Computers in Human Behavior 69 (2017) 151–156

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full length article

Individual differences and Information Security Awareness

Agata McCormac [a,*], Tara Zwaans [b], Kathryn Parsons [a], Dragana Calic [a], Marcus Butavicius [a], Malcolm Pattinson [c]

[a] Defence Science and Technology Group, PO Box 1500, Edinburgh, SA, 5111, Australia
[b] School of Psychology, The University of Adelaide, SA, 5005, Australia
[c] Adelaide Business School, The University of Adelaide, SA, 5005, Australia

ARTICLE INFO

Article history:
Received 15 June 2016
Received in revised form
29 November 2016
Accepted 30 November 2016
Available online 1 December 2016

Keywords:
Information Security Awareness (ISA)
Information security (InfoSec)
Cyber security
Personality
Risk
Individual differences

ABSTRACT

The main purpose of this study was to examine the relationship between individuals' Information Security Awareness (ISA) and individual difference variables, namely age, gender, personality and risk-taking propensity. Within this study, ISA was defined as individuals' knowledge of what policies and procedures they should follow, their understanding of why they should adhere to them (their attitude) and what they actually do (their behaviour). This was measured using the Human Aspects of Information Security Questionnaire (HAIS-Q). Individual difference variables were examined via a survey of 505 working Australians. It was found that conscientiousness, agreeableness, emotional stability and risk-taking propensity significantly explained variance in individuals' ISA, while age and gender did not. Findings highlighted the need for future research to examine individual differences and their impact on ISA. Results of the study can be applied by industry to develop tailored InfoSec training programs.

1. Introduction

This study aims to examine the relationship between individual differences and Information Security Awareness (ISA). ISA was measured using the Human Aspects of Information Security Questionnaire (HAIS-Q), which is based on the knowledge, attitude and behaviour (KAB) model. The following sections will introduce the main constructs considered in this study, namely, the human aspects of information security, the KAB model and individual factors. Results of this research may assist with explaining the variance in ISA amongst employees within organisations.

1.1. Human aspects of information security

Despite employing state-of-the-art technical controls, organisations continue to experience security breaches. The number and impact of information security (InfoSec) breaches is rising, with 38% more security incidents reported during the 2014/15 financial year. On average, these organisations reported a loss of $2.5 million (Pricewaterhouse Coopers, 2015). Security incidents within an organisation were found to outweigh the number of those arising from external parties. Findings suggest that the behaviour of current employees was the source of 34% of security incidents (Pricewaterhouse Coopers, 2015). Consequently, technical measures alone are inadequate to ensure an organisation's InfoSec (Furnell, Jusoh, & Katsabas, 2006; McCormac, Parsons, & Butavicius, 2012; Parsons, McCormac, Butavicius, & Ferguson, 2010; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Schultz, 2005). This highlights the need for a greater focus on human aspects of InfoSec (Australian Standard, 2015; Schneier, 2000; Shropshire, Warkentin, Johnson & Schmidt, 2006).

1.2. Information Security Awareness (ISA) and the knowledge – attitude – behaviour (KAB) model

ISA focuses on the extent to which an employee understands the importance and implications of InfoSec policies, rules and guidelines, and, the extent to which they behave in accordance with these policies, rules and guidelines (Kruger & Kearney, 2006). This definition is consistent with the KAB model that underpins the

[*] Corresponding author. Defence Science and Technology Group, PO Box 1500, Edinburgh, SA, 5111, Australia.

E-mail addresses: agata.mccormac@dsto.defence.gov.au (A. McCormac), tara.zwaans@student.adelaide.edu.au (T. Zwaans), kathryn.parsons@dsto.defence.gov.au (K. Parsons), dragana.calic@dsto.defence.gov.au (D. Calic), marcus.butavicius@dsto.defence.gov.au (M. Butavicius), malcolm.pattinson@adelaide.edu.au (M. Pattinson).

http://dx.doi.org/10.1016/j.chb.2016.11.065
0747-5632/Crown Copyright © 2016 Published by Elsevier Ltd. All rights reserved.

HAIS-Q. In the context of ISA as an employee's level of knowledge of InfoSec policy and procedures increases, their attitude towards InfoSec policy and procedures improves, resulting in improved InfoSec behaviour.

The KAB model has been criticised by some researchers. Bettinghaus (1986) identified a small positive relationship between knowledge, attitude and behaviour, and Baranowski, Cullen, Nicklas, Thompson, and Baranowski (2003) found weak evidence of its applicability within the health field. Conversely, Van der Linden (2012), examined its validity with regard to climate change, and identified significant relationships between knowledge, attitude and behaviour. McGuire (1969) suggested that the problem is not with the model itself, but with the way in which it is applied. It is important to clearly conceptualise the type of knowledge that a particular study is examining. It is also essential to consider how the model relates to other variables of interest, and how they are measured.

1.2.1. *The Human Aspects of Information Security Questionnaire (HAIS-Q)*

As noted above, the KAB model underpins the HAIS-Q, an instrument developed to measure ISA. Within this questionnaire, knowledge is defined as knowledge of InfoSec policies and procedures. The questionnaire was developed in consultation with managers, information technology professionals, and a review of InfoSec policies and standards (Parsons et al., 2014). As shown in Fig. 1, the HAIS-Q comprises of seven focus areas: *Internet use, Email use, Social media use, Password management, Incident reporting, Information handling, Mobile computing*. Each focus area contains statements relating to knowledge, attitude and behaviour. For example, within the password management focus area, the specific statements include:

> *Knowledge: "I am allowed to share my work passwords with a colleague"*
>
> *Attitude: "It's a bad idea to share my work passwords, even if a colleague asks for it"*
>
> *Behaviour: "I share my work passwords with colleagues"*

As demonstrated in Fig. 1, a number of individual, organisational and intervention factors could influence the relationship between knowledge, attitude and behaviour. This is supported by Vroom and Von Solms (2004), who proposed that an organisation's culture is likely to impact both individual behaviour, and the number and impact of breaches experienced by organisations (Vroom & Von Solms, 2004). The current study focusses on individual factors within this model.

Parsons et al. (2014) found that knowledge of policies explained 66% of variance in attitude, while knowledge and attitude together explained 78% of the variance in self-reported behaviour. Even when controlling for attitude, knowledge remained a significant predictor of behaviour. This direct relationship between knowledge and behaviour is an extension of Kruger and Kearney's (2006) use of the KAB model.

1.3. *Individual factors*

It is important to consider the potential impact of individual differences on ISA. Understanding the variability between individuals is essential to understanding the underlying psychological mechanisms which may impact user awareness with regard to InfoSec (Heinström, 2003; Stankov, Boyle, & Cattell, 1995). This can in turn, be used to tailor intervention programs, for example training, for individuals to improve ISA.

1.3.1. *Demographics*

Recent InfoSec research has found small differences between males and females, and individuals of different ages. A role-play phishing study found that women were more susceptible to opening and clicking on links in phishing emails, and individuals aged between 18 and 25 years were more susceptible to phishing compared to older age groups (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010).

Pattinson, Butavicius, Parsons, McCormac, and Calic (2015) examined the behavioural component of the HAIS-Q and found no significant gender differences. However, they found a significant positive relationship between age and InfoSec behaviour, indicating that older adults may have better InfoSec behaviour. As behaviour is only one component of ISA, as defined within the KAB model, this was a limitation of the study.

1.3.2. *Personality and The Big Five model*

The Big Five personality model has been used extensively to understand and predict numerous factors in diverse and complex environments (Shropshire, Warkentin, Johnston, & Schmidt, 2006). The five-factor model of personality, often referred to as The Big Five, is considered to be the leading theoretical model for measuring and understanding personality (Shropshire et al., 2006). It comprises of the following five factors: neuroticism, extraversion, openness, agreeableness and conscientiousness (Costa & McCrae, 1992; John & Srivastava, 1999).

While little research has examined the relationship between personality and ISA, Shropshire et al. (2006) suggested drawing from literature on workplace safety and personality, to guide research on ISA and personality. Cellar, Nelson, Yorke, and Bauer (2001) found a significant inverse relationship between conscientiousness and agreeableness, and the total number of workplace accidents. This suggests that individuals who are more conscientiousness and agreeable experience fewer workplace accidents (Cellar et al., 2001).

In a study exploring personality and self-reported intention to adopt a web-based security software program, it was found that high agreeableness was related to intent to adopt and actual use of security software (Shropshire, Warkentin, & Sharma, 2015). It has also been suggested that individuals who score high on the factor of agreeableness may be more worried about what others think of them, and are therefore more likely to be concerned with security issues (Korzaan & Boswell, 2008; Shropshire et al., 2015). Furthermore, even when individuals did not know that their behaviour was monitored, traits such as "rule following" were positively associated with conscientiousness and agreeableness (Organ & Paine, 1999).

Pattinson et al. (2015) examined non-malicious computer-based behaviour and individual factors, including the employee's age, education level, familiarity with computers and personality. This research found that employees' accidental-naïve behaviour is likely to be less risky if they are more conscientious, more agreeable, less impulsive, more open and less familiar with computers. However, the study was limited in its use of the Ten-Item Personality Inventory (Gosling, Rentfrow, & Swann, 2003). While this measure was considered adequate for their exploratory study, in the current study we have used a more robust measure of personality to more accurately measure the relationship between personality and ISA.

1.3.3. *Risk-taking propensity*

Risk-taking propensity has been defined as the tendency of an individual to either take risks or avoid risks (Nicholson, Soane, Fenton-O'Creevy, & Willman, 2005). While risk perception varies

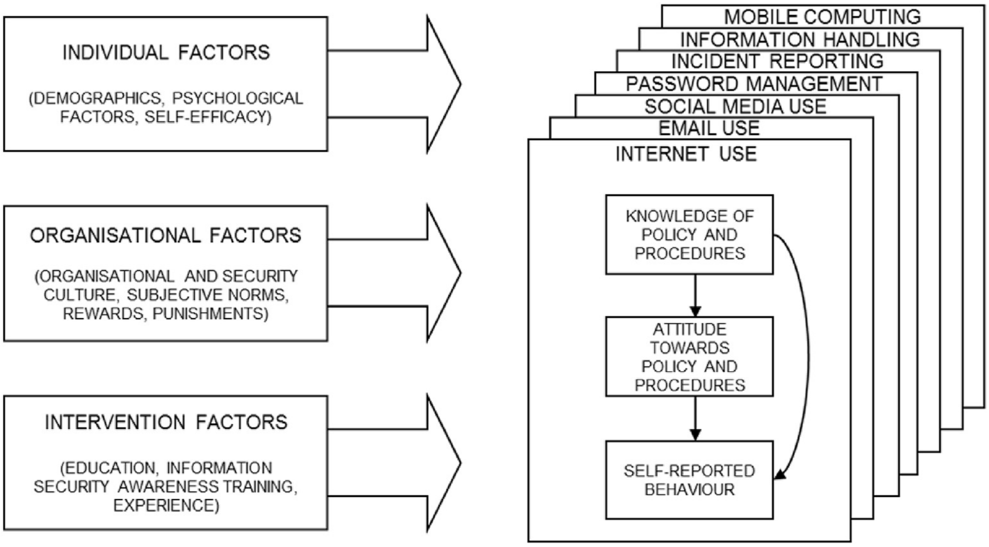
INDIVIDUAL FACTORS
(DEMOGRAPHICS, PSYCHOLOGICAL FACTORS, SELF-EFFICACY)
ORGANISATIONAL FACTORS
(ORGANISATIONAL AND SECURITY CULTURE, SUBJECTIVE NORMS, REWARDS, PUNISHMENTS)
INTERVENTION FACTORS
(EDUCATION, INFORMATION SECURITY AWARENESS TRAINING, EXPERIENCE)
MOBILE COMPUTING
INFORMATION HANDLING
INCIDENT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

Fig. 1. The human aspects of information security model (adapted from Parsons et al., 2014).

across situations, an individual's attitude to perceived risk remains relatively stable (Weber & Milliman, 1997). Everyday risk-taking behaviours tend to peak in adolescence or early adulthood, and then decrease (Figner, Mackinlay, Wilkening & Weber, 2009).

Risk taking propensity may also be related to an individual's personality. In particular, research has shown that individuals who score highly on the traits of extraversion and openness, and who also score low on agreeableness, conscientiousness and neuroticism, exhibited a higher risk propensity (Nicholson et al., 2005).

1.4. Study aims

As noted above, this study aims to investigate the relationship between ISA and individual differences. Specifically, this study will examine the following individual differences: age, gender, personality and risk-taking propensity, and the extent to which they explain variance in individual ISA.

2. Method

Data collection involved an online survey, administered through the web-based survey software Qualtrics, collected over a two-week period. Ethics approval was granted by the Human Research Ethics Subcommittee of The University of Adelaide School of Psychology, and the Defence, Science and Technology Group (DST Group) Human Research Ethics Review Panel.

2.1. Participants

Five hundred and five (286 females and 219 males) working Australians completed the questionnaire online. Approximately 12% of participants were aged between 18 and 29 years of age, about a quarter were in the age ranges of 30–39, and 40 to 49. This left approximately 22% in the 50 to 59 age category, and 15% aged 60 and over. Participants represented over 13 sectors and 8 job areas, including sales, labourers, professionals, management and technicians/trade workers.

Participants had to be over the age of 18 to participate in the study, currently employed, and working within Australia. Additional selection criteria included that they must spend some of their time at work on a computer, and that the organisation in which they work for must have either a formal InfoSec policy, or an informal policy or guidelines. These selection criteria were necessary as the survey focussed on examining factors that influence an individual's knowledge, attitude and behaviour towards their organisation's InfoSec policy, and thus, knowledge of the existence of such a policy was necessary as a point of reference.

2.2. Materials

2.2.1. Demographic information

The survey collected general demographic data, including gender and age.

2.2.2. The Human Aspects of Information Security Questionnaire (HAIS-Q)

Individual knowledge, attitude and behaviour relating to InfoSec were measured via 63 statements, on a five-point Likert scale, rated from 1 = 'Strongly Disagree', to 5 = 'Strongly Agree'. In the present study, alpha levels for knowledge, attitude and behaviour were 0.84, 0.92 and 0.90 respectively, with an alpha level of 0.96 for ISA.

2.2.3. The Big Five inventory (BFI)

The BFI is a 44-item inventory that measures an individual on The Big Five dimensions of personality (Benet-Martinez & John, 1998; John & Srivastava, 1999). Items are measured on a five-point Likert-style scale (ranging from 1 = 'Strongly Disagree' to 5 = 'Strongly Agree') with 16 reverse-scored items (John & Srivastava, 1999). Data from an Australian population suggested good internal reliability; alpha levels ranged from 0.74 to 0.81, with a mean of 0.77 (Losoncz, 2009). The current study found appropriate alpha levels of 0.85 for conscientiousness, 0.79 for agreeableness, 0.74 for openness, 0.83 for emotional stability, and 0.77 for extraversion. The BFI is considered a valid and reliable measure which has undergone extensive norming (Losoncz, 2009).

2.2.4. The Risk Averseness Scale

The Risk Averseness Scale measures an individual's propensity to take risks (Pan & Zinkhan, 2006). The measure contains five items measured on a five-point Likert-style scale (ranging from 1 = 'Strongly Disagree' to 5 = 'Strongly Agree'). Higher scores are associated with more risk-taking behaviour; for example, *"If there is*

Table 1
Correlations, means and standard deviations between knowledge, attitude, behaviour, ISA, age, The Big Five personality factors and risk-taking propensity (N = 505).

Variables	Gender	Age	Knowledge	Attitude	Behaviour	ISA	Extraversion	Agreeableness	Conscientious	Emotional Stability	Openness	Risk-taking Propensity
Age	-0.11^{*}											
Knowledge	0.14^{**}	0.13^{**}										
Attitude	0.13^{**}	0.23^{**}	0.75^{**}									
Behaviour	0.101^{*}	0.25^{**}	0.73^{**}	0.83^{**}								
ISA	0.13^{**}	0.22^{**}	0.89^{**}	0.94^{**}	0.93^{**}							
Extraversion	0.03	−0.03	0.06	0.04	0.10^{*}	0.07						
Agreeableness	0.11^{*}	0.18^{**}	0.38^{**}	0.46^{**}	0.53^{**}	0.49^{**}	0.16^{**}					
Conscientiousness	0.12^{**}	0.22^{**}	0.42^{**}	0.54^{**}	0.58^{**}	0.56^{**}	0.21^{**}	0.56^{**}				
Emotional Stability	−0.04	0.19^{**}	0.23^{**}	0.25^{**}	0.28^{**}	0.28^{**}	0.37^{**}	0.46^{**}	0.52^{**}			
Openness	0.025	−0.00	0.14^{**}	0.16^{**}	0.22^{**}	0.19^{**}	0.38^{**}	0.25^{**}	0.26^{**}	0.25^{**}		
Risk-taking	−0.04	-0.20^{**}	-0.21^{**}	-0.23^{**}	-0.22^{**}	-0.24^{**}	0.11^{*}	−0.08	-0.12^{**}	−0.07	0.14^{**}	
Mean		***	81.3	86.8	84.8	253.0	3.1	3.8	3.9	3.4	3.4	3.2
SD		***	11.3	12.2	11.8	32.5	0.7	0.5	0.6	0.7	0.5	0.6

$^{*}p < 0.05$ (2-tailed) $^{**}p < 0.01$ (2-tailed), *** Mean and SD scores for age are unavailable, as age range, not exact ages were provided by participants.

a great chance of a reward, I will take high risks." In previous research the reliability was acceptable with a Cronbach's alpha of 0.76 (Fogel & Nehmad, 2009), and the results from the present study replicated the same value.

3. Results

The main aim of this study was to investigate the relationship between individual differences and ISA. Assumption testing was conducted throughout the following analyses, with no major violations identified. SPSS was used to analyse the data set. A correlation matrix (Table 1), including mean and standard deviation scores, was produced to examine the relationship between age, individual knowledge, attitude and behaviour scores and overall ISA, in addition to The Big Five personality variables, and risk-taking propensity.

3.1. *ISA and individual differences*

ISA was measured by adding an individual's knowledge, attitude and behaviour scores. This overall ISA score was used to examine the relationship between individual difference variables and ISA.

3.1.1. *Demographics: age and gender*

An ANOVA with a Bonferroni post-hoc test suggested that ISA differed significantly across the age groups, F (4, 500) = 6.9, $p < 0.001$. Specifically, significant differences were found between the 18 to 29 age group ($M = 238.4$, $SD = 33.7$) when compared to those aged: 40 to 49 ($M = 254.7$, $SD = 32.0$) ($p = 0.010$, $d = 0.49$); 50 to 59 ($M = 259.9$, $SD = 31.7$); and, those over 60 years of age ($M = 260.8$, $SD = 26.8$), ($p < 0.001$, $d = 0.66$). Significant differences were also found between the 30 to 39 age group ($M = 247.4$, $SD = 33.5$) and participants in the following two categories: 50 to 59 ($p = 0.025$, $d = 0.38$); and, those over 60 years of age ($p = 0.037$, $d = 0.44$). Overall, it was observed that individuals within the older age brackets had higher ISA scores, compared to individuals in the younger age groups.

A partial correlation was used to test whether the relationship between age and ISA was influenced by risk-taking propensity. When controlling for risk-taking propensity, the correlation between age and ISA remained significant, (r = 0.18, $p < 0.001$), but was slightly lower compared with the correlation between age and ISA when risk-taking propensity was not controlled ($r = 0.22$, $p < 0.001$). This suggests that some of the shared variance between age and ISA is explained by risk-taking propensity.

An independent samples t-test was conducted to examine gender differences in ISA scores. Female participants ($M = 256.8$, $SD = 30.4$) had significantly higher ISA scores compared to male participants ($M = 248.0$, $SD = 34.6$), ($t = -3.0$, $p < 0.001$), although the effect was small, $d = 0.25$.

3.1.2. *Personality and risk-taking propensity*

As shown in Table 1, correlations between ISA and individual differences indicated significant positive relationships between conscientiousness and ISA ($r = 0.56$, $p < 0.001$), agreeableness and ISA ($r = 0.49$, $p < 0.001$), and openness and ISA ($r = 0.19$, $p < 0.001$). There was also a negative correlation between risk-taking propensity and ISA ($r =$ - 0.24, $p < 0.001$).

To further investigate the relationships between ISA and individual differences, we conducted a two-stage hierarchical multiple regression, and investigated which of the independent variables predicted ISA. Based on correlations, extroversion was not included in the regression, because the correlation between ISA and extraversion was not significant. As shown in Table 2, age and gender were entered at stage one of the regression to control for these variables, given the findings already discussed in section 3.1.1. The Big Five personality factors (excluding extroversion), and risk-taking propensity were entered at stage two of the regression.

At stage one, both age and gender were significant, accounting for 7% of the variance. At stage two, the demographic variables were no longer significant, and the addition of agreeableness, conscientiousness, emotional stability, openness and risk-taking propensity explained an additional 33.3% of the variance. The

Table 2
Summary of the hierarchical regression analysis for age, gender, agreeableness, conscientiousness, emotional stability, openness and risk-taking propensity predicting ISA (N = 505).

Variable	β	t
Step 1	$F_{(2,\ 502)} = 19.70$, $R^2 = 0.073^{**}$	
Age	0.24	5.46^{**}
Gender (Female = 2)	0.16	3.67^{**}
Step 2	$F_{(7,\ 497)} = 48.01$, $R^2 = 0.403^{**}$	
Age	0.07	1.95
Gender	0.05	1.47
Agreeableness	0.27	6.12^{**}
Conscientiousness	0.40	8.63^{**}
Emotional Stability	−0.09	-2.13^{*}
Openness	0.06	1.74
Risk-taking propensity	−0.17	-4.82^{**}

$^{*}p < 0.05$, $^{**}p < 0.001$.

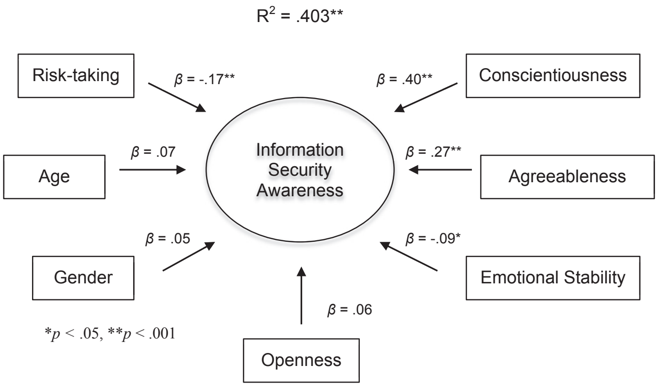

Fig. 2. Variance explained by the individual difference factors age, gender, conscientiousness, agreeableness, emotional stability, openness and risk-taking propensity.

total variance explained by the model was 40.3%, $F(7, 497) = 48.01$, $p < 0.001$, and conscientiousness was the most important contributor, overall, followed by agreeableness and risk-taking propensity. The final pictorial summary of the hierarchical regression is also represented in Fig. 2.

4. Discussion

4.1. Overview and contribution

This study aimed to examine the relationship between individual differences and ISA. ISA was measured using the HAIS-Q. This research has both theoretical and applied contributions. The main contribution has been the consideration of individual differences, including personality, in relation to ISA. From an applied perspective, this can assist organisations in identifying areas where improvement may be necessary, and this can facilitate the development of training programs. Training programs could then be individualised and presented in a manner that matches the individual's personality profile and learning style, in an attempt to maximise learning outcomes. From a theoretical perspective, such research provides an opportunity to empirically evaluate and understand individual differences in relation to ISA. While there is still considerable research to be conducted, this is an important contribution to the field of InfoSec.

The following sections will discuss the findings in relation to ISA and individual differences, the limitations of the study, and future directions will also be covered.

4.2. ISA and individual differences

4.2.1. Demographics: age and gender

Older adults had higher ISA scores when compared to younger adults. Furthermore, this relationship was fairly linear; as individuals got older, their ISA scores increased. This was also reported by Pattinson et al. (2015), who suggested that older adults were more risk averse, with regard to their InfoSec behaviours, than younger adults. Sheng et al. (2010) also found that individuals aged 18 to 35 were more susceptible to phishing emails, compared with older adults. Figner and colleagues (2009) suggested that risk-taking propensity also tends to decline from early adulthood. However, even when controlling for risk-taking propensity, the relationship between age and ISA remained significant.

In relation to gender, a small significant difference was found, with females obtaining higher ISA scores when compared to males. Significant, but small, gender differences were also found in a phishing study (Sheng et al., 2010). However, it was found that females were more susceptible to phishing emails than males. Further investigation of the potential effects of gender on ISA is required.

4.2.2. Personality and risk-taking propensity

Regression analyses were conducted to investigate the impact of personality, individual differences and risk-taking propensity on ISA. First, in relation to personality it was found that more conscientious, agreeable and open individuals, and individuals with a propensity to take fewer risks, had higher ISA scores. Furthermore, regression analyses revealed that conscientiousness, agreeableness, risk-taking propensity, and emotional stability significantly explained variance in ISA.

These findings partially align with previous research. Pattinson et al. (2015) evaluated the impact of personality and individual differences on self-reported InfoSec behaviour. They found that, conscientiousness, agreeableness, age, openness, and ability to control impulsivity explained variance in InfoSec behaviour. While age and openness were not found to be significant predictors in the current study, it is interesting to note that conscientiousness and agreeableness explained the most variance in both studies. This is further supported by Shropshire et al. (2015), who found that agreeableness was positively related to both intent to use, and actual use of security software. Cellar et al. (2001) found that individuals who had higher scores on conscientiousness and agreeableness were involved in fewer workplace accidents.

The results of the current study may be more robust compared to the Pattinson et al. (2015) study, as the current study used a more comprehensive measure of personality, and also examined risk-taking propensity.

4.3. Limitations

While this study makes important theoretical and applied contributions, a number of limitations should be noted. The data collection relied on self-report, often associated with biases, such as social desirability bias and boredom effects (Spector, 1992). Self-report is a subjective method of gathering data, and is therefore prone to measurement error. To help mitigate this, respondents were not asked to provide their name or the name of their employer, thereby assuring confidentiality and anonymity. These measures should have reduced the potential of socially desirable responses and other self-report biases (Donaldson & Grant-Vallone, 2002). Also, Spector (1994) argued that self-report as a data collection method should not be dismissed as being an inferior methodology, as it can provide valuable data.

The current study was not exhaustive with regard to its exploration of individual difference factors. Other variables, such as culture and security culture are also likely to explain variance in individuals' ISA. For example, Vroom and Von Solms (2004) suggested that culture would likely have a major impact on the security breaches experienced by organisations, and individuals’ behaviour. Factors such as education and InfoSec training could also have an impact on ISA; however, they have not been explored in this study. While this research focused on The Big Five personality factors these can be explored further by focusing on specific facets, explained in the following section.

4.4. Future directions

Building on the present study, future research could examine the relationship between ISA and individual differences in each of the seven focus areas. Vulnerability in even one of the seven focus areas renders an organisation susceptible to threats. Furthermore, given that conscientiousness and agreeableness explained the most variance in ISA, these variables warrant further investigation. Particular facets within conscientiousness and agreeableness could be considered in future research. For example, traits such as, “rule-following” and “orderliness”, which are components of conscientiousness, might impact on ISA.

Additionally, given the limited scope of this research, other individual variables might also be included. For example, an individual's confidence with computers, and the frequency with which they access the Internet might explain variance in their ISA. Age differences in ISA should also be further examined, given that there was a significant relationship between age and ISA, even when controlling for risk-taking propensity.

While intervention and organisational factors, such as training programs and the organisation's security culture were not within the scope of this study, it is likely that such factors play an important role in influencing individual security behaviours (Vroom & Von Solms, 2004). Future research might also consider the potential interplay between security culture and individual difference factors.

4.5. Conclusion

This study examined the relationship between individual differences and ISA. It was found that conscientiousness, agreeableness, emotional stability and risk-taking propensity significantly explained variance in individuals’ ISA. Our findings have important implications for organisations as they can assist in the identification of InfoSec strengths and weaknesses, and can facilitate the development of tailored InfoSec training for employees.

Acknowledgements

This research was funded through The Premier's Research Industry Fund (PRIF), which is an initiative of the South Australian government. This was won by the Business School at The University of Adelaide, with Defence Science and Technology Group as a collaborative partner. The Premier's Research Industry Fund had no involvement in the collection, analysis, interpretation of the data, or in writing the report. Part of the PRIF funds was used for payment to Qualtrics for data collection (grant no. CPP 41).

References

Australian Standard, ISO/IEC 27002. (2015). *Information technology - security techniques - code of practice for information security controls, (AS ISO/IEC 27002:2015)*. Standards Australia.

Baranowski, T., Cullen, K. W., Nicklas, T., Thompson, D., & Baranowski, J. (2003). Are current health behavioural change models helpful in guiding prevention of weight gain efforts. *Obesity Research, 11*(10), 23–43.

Benet-Martínez, V., & John, O. P. (1998). Los cinco grandes across cultures and ethnic groups: Multitrait–multimethod analyses of the Big five in spanish and english. *Journal of Personality and Social Psychology, 75*, 729–750.

Bettinghaus, E. (1986). Health promotion and the knowledge – attitude - behavior continuum. *Preventative Medicine, 15*(5), 475–491.

Cellar, D. F., Nelson, Z. C., Yorke, C. M., & Bauer, C. (2001). The five-factor model and safety in the workplace: Investigating the relationships between personality and accident involvement. *Journal of Prevention & Intervention in the community, 22*(1), 43–52.

Costa, P. T., & McCrae, R. R. (1992). *NEO PI-R professional manual*. Inc., Odessa, FL: Psychological Assessment Resources.

Donaldson, S. I., & Grant-Vallone, E. J. (2002). Understanding self-report bias in organizational behavior research. *Journal of Business and Psychology, 17*(2), 245–260.

Figner, B., Mackinlay, R. J., Wilkening, F., & Weber, E. U. (2009). Affective and deliberative processes in risky choice: Age differences in risk taking in the columbia card task. *Journal of Experimental Psychology: Learning, Memory, and Cognition, 35*(3), 709.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153–160.

Furnell, S., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end users. *Computers and Security, 25*(1), 27–35.

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

Heinström, J. (2003). Five personality dimensions and their influence on information behaviour. *Information research, 9*(1), 9–1.

John, O. P., & Srivastava, S. (1999). The Big Five trait taxonomy: History, measurement, and theoretical perspectives. *Handbook of personality: Theory and research, 2*(1999), 102–138.

Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems, 48*(4), 15–24.

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

Losoncz, I. (2009). *Personality traits in HILDA1. Australian Social Policy No. 8* (p. 169).

McCormac, A., Parsons, K., & Butavicius, M. (2012). *Preventing and profiling malicious insider attacks (No. DSTO-TR-2697)*. Defence Science and Technology Organisation Edinburgh (Australia) Command Control Communications and Intelligence Division.

McGuire, W. J. (1969). *The nature of attitudes and attitude change. The handbook of social psychology* (Vol. 3), 136–314.

Nicholson, N., Soane, E., Fenton-O'Creevy, M., & Willman, P. (2005). Personality and domain-specific risk taking. *Journal of Risk Research, 8*(2), 157–176.

Organ, D. W., & Paine, J. B. (1999). *A new kind of performance for industrial and organizational psychology: Recent contributions to the study of organizational citizenship behavior*.

Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing, 82*(4), 331–338.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). *Human factors and information security: Individual, culture and security environment (No. DSTO-TR-2484)*. Defence Science and Technology Organisation Edinburgh (Australia) Command Control Communications and Intelligence Division.

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.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security Behavior: An australian web-based study. In *Proceedings of human aspects of information security, privacy, and trust (LNCS pp. 231–241)*. Springer International Publishing.

Pricewaterhouse Coopers. (2015). *Key findings from the global state of information security survey 2016. Turnaround and transformation in cyber security*.

Schneier, B. (2000). *Secrets and Lies: Digital security in a networked world*. Indianapolis, IB: Wiley Publishing, Inc.

Schultz, E. (2005). The human factor in security. *Computers & Security, 24*(6), 425–426.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phishing? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 373–382). ACM.

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. *AMCIS 2006 Proceedings*, 415.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security, 49*, 177–191.

Spector, P. E. (1992). A consideration of the validity and meaning of self-report measures of job conditions. In C. L. Cooper, & I. T. Robertson (Eds.), *International review of industrial and organizational Psychology* (pp. 123–151). West Sussex, England: John Wiley.

Spector, P. E. (1994). Using self-report questionnaires in OB research: A comment of the use of a conversional method. *Journal of Organizational Behaviour, 15*(5), 385–392.

Stankov, L., Boyle, G. J., & Cattell, R. B. (1995). *Models and paradigms in personality and intelligence research. In International handbook of personality and intelligence*. Springer US.

Van der Linden, S. (2012, July). Understanding and achieving behavioural change: Towards a new model for communicating information about climate change. In *International workshop on psychological and behavioural approaches to understanding and governing sustainable tourism mobility*.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191–198.

Weber, E. U., & Milliman, R. A. (1997). Perceived risk attitudes: Relating risk perception to risky choice. *Management Science, 43*(2), 123–144.