert scale, rated from Strongly Agree to Strongly Disagree, was used for all of the items. These statements are more specific tests of the variables of interest than other information security surveys that tend to measure information security in a very general manner. For example, Siponen, Pahnila and Mahmoud (2010) tested an individual's information security-related behaviour by asking participants to respond to the statement *"I comply with information security policies"* and their intention to comply with the statement *"I intend to comply with information security policies"*. These items do not test specific knowledge, and are potentially more prone to response bias.

Table 1: Focus areas with representative areas

Focus Area	**Sub-areas**
Password Management	Locking workstations Password sharing Choosing a good password
Email Use	Forwarding emails Opening attachments IT department level of responsibility
Internet Use	Installing unauthorised software Accessing dubious websites Inappropriate use of internet
Social Networking Site (SNS) Use	Amount of work time spent on SNS Consequences of SNS Posting about work on SNS
Incident Reporting	Reporting suspicious individuals Reporting bad behaviour by colleagues Reporting all security incidents
Mobile Computing	Physically securing personal electronic devices Sending sensitive information via mobile networks

	Checking work email via free network
Information Handling	Disposing of sensitive documents
	Inserting DVDs / USB devices
	Leaving sensitive material unsecured

It is important to highlight that the KAB statements represent only one part of an overall conceptual model that is being developed, tested and validated using a hybrid, exploratory, iterative approach. We believe the relationship between knowledge, attitude and behaviour is influenced by many individual, intervention and organisational factors as shown in Figure 1. For example, psychological factors; training and seminars attended; and an organisation's information security culture (Veiga & Eloff , 2010) all have the potential to impact on the knowledge, attitude and behaviour of employees. For this reason, the HAIS-Q includes specific items to measure each of the factors depicted in Figure 1 (e.g., organisational factors are measured via organisational and security culture, subjective norms, rewards and punishments). However, the assessment of the influence of these factors on KAB and the different focus areas is part of a larger project, which is beyond the scope of the current paper. Our seven focus areas are displayed in Figure 1 as separate, parallel models because, to date, no research has investigated whether knowledge, attitude and behaviour will be consistent across the different information security policies and procedures.

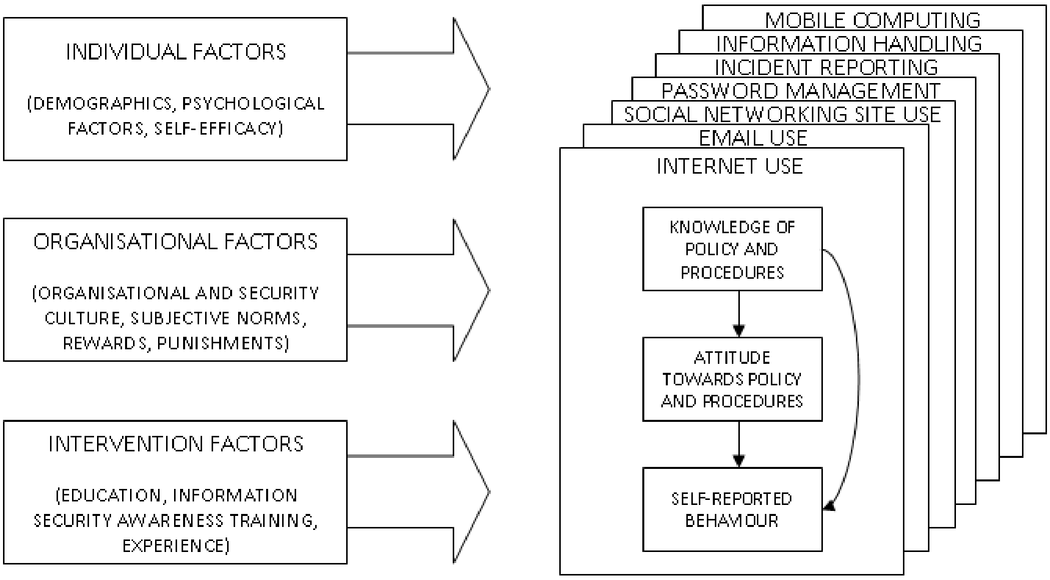
INDIVIDUAL FACTORS
(DEMOGRAPHICS, PSYCHOLOGICAL FACTORS, SELF-EFFICACY)
ORGANISATIONAL FACTORS
(ORGANISATIONAL AND SECURITY CULTURE, SUBJECTIVE NORMS, REWARDS, PUNISHMENTS)
INTERVENTION FACTORS
(EDUCATION, INFORMATION SECURITY AWARENESS TRAINING, EXPERIENCE)
MOBILE COMPUTING
INFORMATION HANDLING
INCIDENT REPORTING
PASSWORD MANAGEMENT
SOCIAL NETWORKING SITE USE
EMAIL USE
INTERNET USE
KNOWLEDGE OF POLICY AND PROCEDURES
ATTITUDE TOWARDS POLICY AND PROCEDURES
SELF-REPORTED BEHAVIOUR

Figure 1: The Human Aspects of Information Security (HAIS) Model

The aim of the current study is to examine the relationships between knowledge of policy and procedures, attitude towards policy and procedures and behaviour when using a work computer and we are addressing this aim through the following hypotheses:

- H1: Better knowledge of policy and procedures is associated with better attitude towards policy and procedures.
- H2: Better attitude towards policy and procedures is associated with self-reported behaviour that is more risk averse.
- H3: Better knowledge of policy and procedures is associated with self-reported behaviour that is more risk averse.

This component of the model is shown in Figure 2, with labels for the associated hypotheses.

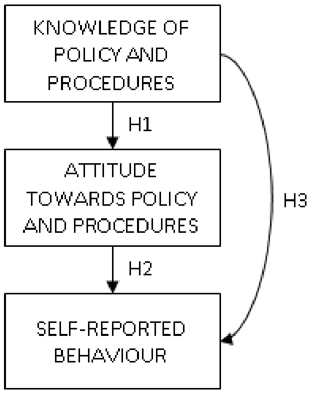
KNOWLEDGE OF POLICY AND PROCEDURES
H1
ATTITUDE TOWARDS POLICY AND PROCEDURES
H2
SELF-REPORTED BEHAVIOUR
H3

Figure 2: The KAB component of the HAIS Model

METHOD

In line with our inductive, exploratory approach, the methodology of this paper is presented in three phases. The first is the pre-testing or validity phase, which was designed to ascertain the content and face validity of the HAIS-Q. The second phase is a pilot study, which was conducted to further refine and examine the reliability of the HAIS-Q, These phases provided preliminary evidence of validity and reliability in the HAIS-Q, and justified implementing the main study, which is presented in phase three.

Phase One – Validity Testing

Before commencing the main study, three pre-testing techniques were utilised to further test the validity and reliability of the survey items. First, an expert in survey design was asked to complete the survey, and a respondent debriefing was conducted. In line with the technique described by DeMaio and Rothbeg (1996), this expert was asked about their understanding of terms, the clarity of directions and any other areas of potential misunderstanding. Following this, cognitive testing, which involves a combination of think-aloud and verbal probing (Draugalis, Coons, & Plaza, 2008; Fowler, 1995) was conducted with an expert in information security. This required the expert to complete the survey with researchers present and to verbalise whatever came to mind while answering (Willis, 2004). Where the researchers believed the think-aloud process had not sufficiently described how the respondent understood, mentally processed and answered survey items, probes were used to obtain additional information. In line with the examples provided by Collins (2003), the researchers asked questions such as “I noticed you hesitated before you answered – what were you thinking about?” and “What did the term X mean to you?” The respondent debriefing and cognitive testing helped to identify any unclear items and to establish the content and face validity of the survey.

Next, a pilot study was conducted, and the results were examined to identify any remaining problematic items and to establish the reliability of the main components of the survey.

Phase Two – Pilot Study

One-hundred and twenty working Australians completed the pilot version of the HAIS-Q. Participants were required to read the information sheet and consent form, and were then asked to complete the HAIS-Q. The questionnaire was completed online using the Qualtrics survey platform[1]. Because the items are based on computer use and adherence to information security policy within an organisation, three exclusion criteria were applied. These were employment status (participants who responded with ‘Not employed’ were excluded), amount of work time spent using a computer or portable device (participants who responded with ‘No time at all’ were excluded) and whether their organisation has an information security policy (participants who responded with ‘No’ or ‘Unsure’ were excluded). This ensured that all respondents worked within an organisation with at least an informal policy or basic rules, and had some work use of a computer or portable device. Whilst we acknowledge that excluding participants who responded with ‘Unsure’ may rule out those

[1] Qualtrics is a research software company that provides survey data collection via a ‘panel’ of in excess of 6 million people who have agreed to receive emails regarding research participation. A closed, ‘by-invitation-only’ panel recruitment method was utilised. More information on recruitment, privacy and panel incentives is available here: http://www.researchnow.com/en-US/Panels.aspx.

with very poor security awareness, this was necessary, as the HAIS-Q measures knowledge of and attitude towards policy and procedure. For the pilot study, no participants fit these three criteria.

Seven participants were excluded based on the 'suspicious case' criteria. Essentially, the HAIS-Q includes a total of 63 knowledge, attitude and behaviour statements, and 10 personality statements. Of the 63 statements, 29 are positively worded and 34 are negatively worded, and each of the Big Five personality factors had a statement measuring the trait at one end of the spectrum (e.g., extraversion) and a statement measuring the opposing personality trait (e.g., introversion) (Gosling, Rentfrow & Swann, 2003). This means that participants who provide the same uniform response for all statements are probably not answering with due care or attention. Responses to these statements were examined for any evidence of uniformity, and cases where participants responded in an identical manner to 53 or more of the 63 statements or all 10 of the personality statements were examined in detail. This identified seven suspicious cases. It was concluded that these participants were not answering honestly, and they were therefore excluded. This left 113 valid responses, 53 of which were male and 60 female. These participants took an average of 18 minutes and 5 seconds (SD = 11 minutes and 24 seconds) to complete the survey.

Consistent with the technique utilised by Arachchilage and Love (2013), Cronbach's alpha was used as a measure of the internal consistency of the survey. This refers to the degree to which the items measure the same underlying construct, and a reliable scale should have a Cronbach's alpha coefficient above 0.70 (Cronbach, 1951). As shown in Table 2, Cronbach's alpha coefficients for each of the three main constructs (i.e., knowledge of policy and procedure, attitude towards policy and procedure and self-reported behaviour) all exceeded this recommended value.

Table 2: Cronbach's alpha coefficients for the KAB survey components in the pilot study

Constructs	**Cronbach's alpha**
Knowledge of policy and procedures	0.875
Attitude towards policy and procedures	0.878
Self-reported behaviour	0.906

A series of Pearson product-moment correlations was conducted to further assess the relationship between the items used to create the three main constructs. An examination of the correlation matrices revealed that all items significantly correlated at 0.3 or above with, on average, 40% of the other items in that construct. The items with three or fewer correlations at 0.3 or above with other items in the construct were examined in detail to ensure they were clearly worded and accurately measuring the item of interest.

This revealed 10 items that were subsequently altered. Some of these items were deemed to be too complicated, and it was thought that a simplification may prevent respondent confusion. For example, the mobile computing statement *"Even if I am having trouble meeting a deadline, it is never acceptable for me to send sensitive work documents via a mobile phone network"* was simplified to *"It is a bad idea to send sensitive work documents using a mobile phone"*. Some of the altered items included unclear terms. For example, the use of the term 'unknown origin' in the information handling statement *"I must not insert a USB flash drive of unknown origin into my work computer"* was deemed to be unclear, and a more specific example was used (i.e., *"If I find a USB flash drive in a public place like a car park, I must not insert it into my work computer"*).

The results of the respondent debriefing, cognitive testing and pilot study provided preliminary evidence of validity and reliability in the HAIS-Q, and justified implementing the main study.

Phase Three – Main Study

Participants

In the main study, 1073 Australians attempted the survey. The same exclusion criteria employed in the pilot study were used. On this basis, 348 participants were excluded because they were not employed, 67 because they spend 'No time at all' using a computer or portable device at work, and 138 participants were excluded because their organisation has no information security policy (53 responses) or they were unsure if their organisation has an information security policy (85 responses). Of the 520 remaining participants, a further 20 responses were excluded based on the same 'suspicious case' criteria employed in the pilot study. This left 500 valid responses, with 51% of respondents male and 49% female. The median time to complete the questionnaire was 23 minutes, with an average time of 37 minutes and 12 seconds (SD = 97 minutes and 40 seconds). This very large standard deviation was likely caused by participants alternating survey completion with other work; 6 respondents took in excess of five hours, and of these, three required in excess of 10 hours.

Procedure

In line with the procedure utilised for the pilot study, participants were required to read the information sheet and consent form, and were then asked to complete the HAIS-Q. Again, the questionnaire was completed online, using the Qualtrics survey platform.

RESULTS

As in the pilot study, Cronbach alpha was calculated for each of the three main constructs as a measure of the internal consistency of the survey items. As shown in Table 3, these scores all exceeded the recommended cut-off value of 0.7, which provides evidence of a high degree of reliability and suggests the items in the scales are measuring the same underlying construct.

Table 3: Cronbach's alpha coefficients for the KAB survey components in the main study

Constructs	**Cronbach's alpha**
Knowledge of policy and procedures	0.844
Attitude towards policy and procedures	0.884
Self-reported behaviour	0.918

To further test the relationship between the items used to create the three main constructs (i.e., knowledge of policy and procedures, attitude towards policy and procedures and self-reported behaviour) a series of Pearson product-moment correlation coefficients were calculated. There was a significant positive relationship between all variables, with correlations ranging between .326 and .695, which indicates a strong relationship, but does not indicate multicollinearity. This therefore provides further support for the reliability of the HAIS-Q, and provides justification for creating total knowledge, attitude and behaviour scores, which can be used to test hypotheses 1, 2 and 3.

As noted earlier, the aim of the current paper is to test the hypothesis that there is a significant positive relationship between respondents' knowledge of policy and procedures, attitude towards policy and procedures and their behaviour when using a work computer. This theory was tested using path-analysis, which is a statistical technique for empirically examining sets of relationships to test the fit of causal models (Huang & Liaw, 2005; Lleras, 2005). It involves using a multiple regression analysis for each of the endogenous variables in the model (Huang & Liaw, 2005; Mathieu, 1988).

The model under evaluation has two endogenous variables (viz., attitude and behaviour) and one exogenous variable (viz., knowledge). Hence, two multiple regressions were conducted. The first regression tested whether knowledge of policy and procedure predicted attitude towards policy and procedures, and produced an R squared of .659, which was statistically significant ($F(1,498) = 960.77$, $p < .001$). The second regression tested whether participants' knowledge of policy and procedures and attitude towards policy and procedures predicted their self-reported behaviour. This produced an R squared of .777, which was statistically significant ($F(2,497) = 863.44$, $p < .001$). Both knowledge ($\beta = .185$, $t = 5.097$, $p < .001$) and attitude ($\beta = .724$, $t = 19.96$, $p < .001$) were positively related to behaviour. These results indicate that approximately 78% of the variance in self-reported behaviour was accounted for by knowledge of policy and procedure and attitude towards policy and procedure. These findings, which provide support for our model, are depicted in Figure 3.

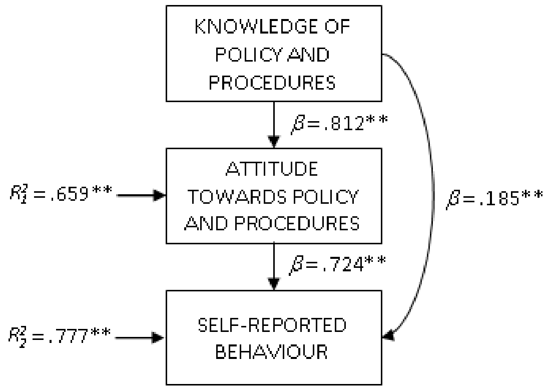

Figure 3: Findings in support of the KAB component of the HAIS Model (** p < .01)

This provides support for the hypotheses that better knowledge of policy and procedures is associated with better attitude towards policy and procedure, and better knowledge and attitude towards policy and procedure are both associated with self-reported behaviour that is more risk averse. However, we acknowledge that the support for our proposed model does not discount the existence of other, competing models (MacCallum, Wegener, Uchino, & Fabrigar, 1993). For instance, it is conceivable that behaviour when using a work computer could, in fact, influence an employee's attitude towards policy and procedure. This is because most information security vulnerabilities are low-probability, high-consequence threats, and evidence suggests that people tend to repeat behaviours that are rewarded (Slovic, Fischhoff, & Lichtenstein, 1978; Thorndike, 1913). For example, if a computer user violates policy and accesses sensitive information from an unfamiliar wireless network, the consequences if this information is intercepted may be high, but the probability of interception is very low, and hence, each experience of using an unfamiliar wireless network without any negative consequences will reinforce or reward that insecure behaviour, and may change an individual's attitude towards that policy. Similarly, there may be cases where employees know an information security policy and may believe that it is unnecessary or excessive, but they may still do the right thing, even when their attitude towards the instruction is poor. This may be due to other mediating factors, such as the desire to keep one's job. These alternate models may describe the relationship between knowledge, attitude and behaviour in rare cases, and will be examined in future research. However, on balance, our model as depicted in Figure 3 best describes the majority of computer users, and hence, has the best potential to explore further.

DISCUSSION AND CONCLUSIONS

The purpose of this study was to outline the development and initial reliability and validity testing of our HAIS-Q and to establish whether there is a positive relationship between respondents' knowledge of policy and procedures, attitude towards policy and procedures and their self-reported behaviour when using a work computer. The data presented in this study support this hypothesis, and provide support for our model and questionnaire.

The results shown in Figure 3 indicate that participants' knowledge of policy and procedure and attitude towards policy and procedure explain a significant amount of the variance in participants' self-reported behaviour. Interestingly, however, the Beta (β) values reported in Figure 3 indicate that an employee's knowledge of policy and procedures had a far stronger influence on attitude towards policy and procedure (β = .812) than self-reported behaviour (β = .185). This suggests the effect of knowledge on behaviour is mediated by attitude towards policy and procedure.

This has implications for training and education campaigns, as it suggests that employers can be relatively confident that improving their employees' knowledge of policy and procedures will have a positive impact on both attitude towards those policies and procedures and employee behaviour. However, our results also indicate that generic courses that do not attempt to influence attitude and instead simply lecture on knowledge of policy and procedure will be far less effective. Instead, training should be contextualised and should use case studies to improve both knowledge of what is expected and also understanding of why this is important (Brooke, 2006; Parsons, McCormac, Butavicius, & Ferguson, 2010).

Future studies will examine individual, organisational and interventional factors, and determine whether these factors have a statistically significant effect on the behaviour of employees and therefore on the security of an organisation's information systems. Future studies will also further develop the HAIS-Q in line with the validation guidelines outlined by Straub, Boudreau and Gefen (2004). For example, alternate measures of knowledge, attitude and behaviour will be obtained to assess the construct validity of the HAIS-Q. The questionnaire will also be implemented on employees within known organisations, which will allow us to assess the actual policies and procedures and methods of training within the organisation and how these influence the responses provided by employees. This will allow us to further test the conclusion of this paper, that generic training courses that only outline requirements will be less effective than contextualised training aimed at improving both knowledge and understanding of policy and procedures.

REFERENCE LIST

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M.J.G., Levi, M., and Savage, S. 2012. "Measuring the cost of cybercrime," *11th Annual Workshop on the Economics of Information Security*, June, Berlin, Germany.

Arachchilage, N.A.G., and Love, S. 2013. "A game design framework for avoiding phishing attacks," *Computers in Human Behavior* (29:3), May, pp 706-714.

Baranowski, T., Cullen, K.W., Nicklas, T., Thompson, D., and Baranowski, J. 2003. "Are current health behavioral change models helpful in guiding prevention of weight gain efforts?" *Obesity Research* (11), October, pp 23S-43S.

Bettinghaus, E.P. 1986. "Health promotion and the knowledge-attitude-behavior continuum," *Preventive Medicine* (15:5), September, pp 475-491.

Brooke, S.L. 2006. "Using the case method to teach online classes: Promoting Socratic dialogue and critical thinking skills," *International Journal of Teaching and Learning in Higher Education* (18:2), pp 142-149.

Bulgurcu, B. 2008. *The antecedents of information security policy compliance*. MSc Thesis, The University of British Columbia, Canada.

Collins, D. 2003. "Pretesting survey instruments: an overview of cognitive methods," *Quality of Life Research* (12:3), May, pp 229-238.

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

Da Veiga, A. & Eloff, J.H.P. (2010). "A framework and assessment instrument for information security culture," *Computers & Security* (29), pp 196-207.

Davis, F.D. 1989. "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS quarterly*, (13:3), September, pp 319-340.

Deloitte. 2011. *Raising the Bar: 2011 TMT Global Security Study - Key Findings.* Report published by Deloitte, 24p.

DeMaio, T.J., and Rothgeb, J.M. 1996. Cognitive interviewing techniques: In the lab and in the field. In N. Schwartz & S. Sudman (Eds.), *Answering questions: Methodology for determining cognitive and communicative processes in survey research (pp. 177-195)*. San Francisco: Jossey-Bass.

Draugalis, J.R., Coons, S.J., and Plaza, C.M. 2008. "Best practices for survey research reports: a synopsis for authors and reviewers," *American journal of pharmaceutical education* (72:1) February, Article 11.

Ernst & Young. 2011. *Into the Cloud, out of the Fog: Ernst & Young's 2011 Global Information Security Survey*. Report published by Ernst & Young.

Fan, J., and Zhang, P. 2011. "Study on e-government information misuse based on General Deterrence Theory," *8th International Conference on Service Systems and Service Management (ICSSSM)*, June, Tianjin, pp 1-6.

Fowler, F.J. 1995. *Improving survey questions: Design and evaluation* Applied Social Research Methods Series, Volume 38. Thousand Oaks, CA: Sage Publications, Incorporated.

Gosling, S.D., Rentfrow, P.J, and Swann, W.B. 2003. "A very brief measure of the Big-Five personality domains," *Journal of Research in Personality* (37:6), December, pp 504-528.

Guillot, A., and Kennedy, S. 2007. "Information Security Surveys: A Review of the Methodologies, the Critics and a Pragmatic Approach to their Purposes and Usage," *5th Australian Information Security Management Conference*, December, Perth, Australia.

Herath, T., and Rao, H.R. 2009. "Encouraging information security behaviors in organizations: Role of penalities, pressures and perceived effectiveness," *Decision Support Systems* (47:2), May, pp 154-165.

Huang, H.M., and Liaw, S.S. 2005. "Exploring users' attitudes and intentions toward the web as a survey tool. Computers in Human Behavior," (21:5), September, pp 729-743.

Karjalainen, M. 2011. *Improving Employees' Information Systems (IS) Security Behaviour: Toward a Meta-Theory of IS Security Training and a New Framework for Understanding Employees' IS Security Behaviour*. PhD, The University of Oulu, Oulu, (A 579).

Khan, B., Alghathbar, K.S., Nabi, S.I., and Khan, M.K. 2011. "Effectiveness of information security awareness methods based on psychological theories," *African Journal of Business Management* (5:26), October, pp 10862-10868.

Kollmuss, A., and Agyeman, J. 2002. "Mind the gap: why do people act environmentally and what are the barriers to pro-environmental behavior?" *Environmental education research* (8:3), August, pp 239-260.

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

Lleras, C. 2005. "Path analysis," *Encyclopedia of social measurement* (3), pp 25-30.

MacCallum, R. C., Wegener, D. T., Uchino, B. N., and Fabrigar, L. R. 1993. "The problem of equivalent models in applications of covariance structure analysis," *Psychological bulletin* (114:1), July, pp 185-185.

Mathieson, K. 1991. "Predicting user intentions: comparing the technology acceptance model with the theory of planned behaviour," *Information systems research* (2:3), September, pp 173-191.

Mathieu, J. E. 1988. "A causal model of organizational commitment in a military training environment," *Journal of Vocational Behavior, 32(3)*, June, pp 321-335.

McGuire, W. J. (Ed.). 1969. *The nature of attitudes and attitude change (Vol. 3)*. Reading, Mass: Addison-Wesley.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. 2009. "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems* (46), March, pp 815-825.

Parsons, K., McCormac, A., Butavicius, M., and Ferguson, L. 2010. *Human Factors and Information Security: Individual, Culture and Security Environment*, Report published by Defence Science and Technology Organisation, DSTO-TR-2484, 45p.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. and Jerram, C., 2013, "An Analysis of Information Security Vulnerabilities at Three Australian Government Organisations", *Proceedings of the European Information Security Multi-Conference (EISMC 2013)*, Lisbon, Portugal, published by Plymouth University, UK.

PricewaterhouseCoopers. 2013. *Changing the game - Key findings from The Global State of Information Security Survey 2013*. Report published by PricewaterhouseCoopers.

Reichardt, C. S. 2002. "The priority of just-identified, recursive models," *Psychological Methods* (7:3), September, pp 323-337.

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

Slovic, P., Fischhoff, B., and Lichtenstein, S. 1978. "Accident probabilities and seat belt usage: A psychological perspective," *Accident Analysis and Prevention* (10:4), December, pp 281-285.

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

Thorndike, E.L. 1913. *The Psychology of Learning*. New York: Teachers College.

Tomarken, A.J., and Waller, N.G. 2003. "Potential problems with "well fitting" models," *Journal of abnormal psychology* (112:4), November, pp 578-598.

van der Linden, S. 2012. "Understanding and achieving behavioural change: Towards a new model for communicating information about climate change," *International Workshop on Psychological and Behavioural Approaches to Understanding and Governing Sustainable Tourism Mobility*, Freiburg, Germany.

Vance, A. 2010. *Why Do Employees Violate IS Security Policies? Insights From Multiple Theoretical Perspectives*. PhD, The University of Oulu, Oulu, (A 563).

Walsh, C. 2006. "CSI/FBI Survey considered harmful". Retrieved November, 2012, from http://www.emergentchaos.com/archives/2006/07/csifbi_survey_considered.html

Willis, G.B. 2004. *Cognitive Interviewing: A Tool for Improving Questionnaire Design*. Thousand Oaks, CA: Sage.

COPYRIGHT