A Cross-Cultural Investigation of Information Security Awareness (ISA)

[redacted]

This report is submitted in partial fulfilment

of the degree

of Master of Psychology (Organisational and Human Factors)

School of Psychology

University of Adelaide

October 2019

Literature Review Word Count: 4998

Research Report Word Count: 8287

Table of Contents

Declaration

This report contains no material which has been accepted for the award of any other degree or diploma in any University, and, to the best of my knowledge, this report contains no materials previously published except where due reference is made.

I give permission for the digital version of my thesis to be made available on the web, via the University's digital research repository, the Library Search and also through web search engines, unless permission has been granted by the School to restrict access for a period of time.

[redacted]

[redacted]

October 2019

Acknowledgements

To my supervisor [redacted] you generously shared your knowledge, support and time. I cannot thank you enough for your expertise, and more importantly, your professionalism and approachability. I am extremely grateful to have had you as my primary supervisor.

Thank you to [redacted] for your assistance as secondary supervisor. Your feedback was invaluable. Also, to [redacted] thank you for your support and feedback.

To [redacted] thank you for your continuous love, support and sympathetic ear. I could not have come so far without you.

List of Tables

List of Figures

Literature Review

Research Report

Literature Review

Word count: 4998

Abstract

The past decade of literature has seen a developing body of research focusing on the role of the employee and the associated individual differences that may influence information security in the workplace. While this research has evoked significant findings which identify a variety of factors that influence individual Information Security Awareness (ISA), the results associated with age and gender have been inconsistent (Hadlington, Popovac, Janicke, Yevseyeva, & Jones, 2018; McCormac et al., 2017). In addition, the rate of security breaches continue to rise, with the behaviours of employees identified as a source of ninety-five percent of security incidents (IMB Global Technology Services, 2014). This highlights the need for a greater focus and understanding on human aspects of information security, particularly concerning national culture, which has been very limited in focus within past research. The challenges to determine the factors contributing to information security prove to be complex. Information security awareness is now attracting more attention from industry, as stakeholders are held accountable for the information with which they work (Kritzinger & Smith, 2009). This review will provide an initial assessment of the literature on ISA, individual differences, and national culture. Industry sector will also be considered.

Keywords: Information Security Awareness (ISA), national culture, Uncertainty avoidant, Long-term orientation, individual differences.

Introduction

A company's reliance on digital information and technology systems is vital for work productivity. However, while organisations expand their use of advanced technologies, insufficient attention is being attributed to the role of human factors in information security awareness (ISA). Information security compromised by employees can pose an enormous threat to an organisation. As a result, experts have stated that the employee is the 'weakest link' in the protection of an organisation's information security system (Dols & Silvius, 2010). Indeed, in a recent report on cyber investigation of breaches it was cited that ninety-five per cent of security incidents were the result of human error, as stated in a recent report on cyber investigation of breaches (IMB Global Technology Services, 2014). Therefore, despite the threats from malicious in-and outsiders, factors such as negligence, carelessness, and naivety amongst employees may pose the greatest security threat to a company (Dols & Silvius, 2010; Parsons et al., 2017). Technology alone cannot sufficiently protect the security of an organisation; thus the human aspect should not be isolated from technology. Safeguarding an organisation's sensitive information requires a complete awareness of the impact of the employee. However, previous research has tended to focus on single areas of interest; for example personality (McCormac et al., 2017). This represents a partial view and is unable to provide a comprehensive representation of an individual's or organisation's ISA.

As the focus of information security measures shifts from technology to human factors, many researchers have investigated the influence of some organisational factors such as information security policy and training (Glaspie & Karwowski, 2018). Parsons, McCormac, Butavicius, Pattinson, and Jerram (2014) state that employee's security related behaviours are influenced by such organisational factors. They concluded that increased knowledge of policy and procedure is highly correlated with a positive attitude towards the organisation's policy and procedure. Researchers have extended this theme with findings that

show that the sharing of information security knowledge, security collaboration and mediation between the organisation and its employees greatly effects compliance. Furthermore, organisations where employees receive training generally adhere to and exhibit a more positive information security culture (Da Veiga & Martins, 2015; Safa et al., 2015). While these findings are extremely useful, much of this research has not included a focus on industry sectors. It is warranted that industry sector, and the nature of work that is encompassed by an industry, would have an influence on ISA as it has been shown that the average level of ISA for bank employees is approximately twenty per cent higher in comparison to the general workforce in Australia (Pattinson et al., 2016). However, a comprehensive comparison of industry sectors and ISA has yet to be explored.

It has been postulated that culture would also have a significant influence on the security breaches experienced by organisations, and individuals' behaviours (Vroom & Von Solms, 2004). Essentially, it is argued that cultural differences may manifest themselves in varied levels of security awareness (Crosslet et al., 2013; Kruger, Drevin, Flowerday & Steyn, 2011; Vroom & Von Solms, 2004). Crosslet et al. (2013) state that national culture, in particular, is likely to have a direct impact on various elements of information security, and they argue for future studies to account for this cross-cultural difference. First proposed by Hofstede (2001), national culture is a concept based on value orientations which are considered important and shared across different countries in which organisations exist. This six-dimension framework represents independent preferences for one state of affairs over another that distinguish countries (rather than individuals) from each other. Human behaviour is largely determined by cultural aspects, and the workplace is no exception; workplace interactions and learning are grounded in a prevalent national culture (Cronk & Salmon, 2017; Kruger et al., 2011). Because of this, the complete management of information security can be ensured only if the behavioural aspects of national culture are also understood.

Given the influence of national culture on employee behaviours and the importance of human factors in information security, this literature review will examine ISA, national culture and individual differences. An exploration into the influence of industry sector will also be included. These constructs have not previously been explored together.

Information Security Awareness

In 2017 and 2018 more than sixty-five percent of Australian organisations were victims of cyber-crime, with one in 10 experiencing losses greater than one million dollars, and nine percent reporting having had the confidentiality, integrity, or availability of sensitive data compromised (PwC, 2018). These results also revealed that employee training on privacy policy and security practices was required for only half of the respondents (PwC, 2018). Understanding ISA and its contributing factors is crucial in alleviating information security attacks such as those reported above.

ISA refers to the degree to which employees understand the importance and implications of their organisation's information security policies, rules and guidelines, and the degree to which they behave in accordance with such policies (Bulgurca, Cavusoglu & Benbasat, 2010; Kruger & Kearney, 2006). Thus, ISA has two essential components; (1) the level of *understanding* an individual has for information security policies and, (2) the extent to which the individual is committed to and *behaves* in a way that meets the requirements of information security policies (Kruger & Kearney, 2006; Hadlington et al., 2018). Technical measures alone are inadequate to protect the security of an organisation's information, and researchers have instead suggested that focusing on the employee's ISA is of higher priority (Parsons, McCormac, Butavicius, Pattinson & Jeram, 2014; Parsons, McCormac, Butavicius, & Ferguson, 2010). Employees' information security behaviours are influenced by several factors, including attitude towards risks and vulnerabilities, knowledge of the organisation's

policy, and training in the proper use of countermeasures (Aytes & Conolly, 2003). ISA has a particular focus on the role of the human, who is often discussed as being the "first line of defence" against information security threats (Von Solms & Van Niekerk, 2013, p.12).

Theories and frameworks.

Several existing behavioural models have been applied to ISA research to understand and explain employee's information security behaviours. The Knowledge-Attitude-Behaviour (KAB) model has become prevalent as a basis for assessing ISA. This model encompasses three components: knowledge (what does the person know), attitude (how do they feel about the topic), and behaviour (what do they do; Kruger & Kearney, 2006; Siponen, 2000). The KAB model purports that, as an employee's knowledge of security behaviours increases, his/her attitude improves, resulting in improved information security related behaviours (Kruger & Kearney, 2006; Parsons et al., 2014).

In the past, the KAB model has been criticised by some researchers (Bulkeley, 2000; Moser, 2006). However, others have argued that the problem is not with the model itself, but with the way in which it has previously been applied (Kaiser & Fuhrer, 2003; McGuire, 1969; Van der Linden, 2012). Parsons and colleagues (2014) also considered this and propose that previous studies using the KAB model often neglect to clearly conceptualise the knowledge component. Parsons and colleagues (2014, p. 167) state that *"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".* Evidence of the validity of the KAB model is now well established, and its use is highly supported (Hadlington et al., 2018; McCormac et al., 2016; McCormac et al., 2017; Parsons et al., 2017; Van der Linden, 2012).

Measurement and Methods

Within the body of literature, there have been few attempts to measure ISA holistically as a complete construct. Much of the previous research represents single focus areas (e.g., password related behaviours), and, as a result, does not encompass a complete understanding of ISA (Stanton, Stam, Mastrangelo, & Jolton, 2005). While behavioural models such as the Theory of Planned Behaviour (Bulgurcu, Cavusoglu, & Benbasat, 2010), General Deterrence Theory (D'Arcy, Hovav, & Galletta, 2009; Fan & Zhang, 2011), Protection Motivation Theory (Vance, 2010), and the Health Belief Model (Ng, Kankanhalli, & Xu, 2009) have been used to understand aspects of ISA, each theory is characterised by a specific focus of particular variables. Again, this provides researchers with a limited representation of ISA as this approach omits additional significant variables.

More recently, research has aimed to create a measure of ISA. The User's Information Security Awareness Questionnaire (UISAQ), for example, measures risk behaviour, level of ISA, beliefs about information security and the quality and security of passwords (Solic, Velki, & Galba, 2015). Researchers such as Egelman and Peer (2015) and Öğütçü, Testik and Chouseinoglou (2016) have also begun to create individual measures of ISA which have demonstrated promising results; however, these more holistic attempts to measure ISA are at the early stages of development. Further validity and reliability testing is necessary before such measures can be confidently used (Parsons et al., 2017).

The Human Aspects of Information Security Questionnaire (HAIS-Q) developed by Parsons and colleagues (2014) is a useful tool to measure individuals' ISA. In line with the KAB model, this measure proposes that as an employee's information security knowledge increases, his/her attitude will improve, resulting in improved information security behaviours (Kruger & Kearney, 2006; Parsons et al., 2014). The HAIS-Q has been developed through a review of information security policies and standards, as well as via consultation with managers and information technology professionals (Parsons et al., 2014). Through this

process, Parsons and colleagues (2014) identified seven focus areas for their measure (see Figure 1). Each focus area comprises three specific sub-areas, each accompanied by a knowledge, attitude, and behaviour statement. For example, within the focus area 'Social media use', the sub-area 'posting about work' includes the following knowledge, attitude and behaviour statements are as follows:

Knowledge: *"I can post what I want about work on social media"*

Attitude: *"It's risky to post certain information about my work on social media"*

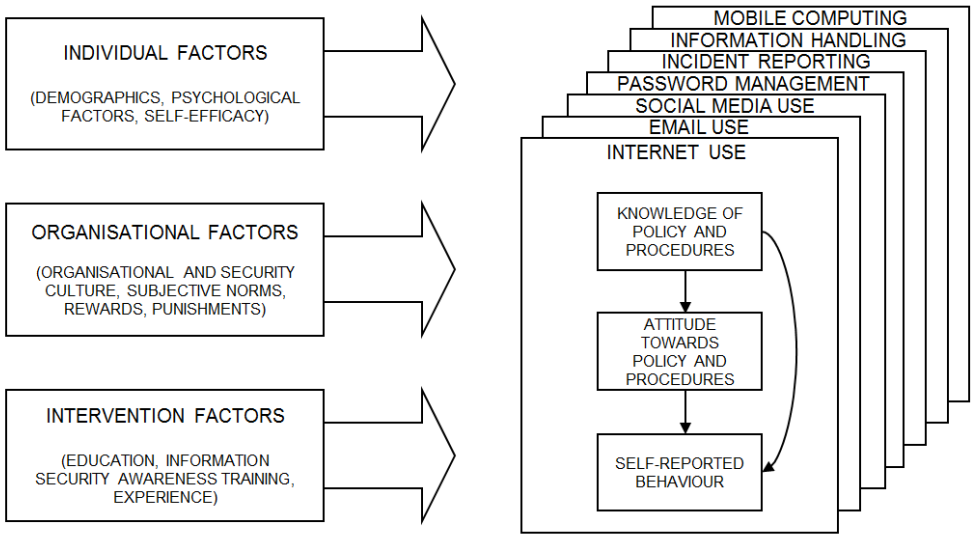
Behaviour: *"I post whatever I want about work on social media"*

Parsons and colleagues (2014) have made an effort to clearly conceptualise knowledge, ensuring that the knowledge, attitude and behaviour statements within the HAIS-Q sub-areas are specific and aligned. In contrast to other similar measures such as the UISAQ, the HAIS-Q has undergone thorough reliability and validity testing; however it is important to note that to date this has primarily focused on the Australian context (Hadlington & Parsons, 2017; McCormac et al., 2016, 2017b; Parsons et al., 2017).

Parsons and colleagues (2014) state that there are likely to be a number of factors which influence the relationship between knowledge, attitude and behaviour towards ISA. Their research has explored a number of factors including intervention, individual and organisational factors. However, within their model, the importance of national culture has not been considered (see Figure 1). With the growing number of multinational companies, investigating the effects of national culture is pivotal. Policies and procedures that are established in one country may not fluently apply to the employees in another country.

Consequently, research is required to investigate whether the HAIS-Q is cross-culturally suitable.

Figure 1: The Human Aspects of Information Security Model (adapted from Parsons et al., 2014)



Individual Differences

The information security literature has seen a developing body of research focusing primarily on the role of the employee and the associated individual differences that may influence information security in the workplace. This research is extremely important as considering the influence of individual differences, particularly the variability between individuals, is crucial to understand the psychological factors which influence ISA.

Previous research.

Preliminary research, such as that conducted by Shropshire, Warkentin and Sharma (2015) and Pattinson, Butavicius, Parsons, McCormac, & Calic, (2015), has provided significant direction for ISA studies investigating individual differences. Shropshire and colleagues (2015) conducted a study in which they surveyed college students' personality and self-reported intention to adopt a web-based security software program known as 'Perimeter Check'. This study objectively recorded when students logged onto the program, in order to

assess their actual use of the software (Shropshire et al., 2015). The results demonstrated that high agreeableness was positively related to both intent to adopt and actual use of the security software. The researchers suggested that individuals high in agreeableness traits might be more concerned about what others think of them, and are therefore more likely to be concerned with security issues in general (Shropshire et al., 2015). Nevertheless, the student sample represents a limitation of this study, as most participants were males aged between 18 and 21, which means the effect of these individual difference variables could not be examined.

Pattinson and colleagues (2015) examined non-malicious computer-based behaviour and individual factors, including employee's age, education level, familiarity with computers and personality. Results found that those employees who are more agreeable, less impulsive, more open, and less familiar with computers were likely to have less risky accidental-naïve behaviour (Pattinson et al., 2015). This study did not investigate the potential differences between males and females and information security behaviour; however, results identified a significant positive relationship between age and information security behaviours, indicating that older adults reported more correct information security behaviours than younger adults. This study utilised the Ten-Item Personality Inventory, which was considered a limitation by the authors as a more robust and extensive measure of personality would have been preferable (Pattinson et al., 2015). Additionally, self-reported behaviour was the only component of ISA that was measured in this study, highlighting another weakness of this research.

To address the limitations of previous research, McCormac and colleagues (2017) examined the relationship between individuals' ISA and individual difference variables, such as age, gender, personality, and risk-taking propensity. This research utilised the 'Big Five Model' to measure personality, which is considered to be the leading theoretical model for

measuring and understanding personality (Shropshire, Warkentin, Johnston, & Schmidt, 2006). Additionally, the HAIS-Q which is also a highly supported measure, was used to capture ISA. This research found that conscientiousness, agreeableness, emotional stability and risk-taking propensity significantly explained variance in individuals' ISA, while age and gender did not (McCormac et al., 2017).

Research conducted by Hadlington and colleagues (2018) also examined the relationship between individual differences and adherence to ISA. This research aimed to extend previous findings by exploring three individual variables directly related to the individuals' perceived control within the workplace, their commitment to current work identity, and the extent to which they are reconsidering committing to work (Hadlington et al., 2018). The results revealed that work locus of control acted as a significant predictor for total scores on the HAIS-Q measure of ISA. Thus, ISA was weaker in those individuals who demonstrated more externality. In line with previous research, a difference between genders was also examined. Their analysis identified a significant difference between males and females in relation to scores on the HAIS-Q. Females were observed to score consistently higher than males in terms of ISA; however, it is noted that the effect size is very small. The effect of age was not accounted for in this study.

Previous research has identified certain individual factors that may affect ISA. However, most indicative has been the inconsistent pattern of results relative to age and gender, and thus, further research is required to investigate the relationship between gender, age and ISA.

Industry Sector

The growth in multinational companies and the wide range of activities now required to plan, control and distribute a product, has undoubtedly altered the competences of

organisations (Banker, Bardhan, Chang, & Lin, 2006). Because of this, researchers have argued that the information value of industries, in particular, trade services in the financial market, typically require capabilities designed to incorporate information security considerations (Davamanirajan, Kauffman, Kriebel, & Mukhopadhyay, 2006). Jung and Lee (2001), found that the threats associated with Internet use varied among industries according to the needs of the organisation for information availability, confidentiality, and integrity. Thus, information security becomes particularly crucial for heavily information-sensitive industries (Yeh & Chang, 2007). The requirements for information security policy evidently varies across industries. Organisations with different information technology architectures differ in their computing needs, network, client-server settings, and subsequently the level of ISA required (Yeh & Chang, 2007).

Previous research.

Researchers investigating ISA have offered many solutions to manage and prevent information security threats, such as relevant training for employees (Glaspie & Karwowski, 2018; Parsons et al., 2014). However, previous studies have infrequently considered how organisational characteristics influence security practices; in particular, little attention is given to industrial influences. Because of this, security threat mitigation strategies rarely consider the differences between industries.

Some researchers have attempted to address this gap in the information security literature, however it is clear that further investigation is necessary. For example, a cross-industry study conducted by Yeh and Chang (2007) investigated managers' perceptions of security threats and explored the differences in the scope of countermeasures adopted across industries. This study included data from 109 Taiwanese firms which mirrored four industry types: 'general manufacturing', 'high-tech industry', 'banking/financial', and

'retailing/service'. The researchers also examined the impact of several variables, and they found that industry type and information technology use (i.e., computerisation level) in particular affected the motivation of firms to adopt security countermeasures. Although the researchers found no statistically significant differences among the countermeasures adopted by the four industry types, the banking/finance and retailing/service industries appeared heavily reliant on information technology, with 38 and 54 per cent of firms falling into the high-level computerisation category. Regarding overall security, the banking/finance industry was most secure. The research model adopted in this study was parsimonious, the authors stating that the comparisons between industries were "relative, rather than absolute", due to a lack of validated measures and the medium to large size of most firms included (Yeh & Chang, 2007, p. 486). Nevertheless, this research highlights the important notion that information security is not simply a technical issue but rather a context-dependent industry concern which should consider the effects of human error as well as industry requirements for developing and implementing an ISA learning platform and/or training.

A more recent attempt to explore industry and ISA is accredited to Pattinson and colleagues (2016). Their research aimed to assess the ISA of employees of an Australian bank using the HAIS-Q and to compare these results with the general workforce in Australia. Pattinson and colleagues predicted that the ISA of the bank employees should be higher than for the general workforce due to the typical characteristics defined by the job role within the finance/banking industry. This includes exposure to more sensitive and confidential information. The results show that the ISA percentage scores for bank employees were twenty percent higher than those for the general workforce. This result was consistent across all information security focus areas (as measured by the HAIS-Q) as well as for the overall ISA percentage scores. Furthermore, consistent with the researcher's predictions, the bank employees recorded their highest ISA scores for the Information Handling focus area (i.e.,

management of sensitive and confidential information). This study provides an indication that industry type, and the associated job roles, has an influence on employee ISA. This research is the first to utilise the HAIS-Q to explore such a phenomenon and justifies further investigation into the effect of industry on ISA.

National Culture

A more holistic approach to information security management comprising technological, organisational and psychosocial components has become necessary due to the number of ways information can now become compromised within organisations. While approaches which focus on the human factor have increased the understanding of information system misuse on an end-user level (i.e., individual differences), they have rarely investigated the effect of national culture. Noteworthy, it is suspected that national culture has a direct link with the human factor due to the value orientations individuals may or may not embody. Thus, acting as a moderating variable, national culture may have an effect on the relationships discovered in previous research by making them stronger, weaker or nonsignificant (Flores, Antonsen, & Ekstedt, 2014). As national culture likely has a direct impact on various elements of information security, Crossler et al. (2013) state that such effects need to be considered, and that research that is adapted to account for national differences is therefore essential. However, to date, the role of national culture in information security contexts has received limited consideration.

Theories and frameworks.

The views of culture represented by Hofstede's (1993; 2001) description of national cultures are adopted as a cultural framework in recent information security research. Hofstede (1993, p. 82) defines culture as *"the collective programming of the mind that distinguishes one group or category of people from another".* This framework is based on the following six

distinct dimensions: Power distance, Individualism versus collectivism, Masculinity versus femininity, Uncertainty avoidance, Long-term versus short-term orientation, and Indulgence versus restraint.

Power distance refers to the degree of adherence to formal authority, more specifically, how a society accepts a hierarchical order and/or managers differences among people (Hofstede, 2001; Hofstede Insights, 2019). *Individualism versus collectivism* focuses on the behaviour regulation of an individual's relationships with others. In an individualistic society, individuals are expected to take care of only themselves and their immediate families. In contrast, in a collectivist society, individuals consider it more important to look after the interest of their group before themselves (i.e., an "I" versus "We" mentality; Dinev, Goo, Hu, & Nam, 2009). *Masculinity versus femininity* measures the extent to which a society represents a preference for achievement, assertiveness, heroism, and material rewards for success in contrast to cooperation, modesty, caring for the weak and quality of life (Hofstede Insights, 2019). *Uncertainty avoidance* measures the degree to which a society feels uncomfortable with uncertainty and ambiguity in the environment. *Long-term versus short-term orientation* is related to the Confucian values of Eastern societies. Societies that score high on long-term orientation tend to place a great significance on thrift, persistence and long-term alliances, whereas low scoring societies prefer to maintain time-honoured traditions and norms and view social change with suspicion (Dinev et al., 2009). Finally, *Indulgence versus restraint* measures the degree to which a society allows for free gratification of basic and natural human drives related to enjoying life and having fun, in contrast to being regulated by strict social norms. These dimensions represent independent preferences for one state of affairs over another which distinguishes countries (rather than individuals) from each other (Hofstede Insights, 2019).

Hofstede's framework has been criticised as its relevance to IT research has been questioned. Some researchers prefer alternative frameworks such as Schwartz's (1994) or Fukuyama's (1995) theory of trust and social capital. However, it has been argued that alternative frameworks have merely achieved a refinement of Hofstede's work, rather than a contradiction (Miller, Batenburg, & Wijngaert, 2006). Hofstede's six-dimensional framework is based on value orientations considered important and shared across cultures. Hofstede's indicators are a stable and slowly changing representation of culture and transcend generations (Dinev et al., 2009). Thus, this framework remains the predominant foundation of cross-cultural studies and has now been employed and validated in information security research (Johnston & Hale, 2009; House, Hangs, Javidan, Dorfman, & Gupta, 2004; Myers & Tan, 2002; Robey & Rodrigues-Diaz, 1989).

Previous Research: National Culture, Information Security and ISA

Although some research has investigated the relationship between information security and national culture, no research has yet explored the influence of national culture on ISA.

Björck and Jiang (2006) made the first attempt to investigate the relationship between the security of IT and business and national culture in their study *"Information Security and National Culture".* The purpose of this study was to identify and explore the potential linkages between information security and national cultures by comparing Singaporean and Swedish companies against Hofstede's cultural framework. It was found that more discrepancies in IT security implementation were identified whenever distinctive national cultural differences existed (Björck & Jiang, 2006). Singapore and Sweden have large differences on two of Hofstede's dimensions (i.e., Power distance, and Individualism vs.

collectivism) and smaller differences in Uncertainty Avoidance and Masculinity vs. Femininity.

Björck and Jiang (2006) noted differences in several security practices, such as how companies controlled security risks and managed information breaches, which they attributed to the differences in Power distance and Individualism vs. Collectivism. No major differences were discovered along dimensions which share a smaller difference. Due to the explorative nature of this study, an inductive methodology was used to uncover knowledge and insights based on the different patterns related to national culture. While this provided a first perspective into information security and the effect of national culture, the exploratory nature of this study means that further research is required. Furthermore, Hofstede's cultural framework has evolved to include six cultural dimensions, whereas this study only investigated the impact of four previous dimensions.

Dinev and colleagues (2009) investigated user behaviour in relation to protective information technologies by empirically testing a behavioural model using data collected from respondents in the USA and South Korea. The five national culture indices that existed at the time were included as moderating variables. Three out of five of the proposed relationships in the model were moderated by national culture (Dinev et al., 2009). Notably, while the relationship between subjective norm and behavioural intention for South Korean users was statistically significant and strong, the relationship for US users was statistically nonsignificant. It was argued that this difference between the two cultures was a cumulative result of Individualism, Masculinity, Power distance and Uncertainty avoidance but required further attention (Dinev et al., 2009). Nevertheless, this study is one of very few in the information security domain that has considered potential national culture effects and demonstrated significant differences. This research highlighted the importance of national culture as significant relationship moderators within the information security literature and

defined the role of organisational factors (in contrast to individual factors) in the formation of user attitude and behaviour towards using protective information technology (Dinev et al., 2009).

Further literature exploring the influence of national culture on non-compliance behaviour has linked national culture and risk taking behaviour, which is defined as being deliberate or not, by insiders or employees who ignore an organisation's security policies and guidelines (Dols & Silvius, 2010). Based on a survey study amongst employees of a big-five accountancy firm in the Netherlands and Belgium, the influence of national culture was shown. Four out of ten non-compliance behaviour statements in the survey showed a significant difference between the two countries and their national culture preferences (Dols & Silvius, 2010). The Netherlands, which orients a low Power distance and Uncertainty avoidance score, demonstrated a willingness to *"bend the rules"* or to disobey orders from their superior (Dols & Silvius, 2010, p.20). However, limiting factors of this study include a small sample size, thus the significance of the outcomes should therefore be viewed with caution. Additionally, this research investigated IT security as a whole, which is a vast area to explore and test, and therefore the conclusions drawn from the outcomes represent a general perspective.

Some research has investigated the effect of behavioural information security governance and national culture. Specifically, a mixed methods study conducted by Flores and colleagues (2014) examined the behavioural information security governance factors that drive information security knowledge in organisations, with a particular focus on national culture. Data was collected from organisations located in different geographical regions of the world, and the amount of data collected from the USA and Sweden, in particular, allowed for an investigation based on national culture. Similar to the findings shown by Dinev et al. (2009), this research found that national culture had a significant moderating effect on the

associations between four of the six proposed relations (Flores et al., 2014). In Sweden (a less individualistic, more feminine country), managers were more likely to implement controls that are aligned with business activities and employee's needs, monitor the effectiveness of such implemented controls and assure that they are not too obtrusive to the employee (Flores et al., 2014). In contrast, US organisations use formal arrangements and structures to establish security knowledge sharing (Flores et al., 2014). Consistent with previous research, the results of this study further reinforce the moderating effects national culture can have and thus highlights the importance of investigating such associations within the ISA literature.

Kruger and colleagues (2011) made the first attempt to investigate the role of cultural factors in ISA, rather than information security as a broader concept. This was achieved by administering an information security vocabulary test to assess the level of awareness amongst students form two different regional universities in South Africa. A security awareness questionnaire, based on a respondent's vocabulary knowledge and associated behaviour was used to assess the information and communication technology (ICT) security awareness level of participants (Kruger at al., 2011). Certain biographical questions were included in the questionnaire, such as mother tongue, to capture the role of cultural factors in ISA. The results highlighted that cultural factors, such as mother tongue and location of secondary schooling (rural or urban), played an important role in the security awareness levels of students (Kruger et al., 2011). Significant differences in the knowledge of security concepts amongst the various language groups and the associated behaviours were therefore identified. This paper is the first to investigate the impact of cultural factors on ISA, by extending the traditional approach to an ISA program. While national culture per se was not included, the findings suggest that cultural factors in general influence ISA. As this was an exploratory study, further research is required.

Discussion

In this review, a detailed overview of Information Security Awareness, individual differences relative to personality, age, gender, and familiarity with computers, as well as the literature on the relationship between information security, ISA, industry sector, and national culture has been provided. In the following section, the theoretical and applied implications of this review will be discussed and a way forward for research will be proposed.

Implications.

Robbins (2001) argues that there is a relationship between national culture and employee behaviours and that considering national culture is vital to accurately predict employee behaviours in an organisation. In this view, if an organisation wants its employees to develop effective ISA, it should not be developed in isolation of national culture. This is because, a work system that is effective in one culture does not necessarily guarantee its effectiveness in other cultures (Hofstede & Bond, 1988). While the relationship between information security and national culture has received some theoretical support, a study is yet to empirically explore ISA and national culture.

Research in this domain has revealed the effect of national culture within the information security context and has begun to consider the effects relative to ISA. Further research investigating ISA and national culture is warranted. Addressing this gap in the literature can provide more detailed information about the potential risk factors employees and their organisations present and may help to explain some of the variance identified in previous studies, which have not considered national culture. This research may serve critical importance by aiding the design of effective interventions and/or training programs which may prove to be especially useful within our global economy of organisations where national cultures exist and can vary (Flores et al., 2014).

Theoretically, this review provides a summary of the problem space, highlights the lack of focused research pertinent to ISA and can therefore act as a guide for further theoretical developments and empirical research in this area. This review also provides a summary of a valid and reliable instrument (the HAIS-Q) that organisations can administer to assess their employees' levels of ISA. However, to date, the majority of research conducted using the HAIS-Q has focused on Australian employees, with a smaller focus on employees from the United Kingdom. In addition, the HAIS-Q has yet to be compared across national cultures, which means it is difficult to determine the extent to which ISA varies across nations or cultures, or whether the HAIS-Q can be applied globally (Parsons et al.,2017).

Limitations and Future Research Directions

Most of the information security research that has considered national culture as an important variable has utilised different behavioural models and/or measurement tools. This research has also relied heavily on self-report methodologies such as quantitative questionnaires and qualitative interviews. Although self-report is prone to common method variance and social desirability, it enables systemisation, repeatability, comparability and convenience (Tucker, McCoy & Evans, 1990). Therefore, using a valid and reliable self-report measure, such as the HAIS-Q, is recommended. To test for the effects of national culture, a comparative approach to this body of literature is necessary by testing the HAIS-Q with data collected from different countries. In doing so, researchers will also examine whether the HAIS-Q is cross-culturally suitable. Additionally, to reduce the effects of biases and enable generalisability of results, it is also recommended that sufficient sample sizes are utilised.

This literature review has identified three main concerns; (1) individual differences, in particular, the results relative to age and gender have exposed inconsistencies, and there is a

clear gap in the literature in regards to the relationship between ISA and (2) national culture and (3) industry sector. An empirical examination of these factors is necessary. Preliminary research within the information security domain has begun to highlight national culture as an influential variable, but this requires further study, especially concerning ISA.

References

Aytes, K., & Connolly, T. (2003). A research model for investigating human behavior related to computer security. *AMCIS 2003 Proceedings*, 260, 45-60.

Banker, R.D., Bardhan, I.R., Change, H., & Lin, S. (2006). Plant information systems, manufacturing capabilities, and plant performance. *MIS Quarterly, 30,* 315-337.

Björck, J., & Jiang, K.W.B (2006). *Information security and national culture: comparison between ERP systems security implementations in Singapore and Sweden,* (Unpublished Master's Thesis). Royal Institute of Technology, Stockholm.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548.

Cronk, L., & Salmon, C. (2017). Culture's influence on behaviour: Steps towards a theory. *Evolutionary Behavioural Science, 11,* 36-52.

Crossler, R., Johnstron, A.,Lowrr, P., Hu, Q., Warkentin, M., & Baskervill, R. (2013). Future directions for behavioural information security research. *Computers & Security, 32,* 90-101. doi:10.1016/j.cose.2012.09.010

Davamanirajan, P., Kauffman, R.J., Kriebel, C.H., & Mukhopadhyay, T. (2006). Systems design, process performance, and economic outcomes in international banking. *Journal of Management Information Systems, 23,* 65-90. doi:10.2753/MIS0742-1222230204

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research, 20,* 79-98. doi:10.1287/isre/1070.0160

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal, 19,* 391-412. doi:10.1111/j.1365-2575.2007. 00289.x

Dols, T., & Silvius A. J. (2010). Exploring the influence of national cultures on non-Compliance behaviour. *Communications of the IIMA, 10,* 11-26. doi:10.1108/1361202111222806

Fan, J., & Zhang, P. (2011). Study on e-government information misuse based on General Deterrence Theory. In Proceedings of the *Service Systems and Service Management (ICSSSM), 2011 8th International Conference,* (pp.1-6). Tianjin: China

Flores, W., Antonsen, E., & Ekstedt, M. (2014). Inforamtion security knowledge sharing in organisations: investigating the effect of behavioural information security governance and national culture. *Computers and Security, 43,* 90-110. doi: 10.1016/j.cose.2014.03.004

Fukuyama, F. (1995). *Trust: The Social Virtues and the Creation of Prosperity*. Free Press, New York.

Hadlington, L., & Parsons, K. (2017). Can Cyberloafing and Internet Addiction Affect Organizational Information Security? *Cyberpsychology, Behavior and Social Networking, 20*(9), 567-571. doi: 10.1089/cyber.2017.0239

Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I., & Jones, K (2018). Exploring the role of work identity and work locus of control in information security awareness. *Psychology and Technology, 81,* 41-48. doi:10.1016/j.cose.2018.10.006

Hofstede, G., & Bond, M. (1988). The Confucius connection: from cultural roots to economic growth. *Organisational Dynamics, 16,* 4-21. doi:10.1016/0090-2616(88)90009-5

Hofstede, G. (1993). Cultural constraints in management theories. *Academy of Management Executive, 7,* 81-94. doi:10.5465/ame.1993.9409142061

Hofstede, G. (2001). *Culture's Consequences: Comparing Values, Behaviours, Institutions and Organisations across Nations,* 2nd edn. Sage Publications, Thousand Oaks, CA, USA.

Hofstede Insights. 2019. Country Comparisons. Retrieved from https://www.hofstede-insights.com/country-comparison/australia,the-uk/

House, R. J., Hangs, P.J., Javidan, M., Dorfman, P.W., & Gupta, V. (2004). *Culture, Leadership and Organisations: The GLOBE Study of 62 Societies Sage, Thousand Oaks, CA, 2004.*

International Business Machines Corporation [IMB] Global Technology Service. (2014). *IMB Security Services 2014 cyber security intelligence index: Analysis of cyber-attack and incident data from IMB's worldwide security operations.* Retrieved from ibm.com/developerworks/library/se-cyberindex2014/index.html

Johnston, A.C., & Hale, R. (2009). Effective security through information security governance. *Communications of the ACM, 52,* 126-129.

Jung, B., & Lee, H.S. (2001). Security threats to Internet: a Korean multi-industry investigation. *Information and Management, 38,* 487-498. doi:10.1016/S0378-7206(01)00071-4

Kaiser, F. G., & Fuhrer, U. (2003). Ecological behavio's dependency on different forms of knowledge. *Applied Psychology: An International Review, 52*, 598-613. doi: 10..1111/1464-0597.00153

Kruger, H. A, Drevin, L., Flowerday, S., & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. *Information Security for South Africa, 10,* 1-7. doi:10.1109/ISSA.2011.6027505

Kruger, H., & Kearney, W. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296. doi: 10.1016/j.cose.2006.02.008

McCorman, 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. doi:10.1016/j.chb.2016.11.065

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T, & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems, 21*, 1-11. doi:10.3127/ajis.v2i0.1697

McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M. & Pattinson, M. (2016). Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q). *Paper presented at the Australian Conference of Information Systems (ACIS).* Wollongong, Australia.

McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lillie, M. (2018). The effect of resilience and job stress on information security awareness. *Information and Computer Security, 26*, 277-289. doi:10.1108/ICS-30-2018-0032

McGuire, W. (1969). The nature of attitudes and attitude change. *The handbook of social psychology*, *3*(2), 136-314.

Miller, S., Batenburg, R. S., & van de Wijngaert, L. (2006). National culture influences on European ERP adoption. In J. Ljungberg & M. Andersson (Eds.), *14th European conference on information systems* (pp.1-12). Goteborg University, Chalmers University.

Myers, M. D., & Tan, F. B. (2002). Beyond models of national culture in information systems research. *Journal of Global Information Management, 10,* 24-32. doi:10.4018/jgim.2002010103

Ng, B-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behaviour: a health belief perspective. *Decis Support Syst, 48, 25-* 815. doi:10.1016/j.dss.2008.11.010

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. doi: 10.1016/j.cise.2013.12.003

Parsons, K., Caoc, D., Pattinson, M., Butavicious, M., McCormac, A., & Zwanns, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security, 66,* 40-51. doi: 10.1016/j.cose.2017.01.004

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.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2016). The information security awareness of bank employees. In *Proceedings of the Tenth*

International Symposium on Human Aspects of Information Security & Assurance (pp. 189-198). HAISA

Pricewaterhouse Coopers. (2018). *Key findings from the Global State of Information Security Survey 2018. Revitalizing privacy and trust in a data-driven world.* Retrieved from pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/revitalizing-privacy-trust-in-data-driven-world.html

Robey, D., & Rodriguez-Diaz, A. (1989). The organizational and cultural context of systems implementation: Case experience from Latin America. *Information & Management, 17,* 229-239. doi:10.1186/s13012-015-0325-y

Robbins, S. (2001). *Organizational behavior*. Upper Saddle River, New Jersey: Prentice Hall.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., & Herawan, T. (2015). Information security conscious care behaviour formation in organisations. *Computers and Security, 53,* 65-78. doi:10.1016/j.istr.2008.10.006

Schwartz, S.H. (1994). "Beyond Individualism/Collectivism: New cultural dimensions of values", in: *Individualism and collectivism: Theory, method and applications,* U. Kim, H.C. Triandis, C. Kagitcibasi, S.C. Choic, G. Yoon (eds), Sage, Thousand Oaks, CA, 85-122.

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. doi:10.1016/j.cose.2015.01.002

Stanton, J. M., Stam, K. R., Mastrangelo P., & Jolton, J.(2005). Analysis of end user security behaviours. *Computer Science, 24,* 33-124. doi:10.1016/j.cose.2004.07.001

Solic, K., Velki, T., & Galba, T. (2015). Empirical study on ICT system's users' risky behavior and security awareness. Paper presented at the *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38TH International Convention,* (pp. 1356-1359). Opatija: Croatia.

Vance, A. (2010). Why do employees violate IS security policies? Insights from multiple theoretical perspectives. University of Oulu, Oulu.

Van der Linden, S. (2012). Understanding and achieving behavioral 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*. Freiburg: Germany.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. doi:10.1016/j.cose.2013.04.004

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23,* 191-198. doi:10.1016/j.cose.2004.01.012

Wiley, A., McCormac, A., Calic, D. (2019). More than the individual: examining the relationship between culture and information security awareness, *Computer and Security.* Submitted under review.

Yeh, Q., & Chang, A. (2007). Threats and countermeasures for information system security: A cross-industry study, *Information & Management, 44,* 480-491. doi:10.1016/j.im.2007.05.003

Research Report

Word Count: 8287

A Cross-Cultural Investigation of Information Security Awareness (ISA)

[redacted]

Affiliation: The University of Adelaide

Postal Address: The University of Adelaide

SA 5005

AUSTRALIA

Email Address: [redacted]

Declarations of interest: none

Abstract

Research focusing on the role of the employee and the associated individual differences has identified a variety of factors that may influence information security awareness (ISA) in the workplace; however, the results associated with age and gender have been inconsistent (Hadlington, Popovac, Janicke, Yevseyeva & Jones, 2018; McCormac et al., 2017). Thus, this study aimed to address discrepancies in the literature by further examining the relationship between ISA, age, gender, employment status, and familiarity with computers. Additionally, this study examined the novel relationship between ISA and country, as well as industry sector, which has received little attention in previous literature. A total of 2823 working adults from the United Kingdom and Australia completed an online questionnaire. ISA was measured using the Human Aspects of Information Security Questionnaire (HAIS-Q). The influence of country was interpreted using Hofstede's framework of national culture. Analysis revealed a significant relationship between percentage of time spent using a computer technology and ISA; a significant interaction effect between age and gender, demonstrating that older females had significantly higher ISA scores; a significant difference in scores between countries, demonstrating that working adults in Australia have a significantly higher ISA score which we attributed to two dimensions of national culture; and finally, a significant difference in scores was found between industry sectors. This research may aid the design of effective intervention strategies to improve cyber security behaviour which are sensitive to the individual and group differences in ISA identified in this research.

Keywords: Information Security Awareness (ISA), national culture, Uncertainty avoidant, Long-term Orientation, individual differences.

1. Introduction

While organisations expand their use of advanced technologies, insufficient attention is being attributed to the role of human factors in information security. Information security relates to preserving the confidentiality, integrity, and availability of an organisation's information, and when this is compromised by employees, it can pose an enormous threat to an organisation (Parsons, McCormac, Butavicius & Ferguson, 2010). As stated in a recent report on cyber investigation of breaches, ninety-five percent of security incidents were the result of human error; this has resulted in experts labelling the employee as the 'weakest link' in the protection of an organisation's information security system (Dols & Silvius, 2010; IMB Global Technology Services, 2014). In 2017 and 2018, more than sixty-five percent of Australian organisations were victims of cyber-crime, with one in 10 experiencing losses greater than one million, and nine percent reporting having had the confidentiality, integrity, or availability of sensitive data compromised (PwC, 2018). These attacks are especially threatening when systems of national interest and critical infrastructure are targeted. In 2017, three percent of Australian cyber-attacks were of this nature (Australian Cyber Security Centre, 2017).

A computer science approach to information security has traditionally focused on technical measures to mitigate risks (Aurigemma & Panko, 2012). However, technology alone cannot sufficiently protect the security of organisations. More recently, the importance of the human factor has become increasingly recognised, yet previous research has tended to focus on single areas of interest; for example, individual factors such as personality (McCormac et al., 2017). Previous research has also demonstrated that organisational policy and training, for example, are correlated with a more positive information security culture (Da Veiga & Martins, 2015; Safa et al., 2015). While such organisational findings are extremely useful, it is argued that the practicalities of these outcomes are limited as such

findings are influenced by industry sector, which has not received adequate research attention. Furthermore, it has also been postulated that national culture would have a significant effect on employee behaviour and the security breaches experienced by organisations (Crossler et al., 2013; Vroom & Von Solms, 2004). Studies that account for this cross-cultural difference are vital, as national culture is likely to have a direct impact on various elements of information security. Consequently, the body of literature to date is unable to provide a comprehensive understanding of an individual's or organisation's Information Security Awareness (ISA).

1.1 Information Security Awareness

ISA refers to the degree to which employees understand the importance and implications of their organisation's information security policies, rules and guidelines, and the degree to which they behave in accordance with such policies (Bulgurca, Cavusoglu, & Benbasat, 2010; Kruger & Kearney, 2006). ISA is a global issue, with major data breaches and cyber-attacks being identified as two of the top five economic social risks that the world will face in the next decade (The World Economic Forum, 2018). Researchers have suggested that focusing on the extent of employee ISA is of higher priority than solely focusing on technical measures (Parsons, McCormac, Butavicius, Pattinson, & Jeram, 2014; Parsons et al., 2010). Thus, understanding ISA and its contributing factors is crucial in alleviating and preventing future information security attacks. Employee ISA behaviours are influenced by several factors, including attitude towards risks and vulnerabilities, knowledge of the organisation's policy, and training in the proper use of countermeasures (Aytes & Conolly, 2003). ISA has a particular focus on the role of the human, who is often discussed as being the *"first line of defence"* against information security threats (Von Solms & Van Niekerk, 2013, p.12).

The Knowledge-Attitude-Behaviour (KAB) model has been applied to the ISA context as a basis for assessing ISA. This model encompasses three components: knowledge (what does the person know), attitude (how do they feel about the topic), and behaviour (what do they do; Kruger & Kearney, 2006; Siponen, 2000). Evidence of the validity of the KAB model is now well established, and its use is highly supported (Hadlington, Popovac, Janicke, Yevseyeva, & Jones, 2018; McCormac et al., 2016; McCormac et al., 2017; Parsons et al., 2017; Van der Linden, 2012).

1.1.1 The Human Aspects of Information Security Questionnaire

The KAB model underpins the Human Aspects of Information Security Questionnaire (HAIS-Q). Developed by Parsons and colleagues (2014), the HAIS-Q is a useful tool to measure an individual's ISA. In line with the KAB model, this measure proposes that as an employee's information security knowledge increases, his/her attitude will improve, resulting in improved information security behaviours (Kruger & Kearney, 2006; Parsons et al., 2014). The HAIS-Q has been developed through a review of information security policies and standards, as well as via consultation with managers and information technology professionals (Parsons et al., 2014). In contrast to other potentially favourable measures such as The User's Information Security Awareness Questionnaire (UISAQ), the HAIS-Q has received significant theoretical support, and has undergone thorough reliability and validity testing with diverse populations; however, it is important to note that, to date, this has primarily focused on the Australian context (Hadlington & Parsons, 2017; McCormac et al., 2016, 2017b; Parsons et al., 2017).

1.2. Individual Differences

The human aspects of information security research has primarily focused on understanding the role of the employee and the associated individual differences and

vulnerabilities that may affect information security behaviours. This research has been crucial towards gaining an understanding of the psychological mechanisms which influence ISA.

Previous research efforts have demonstrated that ISA can, to an extent, be predicted by several factors such as age, gender, resilience, work locus of control, education, familiarity with computers, and some personality factors (Hadlington et al., 2018; McCormac et al., 2017; Öğütçü, Testik, & Chouseinoglou, 2016; Pattinson, Butavicius, Parsons, McCormac, & Calic, 2015; Shropshire, Warkentin, & Sharma, 2015). For example, these studies have found that individuals who are more conscientious and agreeable, display greater resilience, have a higher level of education, are more familiar with computers, are more internally motivated, and have a lower propensity to take risks are likely to have higher ISA scores.

Although previous research has identified many individual differences that may influence ISA, the pattern of results relative to age and gender has been inconsistent. For example, Pattinson et al. (2015) did not report findings based on gender, Hadlington et al. (2018) did not report findings based on age, and McCormac et al. (2017) found that, once other individual factors were considered, neither age nor gender was significant in their regression model. Mostly, studies have found small but significant differences between gender and age and ISA. That is, ISA is positively associated with being female, and increases in age; however, some studies have failed to either (1) explore these variables or (2) identify a significant relationship between one and/or both of these variables and ISA (McCormac et al., 2017).

1.3 Industry Sector

Information security is crucial for information-sensitive industries such as banking and finance or retailing services (Yeh & Chang, 2007), and the requirements for information security policy varies across industries based on the service provided. For example, Jung and

Lee (2001) observed that the threats associated with Internet use, in particular, varied among industries according to the needs of the organisation for information availability, confidentiality, and integrity. Different information technology architectures, computing needs, network, and client-server settings also alter the level of ISA required for an organisation and its employees.

Previous studies examining ISA have infrequently considered how organisational characteristics influence security practice and, in turn, ISA. In particular, research has not adequately explored the effect of differences based on industry sector. One of the limited attempts to explore industry and ISA is accredited to Pattinson and colleagues (2016). This research aimed to assess the ISA of employees of an Australian bank using the HAIS-Q and to compare these results with the general workforce in Australia. It was predicted that the ISA of the bank employees should be higher than for the general workforce due to the typical characteristics defined by the job role within the finance/banking industry. This includes exposure to more sensitive and confidential information. The researchers found that ISA percentage scores for bank employees were twenty percent higher than those for the general workforce. Furthermore, the bank employees recorded their highest ISA scores for the Information Handling focus area as measured by the HAIS-Q. These findings indicate that industry types, and the associated job roles and exposure, has an influence on employee ISA. This research is the first to utilise the HAIS-Q to explore such a phenomenon and justifies further investigation into the effect of industry on ISA.

Furthermore, these findings also suggest that our current security threat mitigation strategies, such as policy implementation and/or training interventions, which do not take into consideration industry differences, may prove to be insufficient. Because of this, researchers have called for separate attention to be paid to the financial services sector as this industry's

characteristics and experiences, concerning information security and privacy issues, are very different from other industries (Ifinedo, 2014).

1.4 National Culture

Very little is known about the impact of environmental or contextual factors on the assessment of ISA. However, it is well established that human behaviour is largely determined by cultural aspects, and the workplace is no exception. Cultures at the national level exert a subtle, yet powerful influence on individuals and organisations (Ifinedo, 2014). Workplace interactions and learnings are grounded in a prevalent national culture (Cronk & Salmon, 2017; Ifinedo, 2014; Kruger, Drevin, Flowerday, & Steyn, 2011). This means that national culture influences the perceptions of employees, management, and whole organisations about a wide range of issues, including those related to information security. Noteworthy, it is suspected that national culture has a direct link with the human factor due to the value orientations individuals may or may not embody. Thus, national culture could affect the relationships discovered in previous research, by making them stronger, weaker or non-significant (Flores, Antonsen & Ekstedt, 2014). Nevertheless, to date, the role of national culture in an ISA context has received limited consideration.

The construct of national culture in this study has been measured using a framework first proposed by Hofstede (1993). As part of this framework, national culture is a concept based on value orientations which are considered important and shared across different countries (Hofstede, 2001). According to Hofstede (1993, p.82) culture refers to *"the collective programming of the mind that distinguishes one group or category of people from another".* His six-dimension framework represents independent preferences for one state of affairs over another that distinguish countries (rather than individuals) from each other. The six dimensions include: Power distance, Individualism versus collectivism, Masculinity

versus femininity, Uncertainty avoidance, Long-term versus short-term orientation, and Indulgence versus restraint. These dimensions have been formulated from a large database of employee value scores collected between 1967 and 1973. The data covered more than 70 countries, from which Hofstede first used the 40 countries with the largest groups of respondents and afterwards extended the analysis to 50 countries and 3 regions (Hofstede Insights, 2019). As a result of this work, each country is scored on a scale of 0 to 100 for each dimension, and a country is often referred to as being either 'high' or 'low' on a dimension based on this scoring system.

This framework is the predominate foundation of cross-cultural studies and has now been employed and validated in information security research (House, Hangs, Javidan, Dorfman, & Gupta, 2004; Johnston & Hale, 2009; Myer and Tan, 2002; Robey & Rodrigues-Diaz, 1989). It is relevant because national culture influences individuals and group behaviour, including the interpretation and implementation of practices within their contexts. National culture may therefore influence, information security related policies within an organisation. Essentially, the complete management of information security can be ensured only if the behavioural aspects of national culture are also understood.

Previous research has begun to identify the importance of national culture in understanding information security related issues. For instance, Björck and Jiang (2006) found that the assessment of information security implementations differed by cultural attributes. For example, the researchers noted differences in several security practices between Singaporean and Swedish companies, such as how the companies controlled for security risks and managed information breaches, which they attributed to the differences in Power distance and Individualism vs. collectivism (Björck & Jiang, 2006).

Similarly, Dinev and colleagues (2009) showed that national cultural differences can be used to differentiate user behaviour towards protective security technologies. Their research found significant differences between respondents from the USA and South Korea, which is argued to be a cumulative result of Individualism, Masculinity, Power distance and Uncertainty avoidance. This research highlighted the importance of national culture as a significant relationship moderator within the information security literature and defined the role of organisational factors (in contrast to individual factors) in the formation of user attitude and behaviour towards using protective information technology (Dinev, Goo, Hu, & Nam, 2009).

Finally, research exploring the influence of national cultures on non-compliance behaviour has linked national culture and risk-taking behaviour. That is, the researchers found that in contrast to Belgium, employees from the Netherlands, which orients a low Power distance and Uncertainty avoidance score, demonstrate a willingness to *"bend the rules"* or to disobey orders from their superior (Dols & Silvius, 2010, p.20). It is clear that while national culture has been examined in the information security realm, to date, it has not yet been paired with ISA specifically.

4.1.1 Long-term Orientation and Uncertainty Avoidance

It is interesting to note that the national cultural dimensions Long-term orientation and Uncertainty avoidance are particularly interesting and relevant to information security research. Both Long-term orientation and Uncertainty avoidant cultural dimensions were developed specifically to address cross-cultural differences in uncertainty when making decisions, and uncertainty is common in the security context (Hofstede, 2001). Uncertainty avoidant refers to a culture's acceptance of ambiguous or uncertain situations (Hofstede, 2001). This concept holds that groups of people are socialised to have different levels of

comfort with ambiguity and uncertainty, and they are socialised to cope and manage the anxiety associated with uncertainty differently (Hofstede, 2001). Certain cultures will therefore have a desire to minimise uncertainty where possible, whereas other cultures are less concerned by this. Hofstede suggests that cultures with a high Uncertainty avoidant score are more likely to welcome a technology that offers to reduce uncertainty, for example, computer technologies. However, there is not a consensus view on how Uncertainty avoidance as a cultural phenomenon affects an individual's acceptance of technologies. Findings from technology-acceptance literature has suggested the opposite, arguing high Uncertainty avoidant cultures tend to adopt new technologies slower, often waiting to learn from the experiences of others (Sundqvist, Frank, & Puumalainen, 2005).

Long-term orientation refers to how a culture balances its past with the challenges of the present or future (Hofstede, 2001). The notion of this cultural dimension is that groups of people are socialised to have differing desires in terms of sacrificing time, money, and effort today for potential future success (Cannon, Doney, Mullen, & Petersen, 2010). Cultures that have a longer term orientation value persistence more than immediate results, while cultures that have a shorter term orientation value immediate results and relatively instant gratification (Hofstede, 2001). Previous literature has demonstrated that Long-term orientation is positively correlated with being innovative and proactive, and negatively correlated with risk taking, which is particularly important within an information security context (Cannon et al., 2010; Vitell et al., 2015; Vitell, Nwachukwu, & Barnes, 1993). Because of its linkage with being proactive and limiting risk taking behaviour, we argue that an individual's Long-term orientation would influence many information security related decisions (such as choosing a strong password, or reporting a security breach).

Given the significance of Uncertainty avoidant and Long-term orientation in influencing decision making and therefore security related behaviours, Hofstede's national

culture framework is used in the current study to analyse and explain differences in ISA scores between employees residing in Australia and the United Kingdom. According to Hofstede Insights (2019), there are two dimension differences to consider between Australia and the United Kingdom, specifically: Uncertainty Avoidance (Aus (51 out of 100) vs. U.K (35 out of 100)) and Long-Term Orientation (Aus (21 out of 100) vs. U.K (51 out of 100)). Thus, these countries provide the opportunity to examine Uncertainty avoidance and Long-term orientation in relation to ISA. This comparison is of particular interest because the United Kingdom is the second largest source of foreign investments in Australia; thus, there is a significant relationship underpinned by closely aligned strategic outlook and interests, substantial trade and investment links, and shared security interests (Australian British Chamber of Commerce, 2019; Department of Foreign Affairs and Trade, 2019). Consequently, exploring the influence of national culture between these nations is useful for both nations acting independently, and in collaboration with one another.

1.5 Study Aims

While there is theoretical support for the relationship between ISA and individual differences, there is discrepancy within the literature relative to age, gender, employment status, and familiarity with computers in the context of ISA. Therefore, this study is exploratory in nature so that the variables mentioned above can be further investigated, with the research aim to eliminate a degree of inconsistency within the literature relative to these variables.

1.5.1 Hypotheses.

As part of this investigation, the relationships between ISA and individual differences such as age, gender, employment status, and familiarity with computers will be explored. In addition, this study also aims to empirically examine the novel relationship between ISA and

country (which is interpreted using Hofstede's national culture framework) as well as the relationship between ISA and industry sector. Founded on previous research outlined above, it is hypothesised that:

1. In line with Hofstede's dimensions, which indicate a difference between Australia and the United Kingdom in Long-term orientation and Uncertainty avoidance, Australian employees will have better ISA scores than employees from the United Kingdom.
2. Employees from industries such as Finance and Insurance and Healthcare and Community will have higher ISA scores due to the job role and its associated tasks.

2. Method

This study used secondary data analysis of pre-existing data. The data has been sourced from four independent studies, which have each utilised the HAIS-Q in order to obtain an ISA score. The data was collected on two separate occasions in both the United Kingdom and Australia in 2017 and 2018 allowing for a comparison of national cultures. Data collection in each of the four studies involved online questionnaire-based surveys of working adults, administered through the web-based survey platform Qualtrics Research Panels. Thus, in total, this study has utilised four pre-existing data sets and for each of the collections of data, ethics approval was granted by one of the following committees: The Human Research Ethics Subcommittee of The University of Adelaide School of Psychology, the Defence, Science and Technology Group (DST Group) Human Research Ethics Review Panel and The University of De Montfort, Health and Life Sciences Ethics Committee.

2.1 Participants

Across the collapsed sample, a total of 2825 (1500 females, 1323 males, 2 gender unspecified) working adults from the United Kingdom (n = 1281) and Australia (n = 1544*)* completed the online questionnaire. Participants were primarily full-time workers (n = 1965) as opposed to part-time workers (n = 660) or contracted/self-employed workers (n= 200). See Table 1 for detailed participant demographics.

2.1.1. Inclusion and Exclusion Criteria

Participants were required to be over the age of 18, currently employed, working within the United Kingdom or Australia, spend at least some part of their standard working day using a computer technology, and work for an organisation with a formal or informal information security policy.

Table 1: *Participant demographics based on data set*

	Australia 2017 (*N* = 1019)[1]	Australia 2018 (*N* = 525)[2]	UK 2017 (*N* =338)[3]	UK 2018 (*N* = 943)[4]	Total (*N* = 2825)
Age Categories					
19 <	7 (.7)	23 (4)	x	38 (4)	68 (2)
20-29	110 (10)	128 (24)	42 (12)	204 (21)	484 (17)
30-39	229 (22)	149 (28)	103 (30)	217 (23)	698 (24)
40-49	228 (22)	88 (16)	86 (25)	179 (19)	581 (20)
50-59	245 (24)	75 (14)	82 (24)	228 (24)	630 (22)
> 60	200 (19)	62 (11)	25 (7)	77 (8)	364 (12)
Gender					
Male	493 (48)	217 (41)	165 (48)	448 (47)	1323 (46)
Female	525 (51)	307 (58)	173 (51)	495 (52)	1500 (53)
Unspecified	1 (.1)	1 (.2)	x	x	2 (.1)
Industry					
(1) Mining, Manufacturing and Construction	96 (9)	x	52 (15)	x	148 (5)
(2) Accommodation and Food	32 (3)	x	10 (3)	x	42 (1)
(3) Education	118 (11)	x	22 (6)	x	140 (5)
(4) Finance and Insurance	62 (6)	x	19 (5)	x	81 (3)
(5) Agriculture, Forestry, Fishing and Hunting	33 (3)	x	3 (.9)	x	36 (1)
(6) Trade (Wholesale and Retail)	122 (12)	x	50 (14)	x	172(6)
(7) Healthcare and Community	122 (12)	x	60 (17)	x	182 (6)
(8) Other	434 (42)	x	122 (36)	x	556 (19)
Employment Status					
Full Time	651 (63)	315 (60)	291 (86)	708 (75)	1965 (69)
Part Time	236 (23)	142 (27)	47 (13)	235 (24)	660 (23)
Contracted/Self employed	132 (13)	68 (13)	x	x	200 (7)
Percentage of time at work spent using a computer technology					
< 20%	175 (17)	78 (14)	x	x	253 (9)
21-60%	297 (29)	171 (32)	64 (18)	211 (22)	743 (26)
61-80%	246 (24)	114 (21)	124 (36)	331 (35)	815 (28)
> 80%	301 (29)	162 (30)	150 (44)	401 (42)	1014 (35)

[1]*(McCormac, et al., 2017),* [2]*(Wiley, McCormac & Calic, 2019)* [3]*(Hadlington & Parsons, 2017)* [4]*(Hadlington, et al., 2018)* x this data was not collected / reporte

2.2 Measures

2.2.1 ***Demographic Information***

The Participants were asked to provide individual demographics including age and gender, as well as organisational demographics including employment status, percentage of time at work spent using a computer technology, and industry sector.

2.2.2 ***The Humans Aspects of Information Security Awareness Questionnaire (HAIS-Q)***

The HAIS-Q was used in each study as measure of ISA. This scale measures ISA based on an individual's knowledge, attitude, and behaviour in relation to appropriate security behaviours. The scale comprises of 63 items which probe seven areas of security. These include: Password management, Email use, Social media, Mobile computing, Information handling, and Incident reporting. Statements were answered on a 5-point Likert scale, ranging from 1= 'Strongly Disagree' to 5 = 'Strongly Agree'. A sample behaviour item reads – *"When working in a public space, I leave my laptop unattended".*

Parsons et al. (2014) reported Cronbach's alpha coefficients of 0.84, 0.84 and 0.92 for Knowledge, Attitude and Behaviour, respectively. This is consistent with alpha levels reported in each of the four studies, with scores ranging from 0.83 to 0.92 (McCormac, et al., 2017; Hadlington & Parsons, 2017; Hadlington, et al., 2018; Wiley, McCormac & Calic, 2019). Refer to Parsons et al. (2017) for detailed validity and reliability assessments of the HAIS-Q.

2.3 Procedure

The four studies followed an identical procedural outline. Data collection for each study involved an online questionnaire-based survey, administered through the web-based survey platform Qualtrics Research Panels. Participants were invited to take part in the survey and were given a brief introductory statement about the nature of the study.

Participants were told that participation was voluntary, and they could withdraw at any point during the process. Participants gave consent prior to completing the survey. In all cases, data responses were examined for signs of content non-responsivity. In instances where responses appeared to be 'mechanical' and therefore indicative of a lack of attention, scores were excluded. For example, if a participant selected 'strongly agree' to all questions, because some items are reverse-scored, this would suggest inattentive responding.

Before participants commenced the HAIS-Q, demographic information was collected, also through the Qualtrics platform. Across all four studies, there were slight variations in the type of demographic data that was collected. For example, questions such as *"What type of employer do you work for?"* or *"What is your ethnic group?"* were not consistently asked. Due to this, the current study only examines and reports on the variables which could be reliably compared across studies. There were instances in which the same question was stated in a slightly different way in the Australian studies compared to the United Kingdom studies. For example, the Australian studies asked participants to report their age in relation to a provided set of age categories (e.g., between 20-29) whereas the United Kingdom studies asked participants to report their age in numerical format (e.g., 25). Therefore, for some of the variables that are included in this study, adjustments to the data were necessary so that the data that has been obtained from each of the four studies is comparable. Finally, it is also important to recognise that for the organisation variable 'Industry Sector', data can only be utilised from the 2017 Australian and the 2017 United Kingdom studies as this information was not consistently collected in the 2018 studies. In summary, to account for differences in data collection and question design across the four studies, not all variables could be included in the analysis. Therefore, to ensure consistency and reliability across comparisons, such amendments to the data has resulted in the following six variables which this study has

analysed: (1) Country, (2) Age, (3) Gender, (4) Employment Status, (5) Percentage of Time at Work Spent Using a Computer Technology, and (6) Industry Sector.

2.3.1 ***National Culture: Hofstede's Cultural Dimensions***

Hofstede's national culture framework is based on six distinct dimensions, which represent independent preferences for one state of affairs over another that distinguish countries (rather than individuals) from each other. Each county is scored on a scale of 0 to 100 for each dimension, and a country is often referred to as being either 'high' or 'low' on a dimension based on this scoring system. This framework represents the predominate foundation of cross-cultural studies and has been validated in Information security research. Thus, Hofstede's national culture framework is used in this study to analyse and explain differences in ISA scores between Australia and the United Kingdom. According to Hofstede Insights (2019) and as shown in Figure 1, there are two dimension differences to consider between Australia and the United Kingdom, that being: Uncertainty Avoidance (Aus (51 out of 100) vs. U.K (35 out of 100)) and Long-Term Orientation (Aus (21) vs. U.K (51)). Hence, as previously mentioned, the focus of this analysis will be on these two dimensions.

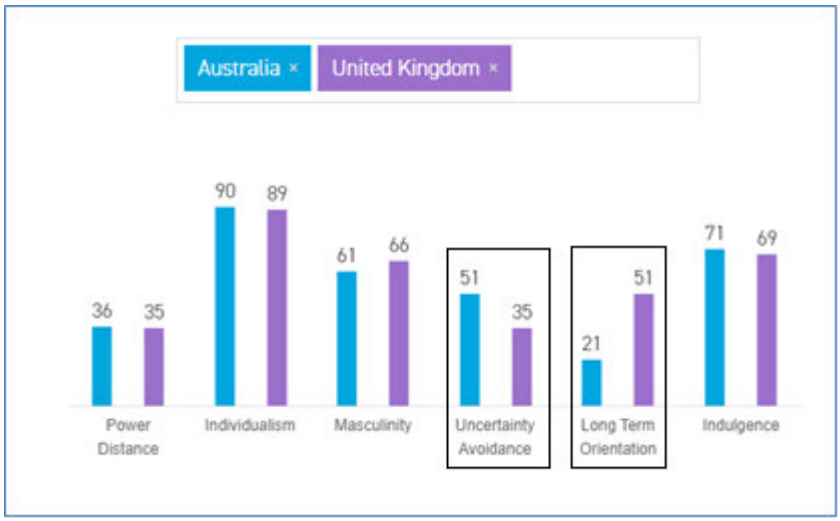


Figure 1. *Comparison of Australia and United Kingdom taken from Hofstede Insights (2019)*

3. Results

Preliminary analyses were conducted to ensure there was no violation of the assumptions of normality, linearity, multicollineraity and homoscedasticity. As no major violations were identified, several parametric tests were used.

The aim of this study was to investigate the relationship between ISA (total HAIS-Q score), country, individual differences, and organisational factors. SPSS was used to analyse the data set. Descriptive statistics and Pearson's correlations for the key variables in the present study (i.e., age, gender, country and overall ISA score, in addition to employment status, and percentage of time spent using computer technology) are shown in Table 2. There were significant correlations between ISA and age, gender, employment status, and country. This suggests that such factors have an influence on an individual's total ISA score. Although the relationship between ISA and percentage of time spent using computer technology was non-significant, since this variable was predictive in previous research (see, for example, Pattinson et al, 2015), it will continue to be explored. As the values assigned to Industry sector are not ordinal, this variable was not included in the correlation matrix.

To further determine how age, gender, country, percentage of time spent using computer technology, and employment status predict total scores on the HAIS-Q, a standard multiple regression was conducted. The results of the regression are presented in Table 3. The model explains a total of 10.3% of the variance in the total scores on the HAIS-Q, $R_{adj}^2 = .103$, $F(5, 2819) = 65.8$, $p < 001$. Age, gender, country, and percentage of time spent using computer technology ($p < .001$) all acted as significant predictors for total scores on the HAIS-Q. Employment status failed to act as a significant predictor for total scores on the HAIS-Q ($p = .84$).

Table 2

Correlations and Descriptive Statistics; Industry Sector (N= 1357) and ISA, Age, Gender, Employment Status, Percentage of Time Spent Using Computer Technology, Country (N=2825)

Variables	ISA	Age	Gender	Employment Status	Percentage of Time	Country
ISA						
Age	.276**					
Gender	.085**	-.195**				
Employment Status	.046*	.072**	.161**			
Percentage of Time	.020	-.155**	.081**	-.243**		
Country	-.083**	-.094**	-.020	-.230**	.299**	
Mean	255.76	***	***	***	***	***
SD	35.631	***	***	***	***	***

Note. *$p < .05$; **$p < .001$: ***Mean and SD scores for ISA are available, the remaining factors are nominal variables, and age ranges, rather than exact ages, were recorded.

Table 3

Summary of Multiple Regression for Variables Predicting Total HAIS-Q scores (N = 2825)

Variable	*B*	*SE B*	β *(standardised)*	*t*	*p*
Age	8.05	.48	0.30	16.71	< .001
Gender	9.7	1.32	0.13	7.34	< .001
Employment Status	0.22	1.14	0.00	0.19	.84
Percentage of Time	2.40	0.58	0.08	4.14	< .001
Country	-5.30	1.35	-.074	-3.90	< .001

3.1 ISA, Age, Gender

To further examine the effects of age and gender on total scores on the HAIS-Q, a two-way between-subjects ANOVA, with two levels for gender (male and female), and six levels for age (19 or less; 20-29; 30-39; 40-49, 50-59; 60 and above), was conducted. This analysis revealed a statistically significant effect for both age, $F(5, 2811) = 25.83$, $p < .001$, $\eta^2 = .044$, and gender, $F(2, 2811) = 13.92$, $p < .001$, $\eta^2 = .010$. Post-hoc comparisons using the Tukey HSD test indicated that the mean ISA scores for the 20-29 age group ($M = 240.68$, $SD = 38.93$) was significantly different to the 30-39 group ($M = 249.41$, $SD = 38.93$), the 40-49 group ($M = 259.76$, $SD = 32.96$), the 50-59 group ($M = 264.77$, $SD = 31.95$), and the 60 and above group ($M = 269.13$, $SD = 25.68$). The mean score for the <19 age group ($M = 238.92$, $SD = 34.43$) was also significantly different to the 60 and above age group. There was also a statistically significant interaction between the effect of age and gender on total scores on the HAIS-Q, $F (6, 2811) = 3.31$, $p = .003$, $\eta^2 = .007$. It was observed that participants in the older age brackets tended to have higher total scores on the HAIS-Q than participants in younger age brackets. Female participants ($M = 258.62$, $SD = 33.8$) were found to have significantly higher total scores on the HAIS-Q than their male counterparts ($M = 252.52$, $SD = 37.33$), although the effect size was small, $d = 0.10$. While men have

lower total scores on the HAIS-Q than women, the differences between genders was particularly large between the ages of 20-29 and then became smaller after the age of 39. Therefore, younger men and in particular men aged 20-29 have particularly low total scores on the HAIS-Q when compared to both older men and women. This demographic finding perhaps helps to explain some of this inconsistency in previous research.

3.2 ISA and National Culture

To explore the relationship between national culture and ISA, an independent samples t-test was conducted to compare the HAIS-Q total scores for the United Kingdom sample and the Australian sample. Working adults in Australia (M = 258.44, SD = 32.88) had significantly higher HAIS-Q scores than working adults in the United Kingdom (M = 252.52, SD = 38.44), t (2531.8) = 4.34, p = <.001. However, the magnitude of the differences in the mean was very small (eta squared = .006).

To further investigate the effect of national culture, a series of independent samples t-tests, using a Bonferroni correction were conducted to compare the total scores of each of the seven focus areas of the HAIS-Q for the United Kingdom and Australian samples. This information has been depicted in Figure 2 and can be further examined in Appendix A. A significant difference in scores was found between the scores for five of the six focus areas (Password management, Email use, Internet use, Social media use, Mobile devices, and Information handling). However, the magnitude of the differences in the means was very small (eta squared = .003). There was no significant difference in scores for Incident reporting found between the United Kingdom (M = 36.39, SD = 5.99) and Australia (M = 36.52, SD = 5.32).

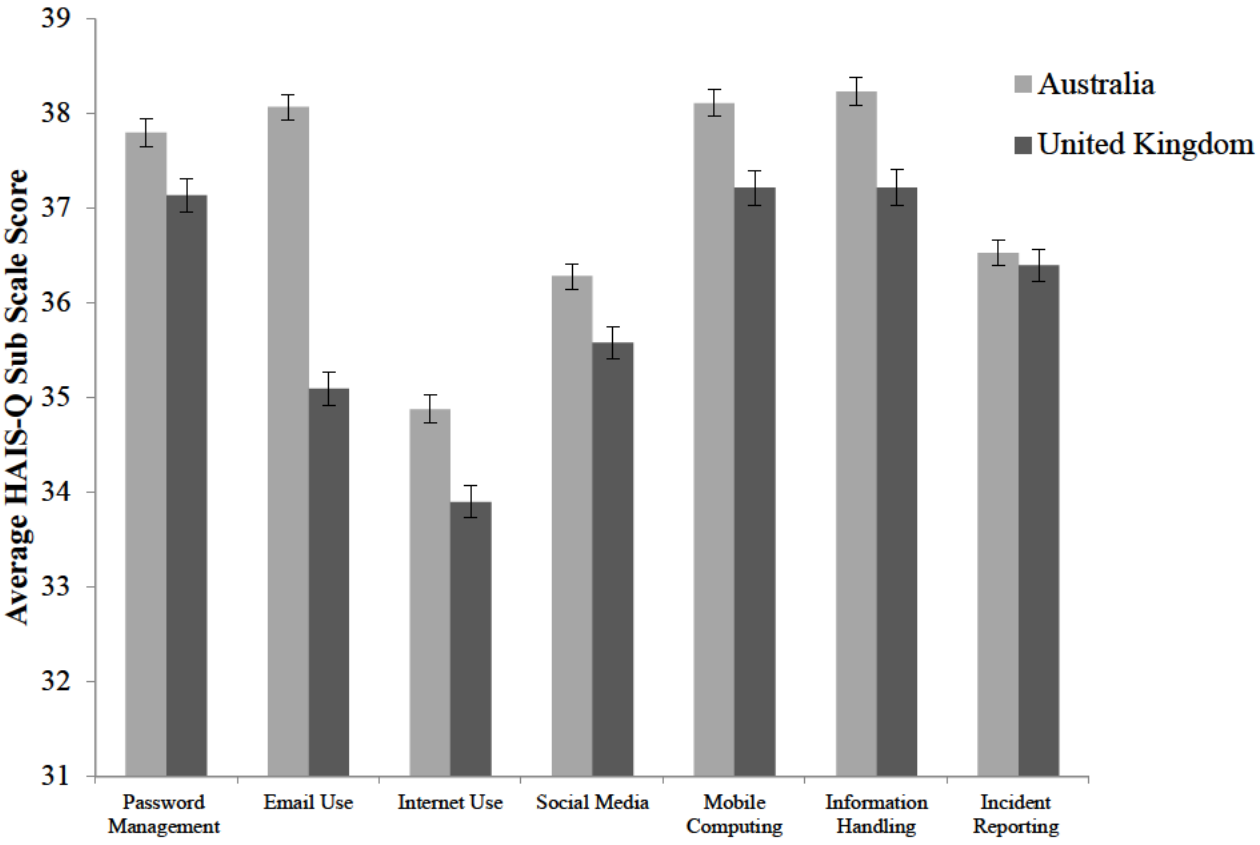


Figure 2. *Average HAIS-Q Focus Area Scores for Australia and United Kingdom. Error bars denote one standard error around the mean.*

3.3 ISA and Industry Sector

A one-way between-groups analysis of variance was conducted to explore the impact of industry sector on total scores on the HAIS-Q. There were no significant differences in scores found for industry sector and total scores on the HAIS-Q. Despite not reaching statistical significance, the actual differences in mean scores between the seven industries are worth examining. As Figure 3 demonstrates, (4) Finance and Insurance (M = 262.49, SD = 32.36) and (7) Healthcare and Community (M = 260.75, SD = 31.43) have a higher mean total score on the HAIS-Q compared to (5) Agriculture, Forestry, Fishing and Hunting (M=250.63, SD= 33.97) or (2) Accommodation and Food (M= 248.85, SD= 31.30). This pattern in mean scores was anticipated; it was hypothesised that industries such as Finance

and Insurance and Healthcare and Community would have higher ISA scores due to the job role and its associated tasks such as managing/processing sensitive information using computer technologies. It is for this reason that further statistical analysis is conducted.

An independent samples t-test was conducted to compare the HAIS-Q total scores for Finance and Insurance and Healthcare and Community (FIHC), and the remaining industry sectors (excluding 'Other'). A significant difference in scores was found between the scores for FIHC (M = 261.28, SD= 31.67) and the remaining industry sectors (M = 255.03, SD = 32.57); t (799) = 2.57, p= <.01. The magnitude of the differences in the mean was very small (eta squared =.008).

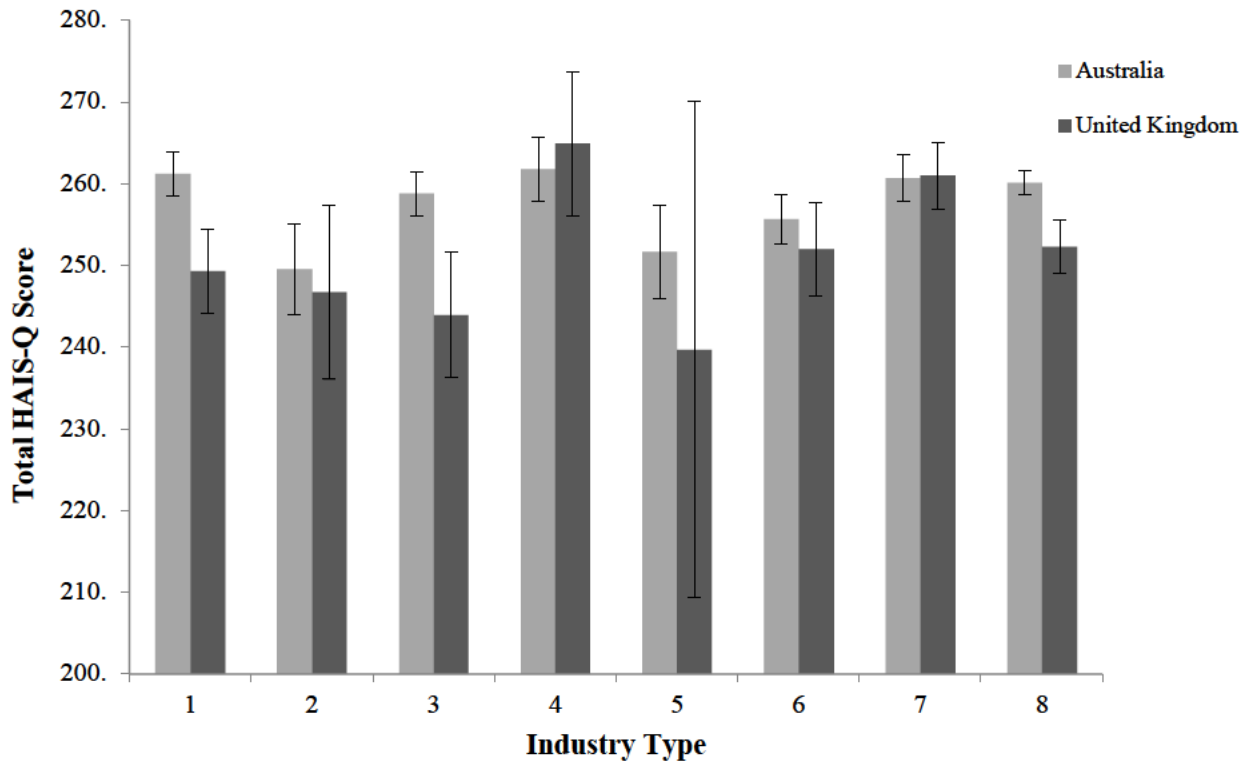


Figure 3. *Mean scores for total scores on the HAIS-Q (ISA) for Industry Sector.*

4. Discussion

The aim of this study was two-fold, first, to empirically examine the relationship between information security awareness (total HAIS-Q score), and (1) country. Secondly,

the aim of this study was to future explore individual differences and organisational factors relative to information security awareness. Individual factors included (2) age, (3) gender, (4) employment status, and (5) familiarity with computers (measured via percentage of time spent using computer technology). Organisational factors explored in this study include (6) industry sector. The following sections will discuss the study's findings, applications, limitations, and future directions.

4.1 Findings and Implications

In the context of the six key variables that were the focus of the present study, a significant linear relationship was found between ISA, country, age, gender, and percentage of time spent using computer technology. These variables explained a total of 10.3% of the variance in ISA. To the authors' knowledge, this is the first time a link between ISA and country (explained using Hofstede's national culture framework) has been noted in the literature.

4.1.1 National Culture.

Information security literature has discovered many important factors that influence an individual's propensity to adopt a high ISA standard. However, much of this literature assumes that their reported findings will be relevant to individuals across different cultures, yet individuals conditioned into different cultures vary across multiple cultural dimensions, which consequently influences their workplace values and behaviours (Hofstede, 1990).

As mentioned previously, Long-term orientation and Uncertainty avoidance are highly relevant to information security research because these cultural dimensions were developed specifically to address cross-cultural differences in uncertainty when making decisions (Hofstede, 2001). People socialised to have different levels of comfort with ambiguity and uncertainty, and those who have different desires relative to persistency and

results, cope and manage the anxiety associated with uncertainty differently and are more or less proactive and likely to take risks (Cannon et al., 2010; Hofstede, 2001; Vitell et al., 2015; Vitell, Nwachukwu, & Barnes, 1993). Furthermore, research has suggested that employees from countries with a lower uncertainty avoidance score demonstrate high risk-raking behaviours, a willingness to *"bend the rules"* or to disobey an order from their superior, and a belief that rules, policy and procedure guidelines are less likely to be documented. (Dols & Silvius, 2010, p.20, Klinger & Mallon, 2015; Martinsons & Westwood, 1997; Oliver, 2011). These behaviour outcomes would influence many information security related decisions, such as choosing when to share client information, or report a security breach.

In this study, it was found that working adults in Australia have significantly higher ISA scores than working adults in the United Kingdom, thus hypothesis 1 was confirmed. In line with Hofstede's (1993; 2001) dimensions and our hypothesis, this finding suggests that having a shorter-term orientation and a higher level of uncertainty avoidance creates better security behaviours and overall, a higher ISA score. This finding was also overall supported for the majority of focus areas. The subscales Informational handling and Incident reporting are arguably the more critical, decision-heavy and policy-related focus areas which would therefore invoke behaviour outcomes demonstrated by previous research. Therefore, it should follow that the scores for subscales Information handling, and Incident reporting, in particular, would differ significantly between Australia and the United Kingdom as a result of long-term orientation and uncertainty avoidance differences. However, a significant difference in scores was found only between the scores for Information handling.

These results are partially in line with past research. Consistent with previous research, the results from this study further reinforce the influence national culture can have, with some of this research arguing that the differences found are attributed to the dimension

Uncertainty avoidance in particular (Dinev et al., 2009; Flores et al., 2014). Thus, this research pattern is in keeping with the findings from this study; employees from the United Kingdom (who have lower uncertainty avoidance relative to Australian employees) had lower mean scores for both subscales Information handling and Incident reporting. The findings from this study therefore emphasise the importance for security managers and information security policy to consider cultural differences of their employees, especially in the workplace where diverse cultural background is evident, when formulating information security policy.

Although Australia had a higher score for Incident reporting, a significant difference was not achieved. Therefore, contrary to previous research, it was not the case that those employees who are more tolerant of risks and uncertainties appeared more willing to report threat incidents than their counterparts (Ifinedo, 2014). However, previous research has suggested that the Australian attitude "it is bad to be a dobber", i.e. report on another individual, can explain why results relative to Incident reporting have been comparatively lower in the past (Parsons et al., 2017). This might suggest that Hofstede's Uncertainty avoidant dimension does not capture the Australian aversion to reporting on others, which seems to play a significant role in how many Australians think and live (Wierzbicka, 2001). This presents a particularly interesting challenge for Australian organisations, which may be less problematic in other cultures (i.e. collectivist cultures) (Parsons et al., 2017).

4.1.2 Age, Gender and Percentage of time spent using computer technology.

The study aimed to further explore and address a degree of inconsistency within the literature relative to age, gender, employment status, and familiarity with computers in the context of ISA. In line with previous research (Hadlington et al, 2018; McCormac et al., 2018; Pattinson et al., 2015), a relationship between ISA and demographic variables was

found in this study. A positive linear relationship between age and ISA was demonstrated, with ISA increasing as age increased. Similar to McCormac and colleagues (2017), a significant interaction effect was also found between age and gender, demonstrating that female participants have significantly higher ISA scores than their male counterparts. While men had worse ISA than women, the difference between genders was particularly large between the ages of 20 and 29 and then plateaued after the age of 39. Previous cybersecurity research often demonstrates that women are generally more concerned about privacy than men, are more likely to comply with security policy, and thus, have better cyber-security behaviours (Hoy & Milne, 2010; Ifinefo, 2014; Laric, Pitta, & Katsanis, 2009). Additionally, factors such as conscientiousness, agreeableness, and emotional stability, and risk-adverseness have been shown to influence ISA, and these factors are arguably less prevalent in younger men (McCormac et al., 2017). Therefore, conclusions must be made with caution and further investigation of the potential effects of gender and age on ISA is required. For example, do security behaviours truly differ, or is it just a function of overconfidence in the younger males? And will this overconfidence decrease with age, or do the findings represent a generational difference? Longitudinal research is required to address these questions.

Percentage of time spent using computer technology was revealed to have no relationship with ISA, while employment status was positively correlated. Interestingly, employment status and percentage of time spent using computer technology were shown to be significantly and negatively correlated. This is a counter-intuitive finding; however, the number of responses for ‘contracted/self-employed’ might have influenced this direction. Additionally, to make the percentage of time variable comparable across the four pre-existing data sets, responses were converted from hours spent per day (average 7-hour workday) on a computer to the average percentage of time at work spent using computer

technology. This process may have unforeseeably altered the integrity of the categories by either over or under-representing such choices (i.e. < 20%). Nevertheless, percentage of time was predictive in previous research (see, for example, Pattinson et al., 2015), thus it was further explored in this study and the results of the regression revealed that percentage of time did, in fact, act as a significant predictor for ISA scores, whereas employment status did not. That is, those participants who spent more of their time using computer technology and were therefore more familiar with computer technology were likely to have higher ISA scores. Although this is a logical finding, it is inconsistent with previous research. Pattinson and colleagues (2015) found that those employees who were less familiar with computers were likely to have less risky accidental-naïve ISA behaviour (Pattinson et al., 2015). The researchers suggest that this finding could possibly be due to the complacent nature of people. In contrast, the findings from this study suggests that those who spent more of their time using computer technology may have been more exposed to the correct rules and processes at work, and therefore have better ISA behaviours.

4.1.3 Industry Sector.

There were no significant differences in scores found for industry sector and ISA. However, despite not reaching statistical significance, the actual differences in mean scores between the seven industries are telling. The observed pattern in mean score was anticipated; industries that require managing and/or processing sensitive information using computer technologies had higher ISA scores. For example, (4) *Finance and Insurance* had the highest ISA mean score, whereas (2) *Accommodation and Food* had the lowest. These findings are consistent with previous research (Pattinson et al., 2016), where the ISA of bank employees was compared to the general workforce and demonstrated to be higher. To further analyse this result, ISA scores from the industries that are more likely to be exposed to sensitive information (i.e., *Finance and Insurance* and *Healthcare and Community*) were

combined and compared to the remaining five industries. Hypothesis 2 was supported as a significant difference in scores was found. This finding further supports the hypothesis that industries where their job role requires access to sensitive information will have higher ISA scores. As mentioned previously, more time spent using computer technology, which is associated with the industry type, possibly results in those employees having acquired more frequent information security training. The results of the current study may be more robust compared to the Pattinson et al. (2016) study, as the current study investigated both familiarity with computers and compared ISA score across several industry sectors.

4.1.4 Applied Implications.

These findings have both theoretical and practical implications. The results contribute to the theoretical literature by further exploring and addressing a degree of inconsistency relative to age, gender, employment status, familiarity with computers, and industry sector in the context of ISA. In particular, this study has contributed to the literature by addressing a gap relative to the influence of country and providing support for the relationship between ISA and national culture.

In culturally diverse organisations, ignoring the effect of cultural dimensions can have a deleterious impact on the overall organisational information security posture. Thus, the main practical contribution of this study is that information security managers need to know the composition and behavioural orientations of the people receiving security-related training to maximise their effectiveness. It is therefore recommended that multinational organisations and industry practitioners begin to consider the influence of national culture so that future intervention initiatives are adequately informed and can increase the overall information security posture of employees.

Prior to this study, the HAIS-Q had yet to be compared across national culture, which means it was difficult to determine the extent to which ISA varies across nations or cultures, and whether the HAIS-Q can be applied globally. In this study, ISA scores were influenced by national culture, and the HAIS-Q was able to determine this. This provides preliminary evidence for the valid use of the HAIS-Q cross-culturally.

4.2 Limitations and Future Directions

The pre-existing data utilised in this study relies heavily on self-report data collected from employees. Whilst this approach has been common in previous research exploring aspects of ISA, it is important to consider the implications associated with this method. For example, participants may be motivated to bias their responses if their attitudes are not aligned with their organisations' information security policy, if they have a tendency to respond in a socially desirable manner, and if they believe that honest responses might lead to reprimand (Donaldson & Grant-Vallone, 2002; Parsons et al., 2014). Self-report is evidently prone to common method variance and social desirability; however, it allows for convenience, systematisation, repeatability, and comparability. The usefulness of self-reported questionnaires, with the above limitations, has been demonstrated to be an effective approach, especially in the context of ISA (Spector, 1994; Hadlington & Parsons, 2017).

To reduce the effects of the above limitation, data was collected through a third-party organisation (Qualtrics), respondents were not asked to provide their name or the name of their employer, and confidentiality and anonymity were assured and detailed within the Participant Information Sheet. The HAIS-Q has undergone thorough reliability and validity testing, the questions are randomised and reverse scored items are included (in an

attempt to reduce inattentive responding); thus, biased responses were no more prevalent within this study in comparison to past research.

This study has valuable theoretical and applied contributions; the exploration of the relationship between national culture and ISA is novel, however, as a consequence, quantitative methods alone may be insufficient to provide a thorough assessment of this phenomenon. Nevertheless, this approach has allowed for the identification and measure of national culture relative to ISA across two nations – the United Kingdom and Australia. This research has, therefore, addressed the limitations and future research directions suggested by previous researchers (Wiley, McCormac, & Calic, 2019). This study now provides preliminary evidence to justify further investigation into the relationship between national culture and ISA, one where a greater breadth of understanding may be achievable using a mixed methods design.

The use of pre-existing data allowed for the convenience of exploring the influence of country on ISA relative to the national cultures of the United Kingdom and Australia. Whilst this research is viewed as a preliminary investigation into this phenomenon, this study has extended the traditional approach to investigating ISA and diversified this body of literature. As mentioned previously, the United Kingdom is the second largest source of foreign investments in Australia; thus, there is a significant relationship underpinned by closely aligned strategic outlook and interests, substantial trade and investment links, and shared security interests (Australian British Chamber of Commerce, 2019; Department of Foreign Affairs and Trade, 2019). Because of this, the findings from this research hold an important practical element of use for both nations independently and in collaboration with one another. Nonetheless, due to the cultural similarities that these countries share, there are limitations to these findings. The United Kingdom and Australia share small differences on many dimensions of national culture; therefore, it was only possible to make meaningful

comparisons based on two of the six dimensions – Uncertainty avoidance and Long-term orientation. The sample did not include any participants from the highest and the lowest extreme of cultural dimensions, which might have strengthened or weakened the reported findings. Hofstede and colleagues (1990), Schein (2004) and House et al. (2004), have found that Western and Asian countries have profoundly different national cultures. Therefore, utilising the HAIS-Q, future research should aim to examine the relationship between national culture and ISA with more diverse countries, and ideally aim to collect a global sample. Furthermore, instead of assigning national culture scores at the country level, future research could measure the dimensions at the individual level, which can be important in multicultural countries, like Australia.

This research has detailed the level of ISA associated with several industry sectors; however, these findings are not definite and this research path deserves further investigation. This study has demonstrated that it is those industries where the job requires handling of sensitive information which are of particular interest, for example, Finance and Insurance. Since the values in a workplace are influenced by national culture, there might be a key relationship between ISA, industry sector and national culture that is worth considering. For example, while we can discover leading industries in information security, national culture might influence the ability of such industries policy and/or training programs to be leveraged and adopted within multinational organisations. Incorporating this consideration with the evidence relative to individual differences would give multinational organisations and industry practitioners a greater understanding of the factors contributing to the ISA of their employees. In turn, this could influence and inform intervention initiatives relative to the leveraging of good policy, industry-specific training programs, risk analysis modelling, and culture change.

4.3 Conclusion

This study empirically examined a novel relationship between ISA and country, interpreted using Hofstede's framework of national culture. This study also explored five key variables relative to ISA, to eliminate a degree of inconsistency in the literature. A significant relationship was found between ISA and age, gender, percentage of time spent using computer technology, and country. To the author's knowledge, this is the first time a link between ISA and national culture has been noted in the literature. These findings have important theoretical and applied implications. Theoretically, the results of this study help eliminate a degree of inconsistency in the literature and should be further developed by future research to more comprehensively investigate these relationships. From an applied perspective, multinational organisations and industry practitioners may achieve greater employee ISA by incorporating the influence of national culture, so that future intervention initiatives will work towards strengthening all employees' ISA in a more holistic manner.

5. References

Australian British Chamber of Commerce. (2019). The Australia-UK relationship. Retrieved from https://www.britishchamber.com/about-us

Australian Cyber Security Centre (2017). *Cyber Security Survey 2016.* Retrieved from acsc.gov.au/publications/ACSC_Cyber_Security_Survey_2016.pdf

Aurigemma, S., & Panko, R. (2012). A Composite Framework for Behavioral Compliance with Information Security Policies. In Proceedings of the *System Science (HICSS), 2012 45th Hawaii International Conference* (pp. 3248-3257). Wailea, Maui: Hawaii.

Aytes, K., & Connolly, T. (2003). A research model for investigating human behaviour related to computer security. *AMCIS 2003 Proceedings*, 260, 45-60.

Bjöck, J., & Jiang, K.W.B (2006). "Information security and national culture: comparison between ERP systems security implementations in Singapore and Sweden", Master degree thesis, Royal Institute of Technology, Stockholm.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548. doi:10.2307/25750690

Cannon, J.P., Doney, P.M., Mullen, M.R., & Peterson, K.J. (2010). Building long-term orientation in buyer-supplier relationships: the moderating role of culture. *Journal of Operations Management, 28,* 506-521. doi:10.1016/j.jom.2010.02.002

Crossler, R., Johnstron, A.,Lowrr, P., Hu, Q., Warkentin, M., & Baskervill, R. (2013). Future directions for behavioural information security research. *Computers & Security, 32,* 90-101. doi:10.1016/j.cose.2012.09.010

Cronk, L., Salmon, C. (2017). Culture's influence on behaviour: Steps towards a theory. *Evolutionary Behavioural Science, 11,* 36-52. doi:10.1037/ebs0000069

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review: The International Journal of Technology Law and Practice, 31*(2), 243-256. doi:10.1016/j.clsr.2015.01.005

Department of Foreign Affairs and Trade. (2019). United Kingdom country brief. Retrieved from https://dfat.gov.au/geo/united-kingdom/Pages/united-kingdom-country-brief.aspx

Dinev, T., Goo, J., Hu, Q., Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal, 19,* 391-412. doi:10.1111/j.1365-2575.2007.00289.x

Donaldson, S., & Grant-Vallone, E. (2002). Understanding Self-Report Bias in Organizational Behavior Research. *Journal of Business and Psychology, 17*(2), 245-260. doi:10.1023/A:1019637632584

Dols, T., & Silvius A. J. (2010). Exploring the influence of national cultures on non-Compliance behaviour. *Communications of the IIMA, 10,* 11-26. doi:10.1108/13612021211222806

Flores, W., Antonsen, E., & Ekstedt, M. (2014). Inforamtion security knowledge sharing in organisations: investigating the effect of behavioural information security governance and national culture. *Computers & Security, 43,* 90-110. doi: 10.1016/j.cose.2014.03.004

Hadlington, L., & Parsons, K. (2017). Can Cyberloafing and Internet Addiction Affect Organizational Information Security? *Cyberpsychology, Behavior and Social Networking, 20*(9), 567-571. doi:10.1089/cyber.2017.0239

Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I., & Jones, K (2018). Exploring the role of work identity and work locus of control in information security awareness. *Psychology and Technology, 81,* 41-48. doi:10.1016/j.cose.2018.10.006

Hofstede, G., Neuijen, B., Ohayv, D., & Sanders, G. (1990). Measuring organisational cultures: A qualitative study across twenty cases. *Administrative Science Quarterly, 35,* 286-316. doi:10.2307/2393392

Hofstede, G. (1993). Cultural constraints in management theories. *Academy of Management Executive, 7,* 81-94. doi:10.5465/ame.1993.9409142061

Hofstede, G. (2001). *Culture's Consequences: Comparing Values, Behaviours, Institutions and Organisations across Nations,* 2nd edn. Sage Publications, Thousand Oaks, CA, USA.

Hofstede Insights. 2019. Country Comparisons. Retrieved from https://www.hofstede-insights.com/country-comparison/australia,the-uk/

House, R., & Global Leadership Organizational Behavior Effectiveness Research Program. (2004). *Culture, leadership, and organizations: The GLOBE study of 62 societies.* Thousand Oaks, London: SAGE.

Hoy, M.G, & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*, 28-45. doi:10.1080/15252019.2010.10722168

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management, 51,* 69-79. doi:10.1016/j.im.2013.10.001

Ifinedo, P. (2014). The effects of national culture on the assessment of information security threats and controls in financial service industry. *International Journal of Electronic Business Management, 12,* 75-89. doi:10.1057/palgrave.jibs.8400188

International Business Machines Corporation [IMB] Global Technology Service. (2014). *IMB Security Services 2014 cyber security intelligence index: Analysis of cyber-attack and incident data from IMB's worldwide security operations.* Retrieved from ibm.com/developerworks/library/se-cyberindex2014/index.html

Johnston, A.C., & Hale, R. (2009). Effective security through information security governance. *Communications of the ACM, 52,* 126-129. doi:10.1109/MITP.2016.27.

Jung, B., & Lee, H.S. (2001). Security threats to Internet: a Korean multi-industry investigation. *Information and Management, 38,* 487-498. doi:10.1016/S0378-7206(01)00071-4

Kruger, H. A, Drevin, L., Flowerday, S., & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. *Information Security for South Africa, 10,* 1-7. doi:10.1109/ISSA.2011.6027505

Kruger, H., & Kearney, W. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296. doi:10.1016/j.cose.2006.02.008

Laric, M.V., Pitta, D.A., & Katsanis, L.P. (2009). Consumer concerns for healthcare information privacy: A comparison of US and Canadian perspectives. *Research in Healthcare Financial Management, 12,* 93-111. doi:10.1016/j.procs.2015.08.356

McCorman, 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. doi:10.1016/j.chb.2016.11.065

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T, & Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in

responses. *Australasian Journal of Information Systems, 21*, 1-11. doi:10.3127/ajis.v21i0.1697.

McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M. & Pattinson, M. (2016). Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q). *Paper presented at the Australian Conference of Information Systems (ACIS).* Wollongong, Australia.

Myers, M. D., & Tan, F. B. (2002). Beyond models of national culture in information systems research. *Journal of Global Information Management, 10,* 24-32. doi:10.4018/jgim.2002010103

Öğütçü, M., Testik, Ö., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93. doi:10.1016/j.cose.2015.10.002

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. doi:10.1016/j.cose.2013.12.003

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., Caoc, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwanns, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security, 66,* 40-51. doi: 10.1016/j.cose.2017.01.004

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. (2018). *Key findings from the Global State of Information Security Survey 2018. Revitalizing privacy and trust in a data-driven world.* Retrieved from pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/revitalizing-privacy-trust-in-data-driven-world.html

Robey, D., & Rodriguez-Diaz, A. (1989). The organizational and cultural context of systems implementation: Case experience from Latin America. *Information & Management, 17,* 229-239. doi:10.1016/0378-7206(89)90046-3

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., & Herawan, T. (2015). Information security conscious care behaviour formation in organisations. *Computers & Security, 53,* 65-78. doi:10.1016/j.istr.2008.10.006

Schein, E. (2004). *Organizational Culture and Leadership (3rd ed.)*. San Francisco, CA: Jossey-Bass Business & Management Series.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177-191. doi:10.1016/j.istr.2008.10.006

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41. doi:10.1108/09685220010371394

Spector, P. (1994). Using Self-Report Questionnaires in OB Research: A Comment on the Use of a Controversial Method. *Journal of Organizational Behavior, 15*(5), 385-392. doi:10.1002/job.4030150503

Sundqvist, S., Frank, L., Pummalainen, K. (2005). The effect of country characteristics, cultural similarity and adoption timing on the diffusion of wireless communications. *Journal of Business Research, 58,* 107-110. doi:10.1016/S0148-2963(02)00480-0

Van der Linden, S. (2012). Understanding and achieving behavioral 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*. Freiburg: Germany.

Vitell, S.J, King, R., Howie, K., Toti, J.F., Albert, L., Hidalgo, E.R., & Yacout, O. (2015). Spirituality, moral identity, and consumer ethics: a multi-cultural study. *Journal of Business Ethics, 136,* 147-160. doi:10.1007/s10551-015-2626-0

Vitell, S.J., Nwachukwu, S.L., & Barnes, J.H. (1993). The effects of culture on ethical decision-making: an application of Hofstede's typology. *Journal of Business Ethics, 12,* 753-760. doi:10.1007/BF00881307

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23,* 191-198. doi:10.1016/j.cose.2004.01.012

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. doi:10.1016/j.cose.2013.04.004

Wiley, A., McCormac, A., Calic, D. (2019). More than the individual: examining the relationship between culture and information security awareness, *Computer and Security.* Submitted under review.

World Economic Forum. (2018). *World Economic Forum Annual Meeting: Creating a Shared Future in a Fractured World.* Retrieved from http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Yeh, Q., & Chang, A. (2007). Threats and countermeasures for information system security: A cross-industry study, *Information & Management, 44,* 480-491. doi:10.1016/j.im.2007.05.003

Appendices

Appendix A: T-test and Descriptive Statistics for Average HAIS-Q Total Sub Scales Scores by Country

Results of t-test and Descriptive Statistics for Average HAIS-Q Total Sub Scale Scores by Country

	Country						95% CI for Mean Difference		
	Australia			United Kingdom					
	M	SD	n	M	SD	n		t	df
Password Management	37.79	5.6	1544	37.13	6.22	1281	.21, 1.10	2.93**	2620
Email Use	38.06	5.38	1544	35.09	6.19	1281	2.53, 3.40	13.44**	2555
Internet Use	34.87	5.90	1544	33.89	6.08	1281	.53, 1.42	4.31**	2696
Social Media	36.27	5.18	1544	35.58	6.07	1281	.27, 1.11	3.23**	2527
Mobile Computing	38.10	5.47	1544	37.21	6.42	1281	.45, 1.33	3.94**	2528
Information Handling	38.22	5.85	1544	37.21	6.80	1281	.54, 1.48	4.20**	2540
Incident Reporting	36.52	5.32	1544	36.39	5.99	1281	-.29, .55	.60	2585

**p <.001

Appendix B: Journal Guidelines for Submission

Computers & Security

COMPUTERS & SECURITY

The International Source of Innovation for the Information Security and IT Audit Professional

AUTHOR INFORMATION PACK

DESCRIPTION

The official journal of Technical Committee 11 (computer security) of the International Federation for Information Processing.

Computers & Security is the most respected technical journal in the IT security field. With its high profile editorial board and informative regular features and columns, the journal is essential reading for IT security professionals around the world.

Computers & Security provides you with a unique blend of leading edge research and sound practical management advice. It is aimed at the professional involved with computer security, audit, control and data integrity in all sectors - industry, commerce and academia. Recognized worldwide as THE primary source of reference for applied research and technical expertise it is your first step to fully secure systems.

Subscribe today and see the benefits immediately!

- Our cutting edge research will help you secure and maintain the integrity of your systems
- We accept only the highest quality of papers ensuring that you receive the relevant and practical advice you need
- Our editorial board's collective expertise will save you from paying thousands of pounds to IT consultants
- We don't just highlight the threats, we give you the solutions

AUDIENCE

Organizational top and middle management, industrial security officers, computer specialists working in: systems design, implementation and evaluation; computer personnel selection, training and supervision; database development and management; operating systems design and maintenance; applications programming; telecommunications hardware and software development; computer architecture design; computer security, attorneys, accountants and auditors, industrial and personnel psychologists.

IMPACT FACTOR

2017: 2.650 © Clarivate Analytics Journal Citation Reports 2018

ABSTRACTING AND INDEXING

Engineering Index

Computer Science Index

Scopus

Science Citation Index Expanded

Costas Lambrinoudakis, University of Piraeus, Pireaus, Greece

Adam Lee, University of Pittsburgh, Pittsburgh, Ohio, USA

Heather Lipford, UNC Charlotte, North Carolina, USA

Thomas Longstaff, Johns Hopkins University, Laurel, Maryland, USA

Javier Lopez, Universidad de Málaga, Malaga, Spain

J Todd McDonald, University of South Alabama, Mobile, Alabama, USA

Stig Frode Mjølsnes, Norwegian University of Science & Technology NTNU, Trondheim, Norway

Tatsuya Mori, Waseda University, Japan

David Naccache, Centre National de la Recherche Scientifique (CNRS), Paris, France

Kai Rannenberg, Goethe University, Frankfurt, Germany

Golden Richard III, Louisiana State University, Louisiana, USA

Basit Shafiq, Lahore University of Management Sciences (LUMS), Lahore, Pakistan

Seungwon Shin, Korea Advanced Institute of Science and Technology (KAIST)

Juan Tapiador, Universidad Carlos III de Madrid, Madrid, Spain

Jaideep Vaidya, Rutgers University, Newark, New Jersey, USA

Wendy Hui Wang, Stevens Institute of Technology, Hoboken, New Jersey, USA

Wei Wang, Beijing Jiaotong University, Beijing, China

Edgar R. Weippl, SBA Research, Vienna, Austria

Christos Xenakis, University of Piraeus, Pireaus, Greece

Alec Yasinsac, University of South Alabama, Mobile, Alabama, USA

Ting Yu, Qatar Computing Research Institute, Doha, Qatar

Stefano Zanero, Politecnico di Milano, Milan, Italy

Zonghua Zhang, Institut Mines-Télécom/TELECOM Lille, Villeneuve-d'Ascq, France

GUIDE FOR AUTHORS

Your Paper Your Way

We now differentiate between the requirements for new and revised submissions. You may choose to submit your manuscript as a single Word or PDF file to be used in the refereeing process. Only when your paper is at the revision stage, will you be requested to put your paper in to a 'correct format' for acceptance and provide the items required for the publication of your article.

Computers & Security is the most comprehensive, authoritative survey of the key issues in computer security today. It aims to satisfy the needs of managers and experts involved in the computer security field by providing a combination of leading edge research developments, innovations and sound practical management advice for computer security professionals worldwide. Computers & Security provides detailed information to the professional involved with computer security, audit, control and data integrity in all sectors – industry, commerce and academia.

Submissions

Original submissions on all computer security topics are welcomed, especially those of practical benefit to the computer security practitioner.
From 1 April 2006, submissions with cryptology theory as their primary subject matter will no longer be accepted by Computers & Security as anything other than invited contributions. Authors submitting papers that feature cryptologic results as an important supporting feature should ensure that the paper, as a whole, is of importance to the advanced security practitioner or researcher, and ensure that the paper advances the overall field in a significant manner. Authors who submit purely theoretical papers on cryptology may be advised to resubmit them to a more appropriate journal; the Editorial Board reserves the right to reject such papers without the full reviewing process. Cryptography papers submitted before this date will be subject to the usual reviewing process, should the paper pass the pre-review process which has been in place since 2004.

All contributions should be in English and, since the readership of the journal is international, authors are reminded that simple, concise sentences are our preferred style. It is also suggested that papers are spellchecked and, if necessary, proofread by a native English speaker in order to avoid grammatical errors. All technical terms that may not be clear to the reader should be clearly explained.

Copyright is retained by the Publisher. Submission of an article implies that the paper has not been published previously; that it is not under consideration for publication elsewhere; that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out; and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.
All papers will be submitted to expert referees from the editorial board for review. The usual size of a paper is 5000 to 10 000 words.

You can use this list to carry out a final check of your submission before you send it to the journal for review. Please check the relevant section in this Guide for Authors for more details.

Ensure that the following items are present:

One author has been designated as the corresponding author with contact details:

• E-mail address
• Full postal address

All necessary files have been uploaded:
Manuscript:
• Include keywords
• All figures (include relevant captions)
• All tables (including titles, description, footnotes)
• Ensure all figure and table citations in the text match the files provided
• Indicate clearly if color should be used for any figures in print
Graphical Abstracts / Highlights files (where applicable)
Supplemental files (where applicable)

Further considerations
• Manuscript has been 'spell checked' and 'grammar checked'. Our system also automatically adds line numbers to the PDF
• All references mentioned in the Reference List are cited in the text, and vice versa
• Permission has been obtained for use of copyrighted material from other sources (including the Internet)
• Relevant declarations of interest have been made
• Journal policies detailed in this guide have been reviewed
• Referee suggestions and contact details provided, based on journal requirements

For further information, visit our Support Center.

SUBMISSIONS: BEFORE YOU BEGIN

Ethics in publishing

Please see our information pages on Ethics in publishing and Ethical guidelines for journal publication.

Declaration of interest

All authors must disclose any financial and personal relationships with other people or organizations that could inappropriately influence (bias) their work. Examples of potential competing interests include employment, consultancies, stock ownership, honoraria, paid expert testimony, patent applications/registrations, and grants or other funding. Authors must disclose any interests in two places: 1. A summary declaration of interest statement in the title page file (if double-blind) or the manuscript file (if single-blind). If there are no interests to declare then please state this: 'Declarations of interest: none'. This summary statement will be ultimately published if the article is accepted. 2. Detailed disclosures as part of a separate Declaration of Interest form, which forms part of the journal's official records. It is important for potential interests to be declared in both places and that the information matches. More information.

Submission declaration and verification

Submission of an article implies that the work described has not been published previously (except in the form of an abstract, a published lecture or academic thesis, see 'Multiple,

redundant or concurrent publication' for more information), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. To verify originality, your article may be checked by the originality detection service Crossref Similarity Check.

Preprints

Please note that preprints can be shared anywhere at any time, in line with Elsevier's sharing policy. Sharing your preprints e.g. on a preprint server will not count as prior publication (see 'Multiple, redundant or concurrent publication' for more information).

Use of inclusive language

Inclusive language acknowledges diversity, conveys respect to all people, is sensitive to differences, and promotes equal opportunities. Articles should make no assumptions about the beliefs or commitments of any reader, should contain nothing which might imply that one individual is superior to another on the grounds of race, sex, culture or any other characteristic, and should use inclusive language throughout. Authors should ensure that writing is free from bias, for instance by using 'he or she', 'his/her' instead of 'he' or 'his', and by making use of job titles that are free of stereotyping (e.g. 'chairperson' instead of 'chairman' and 'flight attendant' instead of 'stewardess').

Contributors

Each author is required to declare his or her individual contribution to the article: all authors must have materially participated in the research and/or article preparation, so roles for all authors should be described. The statement that all authors have approved the final article should be true and included in the disclosure.

Changes to authorship

Authors are expected to consider carefully the list and order of authors **before** submitting their manuscript and provide the definitive list of authors at the time of the original submission. Any addition, deletion or rearrangement of author names in the authorship list should be made only **before** the manuscript has been accepted and only if approved by the journal Editor. To request such a change, the Editor must receive the following from the **corresponding author**: (a) the reason for the change in author list and (b) written confirmation (e-mail, letter) from all authors that they agree with the addition, removal or rearrangement. In the case of addition or removal of authors, this includes confirmation from the author being added or removed.
Only in exceptional circumstances will the Editor consider the addition, deletion or rearrangement of authors **after** the manuscript has been accepted. While the Editor considers the request, publication of the manuscript will be suspended. If the manuscript has already been published in an online issue, any requests approved by the Editor will result in a corrigendum.

Copyright

Upon acceptance of an article, authors will be asked to complete a 'Journal Publishing Agreement' (see more information on this). An e-mail will be sent to the corresponding author confirming receipt of the manuscript together with a 'Journal Publishing Agreement' form or a link to the online version of this agreement.

Subscribers may reproduce tables of contents or prepare lists of articles including abstracts for internal circulation within their institutions. Permission of the Publisher is required for resale or distribution outside the institution and for all other derivative works, including compilations and translations. If excerpts from other copyrighted works are included, the author(s) must obtain written permission from the copyright owners and credit the source(s) in the article. Elsevier has preprinted forms for use by authors in these cases.

For gold open access articles: Upon acceptance of an article, authors will be asked to complete an 'Exclusive License Agreement' (more information). Permitted third party reuse of gold open access articles is determined by the author's choice of user license.

Author rights
As an author you (or your employer or institution) have certain rights to reuse your work. More information.

Elsevier supports responsible sharing
Find out how you can share your research published in Elsevier journals.

Role of the funding source

You are requested to identify who provided financial support for the conduct of the research and/or preparation of the article and to briefly describe the role of the sponsor(s), if any, in study design; in the collection, analysis and interpretation of data; in the writing of the report; and in the decision to submit the article for publication. If the funding source(s) had no such involvement then this should be stated.

Funding body agreements and policies
Elsevier has established a number of agreements with funding bodies which allow authors to comply with their funder's open access policies. Some funding bodies will reimburse the author for the gold open access publication fee. Details of existing agreements are available online.

Open access

This journal offers authors a choice in publishing their research:

Subscription
• Articles are made available to subscribers as well as developing countries and patient groups through our universal access programs.
• No open access publication fee payable by authors.
• The Author is entitled to post the accepted manuscript in their institution's repository and make this public after an embargo period (known as green Open Access). The published journal article cannot be shared publicly, for example on ResearchGate or Academia.edu, to ensure the sustainability of peer-reviewed research in journal publications. The embargo period for this journal can be found below.
Gold open access
• Articles are freely available to both subscribers and the wider public with permitted reuse.
• A gold open access publication fee is payable by authors or on their behalf, e.g. by their research funder or institution.

Regardless of how you choose to publish your article, the journal will apply the same peer review criteria and acceptance standards.

For gold open access articles, permitted third party (re)use is defined by the following Creative Commons user licenses:

Creative Commons Attribution (CC BY)
Lets others distribute and copy the article, create extracts, abstracts, and other revised versions, adaptations or derivative works of or from an article (such as a translation), include in a collective work (such as an anthology), text or data mine the article, even for commercial purposes, as long as they credit the author(s), do not represent the author as endorsing their adaptation of the article, and do not modify the article in such a way as to damage the author's honor or reputation.

Creative Commons Attribution-Non Commercial-No Derivs (CC BY-NC-ND)
For non-commercial purposes, lets others distribute and copy the article, and to include in a collective work (such as an anthology), as long as they credit the author(s) and provided they do not alter or modify the article.

The gold open access publication fee for this journal is **USD 2600**, excluding taxes. Learn more about Elsevier's pricing policy: https://www.elsevier.com/openaccesspricing.

Green open access
Authors can share their research in a variety of different ways and Elsevier has a number of green open access options available. We recommend authors see our green open access page for further information. Authors can also self-archive their manuscripts immediately and enable public access from their institution's repository after an embargo period. This is the version that has been accepted for publication and which typically includes author-incorporated changes suggested during submission, peer review and in editor-author communications. Embargo period: For subscription articles, an appropriate amount of time is needed for journals to deliver value to subscribing customers before an article becomes freely available to the public. This is the embargo period and it begins from the date the article is formally published online in its final and fully citable form. Find out more.

This journal has an embargo period of 24 months.

Elsevier Researcher Academy
Researcher Academy is a free e-learning platform designed to support early and mid-career researchers throughout their research journey. The "Learn" environment at Researcher Academy offers several interactive modules, webinars, downloadable guides and resources to guide you through the process of writing for research and going through peer review. Feel free to use these free resources to improve your submission and navigate the publication process with ease.

Language (usage and editing services)
Please write your text in good English (American or British usage is accepted, but not a mixture of these). Authors who feel their English language manuscript may require editing to eliminate possible grammatical or spelling errors and to conform to correct scientific English may wish to use the English Language Editing service available from Elsevier's WebShop.

Submission

Our online submission system guides you stepwise through the process of entering your article details and uploading your files. The system converts your article files to a single PDF file used in the peer-review process. Editable files (e.g., Word, LaTeX) are required to typeset your article for final publication. All correspondence, including notification of the Editor's decision and requests for revision, is sent by e-mail.

Referees
Please submit the names and institutional e-mail addresses of several potential referees. For more details, visit our Support site. Note that the editor retains the sole right to decide whether or not the suggested reviewers are used.

PREPARATION

NEW SUBMISSIONS

Submission to this journal proceeds totally online and you will be guided stepwise through the creation and uploading of your files. The system automatically converts your files to a single PDF file, which is used in the peer-review process.

As part of the Your Paper Your Way service, you may choose to submit your manuscript as a single file to be used in the refereeing process. This can be a PDF file or a Word document, in any format or lay-out that can be used by referees to evaluate your manuscript. It should contain high enough quality figures for refereeing. If you prefer to do so, you may still provide all or some of the source files at the initial submission. Please note that individual figure files larger than 10 MB must be uploaded separately.

There are no strict requirements on reference formatting at submission. References can be in any style or format as long as the style is consistent. Where applicable, author(s) name(s), journal title/book title, chapter title/article title, year of publication, volume number/book chapter and the pagination must be present. Use of DOI is highly encouraged. The reference style used by the journal '4 Vancouver name/year' will be applied to the accepted article by Elsevier at the proof stage. Note that missing data will be highlighted at proof stage for the author to correct.

Formatting requirements
There are no strict formatting requirements but all manuscripts must contain the essential elements needed to convey your manuscript, for example Abstract, Keywords, Introduction, Materials and Methods, Results, Conclusions, Artwork and Tables with Captions.
If your article includes any Videos and/or other Supplementary material, this should be included in your initial submission for peer review purposes.
Divide the article into clearly defined sections.

Figures and tables embedded in text
Please ensure the figures and the tables included in the single file are placed next to the relevant text in the manuscript, rather than at the bottom or the top of the file. The corresponding caption should be placed directly below the figure or table.

Peer review

This journal operates a single blind review process. All contributions will be initially assessed by the editor for suitability for the journal. Papers deemed suitable are then typically sent to a minimum of two independent expert reviewers to assess the scientific quality of the paper. The Editor is responsible for the final decision regarding acceptance or rejection of articles. The Editor's decision is final. More information on types of peer review.

REVISED SUBMISSIONS

Use of word processing software
Regardless of the file format of the original submission, at revision you must provide us with an editable file of the entire article. Keep the layout of the text as simple as possible. Most formatting codes will be removed and replaced on processing the article. The electronic text should be prepared in a way very similar to that of conventional manuscripts (see also the Guide to Publishing with Elsevier). See also the section on Electronic artwork.
To avoid unnecessary errors you are strongly advised to use the 'spell-check' and 'grammar-check' functions of your word processor.

Article structure

Subdivision - numbered sections
Divide your article into clearly defined and numbered sections. Subsections should be numbered 1.1 (then 1.1.1, 1.1.2, ...), 1.2, etc. (the abstract is not included in section numbering). Use this numbering also for internal cross-referencing: do not just refer to 'the text'. Any subsection may be given a brief heading. Each heading should appear on its own separate line.

Introduction
State the objectives of the work and provide an adequate background, avoiding a detailed literature survey or a summary of the results.

Material and methods
Provide sufficient details to allow the work to be reproduced by an independent researcher. Methods that are already published should be summarized, and indicated by a reference. If quoting directly from a previously published method, use quotation marks and also cite the source. Any modifications to existing methods should also be described.

Theory/calculation
A Theory section should extend, not repeat, the background to the article already dealt with in the Introduction and lay the foundation for further work. In contrast, a Calculation section represents a practical development from a theoretical basis.

Results
Results should be clear and concise.

Discussion
This should explore the significance of the results of the work, not repeat them. A combined Results and Discussion section is often appropriate. Avoid extensive citations and discussion of published literature.

Conclusions
The main conclusions of the study may be presented in a short Conclusions section, which may stand alone or form a subsection of a Discussion or Results and Discussion section.

Appendices
If there is more than one appendix, they should be identified as A, B, etc. Formulae and equations in appendices should be given separate numbering: Eq. (A.1), Eq. (A.2), etc.; in a subsequent appendix, Eq. (B.1) and so on. Similarly for tables and figures: Table A.1; Fig. A.1, etc.

Vitae

For Full Length Articles a Biographical Sketch for each author (50-100 words) is required.

Essential title page information

• ***Title.*** Concise and informative. Titles are often used in information-retrieval systems. Avoid abbreviations and formulae where possible.
• ***Author names and affiliations.*** Please clearly indicate the given name(s) and family name(s) of each author and check that all names are accurately spelled. You can add your name between parentheses in your own script behind the English transliteration. Present the authors' affiliation addresses (where the actual work was done) below the names. Indicate all affiliations with a lower-case superscript letter immediately after the author's name and in front of the appropriate address. Provide the full postal address of each affiliation, including the country name and, if available, the e-mail address of each author.
• ***Corresponding author.*** Clearly indicate who will handle correspondence at all stages of refereeing and publication, also post-publication. This responsibility includes answering any future queries about Methodology and Materials. **Ensure that the e-mail address is given and that contact details are kept up to date by the corresponding author.**
• ***Present/permanent address.*** If an author has moved since the work described in the article was done, or was visiting at the time, a 'Present address' (or 'Permanent address') may be indicated as a footnote to that author's name. The address at which the author actually did the work must be retained as the main, affiliation address. Superscript Arabic numerals are used for such footnotes.

Abstract

A concise and factual abstract is required. The abstract should state briefly the purpose of the research, the principal results and major conclusions. An abstract is often presented separately from the article, so it must be able to stand alone. For this reason, References should be avoided, but if essential, then cite the author(s) and year(s). Also, non-standard or uncommon abbreviations should be avoided, but if essential they must be defined at their first mention in the abstract itself.

Graphical abstract

Although a graphical abstract is optional, its use is encouraged as it draws more attention to the online article. The graphical abstract should summarize the contents of the article in a concise, pictorial form designed to capture the attention of a wide readership. Graphical abstracts should be submitted as a separate file in the online submission system. Image size: Please provide an image with a minimum of 531 × 1328 pixels (h × w) or proportionally more. The image should be readable at a size of 5 × 13 cm using a regular screen resolution of 96 dpi. Preferred file types: TIFF, EPS, PDF or MS Office files. You can view Example Graphical Abstracts on our information site.
Authors can make use of Elsevier's Illustration Services to ensure the best presentation of their images and in accordance with all technical requirements.

Highlights

Highlights are a short collection of bullet points that convey the core findings of the article. Highlights are optional and should be submitted in a separate editable file in the online submission system. Please use 'Highlights' in the file name and include 3 to 5 bullet points (maximum 85 characters, including spaces, per bullet point). You can view example Highlights on our information site.

Keywords

Immediately after the abstract, provide 5-10 keywords, avoiding general and plural terms and multiple concepts (avoid, for example, "and", "of"). Be sparing with abbreviations: only abbreviations firmly established in the field may be eligible. These keywords will be used for indexing purposes.

Abbreviations

Define abbreviations that are not standard in this field in a footnote to be placed on the first page of the article. Such abbreviations that are unavoidable in the abstract must be defined at their first mention there, as well as in the footnote. Ensure consistency of abbreviations throughout the article.

Acknowledgements

Collate acknowledgements in a separate section at the end of the article before the references and do not, therefore, include them on the title page, as a footnote to the title or otherwise. List here those individuals who provided help during the research (e.g., providing language help, writing assistance or proof reading the article, etc.).

Formatting of funding sources

List funding sources in this standard way to facilitate compliance to funder's requirements:

Funding: This work was supported by the National Institutes of Health [grant numbers xxxx, yyyy]; the Bill & Melinda Gates Foundation, Seattle, WA [grant number zzzz]; and the United States Institutes of Peace [grant number aaaa].

It is not necessary to include detailed descriptions on the program or type of grants and awards. When funding is from a block grant or other resources available to a university, college, or other research institution, submit the name of the institute or organization that provided the funding.

If no funding has been provided for the research, please include the following sentence:

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Math formulae

Please submit math equations as editable text and not as images. Present simple formulae in line with normal text where possible and use the solidus (/) instead of a horizontal line for small fractional terms, e.g., X/Y. In principle, variables are to be presented in italics. Powers of e are often more conveniently denoted by exp. Number consecutively any equations that have to be displayed separately from the text (if referred to explicitly in the text).

Footnotes

Footnotes should be used sparingly. Number them consecutively throughout the article. Many word processors build footnotes into the text, and this feature may be used. Should this not be the case, indicate the position of footnotes in the text and present the footnotes themselves separately at the end of the article.

Artwork

Electronic artwork

General points

• Make sure you use uniform lettering and sizing of your original artwork.

• Preferred fonts: Arial (or Helvetica), Times New Roman (or Times), Symbol, Courier.
• Number the illustrations according to their sequence in the text.
• Use a logical naming convention for your artwork files.
• Indicate per figure if it is a single, 1.5 or 2-column fitting image.
• For Word submissions only, you may still provide figures and their captions, and tables within a single file at the revision stage.
• Please note that individual figure files larger than 10 MB must be provided in separate source files.
A detailed guide on electronic artwork is available.
You are urged to visit this site; some excerpts from the detailed information are given here.
Formats
Regardless of the application used, when your electronic artwork is finalized, please 'save as' or convert the images to one of the following formats (note the resolution requirements for line drawings, halftones, and line/halftone combinations given below):
EPS (or PDF): Vector drawings. Embed the font or save the text as 'graphics'.
TIFF (or JPG): Color or grayscale photographs (halftones): always use a minimum of 300 dpi.
TIFF (or JPG): Bitmapped line drawings: use a minimum of 1000 dpi.
TIFF (or JPG): Combinations bitmapped line/half-tone (color or grayscale): a minimum of 500 dpi is required.
Please do not:
• Supply files that are optimized for screen use (e.g., GIF, BMP, PICT, WPG); the resolution is too low.
• Supply files that are too low in resolution.
• Submit graphics that are disproportionately large for the content.

Color artwork
Please make sure that artwork files are in an acceptable format (TIFF (or JPEG), EPS (or PDF), or MS Office files) and with the correct resolution. If, together with your accepted article, you submit usable color figures then Elsevier will ensure, at no additional charge, that these figures will appear in color online (e.g., ScienceDirect and other sites) regardless of whether or not these illustrations are reproduced in color in the printed version. **For color reproduction in print, you will receive information regarding the costs from Elsevier after receipt of your accepted article**. Please indicate your preference for color: in print or online only. Further information on the preparation of electronic artwork.

Figure captions
Ensure that each illustration has a caption. A caption should comprise a brief title (**not** on the figure itself) and a description of the illustration. Keep text in the illustrations themselves to a minimum but explain all symbols and abbreviations used.

Tables

Please submit tables as editable text and not as images. Tables can be placed either next to the relevant text in the article, or on separate page(s) at the end. Number tables consecutively in accordance with their appearance in the text and place any table notes below the table body. Be sparing in the use of tables and ensure that the data presented in them do not duplicate results described elsewhere in the article. Please avoid using vertical rules and shading in table cells.

References

Citation in text
Please ensure that every reference cited in the text is also present in the reference list (and vice versa). Any references cited in the abstract must be given in full. Unpublished results and personal communications are not recommended in the reference list, but may be mentioned in the text. If these references are included in the reference list they should follow the standard reference style of the journal and should include a substitution of the publication date with either 'Unpublished results' or 'Personal communication'. Citation of a reference as 'in press' implies that the item has been accepted for publication.

Reference links
Increased discoverability of research and high quality peer review are ensured by online links to the sources cited. In order to allow us to create links to abstracting and indexing services, such as Scopus, CrossRef and PubMed, please ensure that data provided in the references are correct. Please note that incorrect surnames, journal/book titles, publication year and pagination may prevent link creation. When copying references, please be careful as they may already contain errors. Use of the DOI is highly encouraged.

A DOI is guaranteed never to change, so you can use it as a permanent link to any electronic article. An example of a citation using DOI for an article not yet in an issue is: VanDecar J.C., Russo R.M., James D.E., Ambeh W.B., Franke M. (2003). Aseismic continuation of the Lesser Antilles slab beneath northeastern Venezuela. Journal of Geophysical Research, https://doi.org/10.1029/2001JB000884. Please note the format of such citations should be in the same style as all other references in the paper.

Web references
As a minimum, the full URL should be given and the date when the reference was last accessed. Any further information, if known (DOI, author names, dates, reference to a source publication, etc.), should also be given. Web references can be listed separately (e.g., after the reference list) under a different heading if desired, or can be included in the reference list.

Data references
This journal encourages you to cite underlying or relevant datasets in your manuscript by citing them in your text and including a data reference in your Reference List. Data references should include the following elements: author name(s), dataset title, data repository, version (where available), year, and global persistent identifier. Add [dataset] immediately before the reference so we can properly identify it as a data reference. The [dataset] identifier will not appear in your published article.

References in a special issue
Please ensure that the words 'this issue' are added to any references in the list (and any citations in the text) to other articles in the same Special Issue.

Reference management software
Most Elsevier journals have their reference template available in many of the most popular reference management software products. These include all products that support Citation Style Language styles, such as Mendeley and Zotero, as well as EndNote. Using the word processor plug-ins from these products, authors only need to select the appropriate journal template when preparing their article, after which citations and bibliographies will be automatically formatted in the journal's style. If no template is yet available for this journal, please follow the format of the sample references and citations as shown in this Guide. If you use reference management software, please ensure that you remove all field codes before

submitting the electronic manuscript. More information on how to remove field codes.

Users of Mendeley Desktop can easily install the reference style for this journal by clicking the following link:
http://open.mendeley.com/use-citation-style/computers-and-security
When preparing your manuscript, you will then be able to select this style using the Mendeley plug-ins for Microsoft Word or LibreOffice.

Reference formatting
There are no strict requirements on reference formatting at submission. References can be in any style or format as long as the style is consistent. Where applicable, author(s) name(s), journal title/book title, chapter title/article title, year of publication, volume number/book chapter and the article number or pagination must be present. Use of DOI is highly encouraged. The reference style used by the journal will be applied to the accepted article by Elsevier at the proof stage. Note that missing data will be highlighted at proof stage for the author to correct. If you do wish to format the references yourself they should be arranged according to the following examples:

Reference formatting
There are no strict requirements on reference formatting at submission. References can be in any style or format as long as the style is consistent. Where applicable, author(s) name(s), journal title/book title, chapter title/article title, year of publication, volume number/book chapter and the pagination must be present. Use of DOI is highly encouraged. The reference style used by the journal '4 Vancouver name/year' will be applied to the accepted article by Elsevier at the proof stage. Note that missing data will be highlighted at proof stage for the author to correct. If you do wish to format the references yourself they should be arranged according to the following examples:

Reference style
Text: All citations in the text should refer to:
1. *Single author:* the author's name (without initials, unless there is ambiguity) and the year of publication;
2. *Two authors:* both authors' names and the year of publication;
3. *Three or more authors:* first author's name followed by 'et al.' and the year of publication.
Citations may be made directly (or parenthetically). Groups of references can be listed either first alphabetically, then chronologically, or vice versa.
Examples: 'as demonstrated (Allan, 2000a, 2000b, 1999; Allan and Jones, 1999).... Or, as demonstrated (Jones, 1999; Allan, 2000)... Kramer et al. (2010) have recently shown ...'
List: References should be arranged first alphabetically and then further sorted chronologically if necessary. More than one reference from the same author(s) in the same year must be identified by the letters 'a', 'b', 'c', etc., placed after the year of publication.
Examples:
Reference to a journal publication:
Van der Geer J, Hanraads JAJ, Lupton RA. The art of writing a scientific article. J Sci Commun 2010;163:51–9. https://doi.org/10.1016/j.Sc.2010.00372.
Reference to a journal publication with an article number:
Van der Geer J, Hanraads JAJ, Lupton RA. The art of writing a scientific article. Heliyon. 2018;19:e00205. https://doi.org/10.1016/j.heliyon.2018.e00205.
Reference to a book:
Strunk Jr W, White EB. The elements of style. 4th ed. New York: Longman; 2000.
Reference to a chapter in an edited book:
Mettam GR, Adams LB. How to prepare an electronic version of your article. In: Jones BS, Smith RZ, editors. Introduction to the electronic age. New York: E-Publishing Inc; 2009. p. 281–304.
Reference to a website:

Cancer Research UK, Cancer statistics reports for the UK.
http://www.cancerresearchuk.org/aboutcancer/statistics/cancerstatsreport/, 2003 (accessed 13 March 2003).
Reference to a dataset:
[dataset] Oguro M, Imahiro S, Saito S, Nakashizuka T. Mortality data for Japanese oak wilt disease and surrounding forest compositions, Mendeley Data, v1; 2015.
https://doi.org/10.17632/xwj98nb39r.1.
Note shortened form for last page number. e.g., 51–9, and that for more than 6 authors the first 6 should be listed followed by "et al." For further details you are referred to "Uniform Requirements for Manuscripts submitted to Biomedical Journals" (J Am Med Assoc 1997;277:927–34) (see also Samples of Formatted References).

Journal abbreviations source
Journal names should be abbreviated according to the List of Title Word Abbreviations.

Video

Elsevier accepts video material and animation sequences to support and enhance your scientific research. Authors who have video or animation files that they wish to submit with their article are strongly encouraged to include links to these within the body of the article. This can be done in the same way as a figure or table by referring to the video or animation content and noting in the body text where it should be placed. All submitted files should be properly labeled so that they directly relate to the video file's content. . In order to ensure that your video or animation material is directly usable, please provide the file in one of our recommended file formats with a preferred maximum size of 150 MB per file, 1 GB in total. Video and animation files supplied will be published online in the electronic version of your article in Elsevier Web products, including ScienceDirect. Please supply 'stills' with your files: you can choose any frame from the video or animation or make a separate image. These will be used instead of standard icons and will personalize the link to your video data. For more detailed instructions please visit our video instruction pages. Note: since video and animation cannot be embedded in the print version of the journal, please provide text for both the electronic and the print version for the portions of the article that refer to this content.

Data visualization

Include interactive data visualizations in your publication and let your readers interact and engage more closely with your research. Follow the instructions hereto find out about available data visualization options and how to include them with your article.

Supplementary material

Supplementary material such as applications, images and sound clips, can be published with your article to enhance it. Submitted supplementary items are published exactly as they are received (Excel or PowerPoint files will appear as such online). Please submit your material together with the article and supply a concise, descriptive caption for each supplementary file. If you wish to make changes to supplementary material during any stage of the process, please make sure to provide an updated file. Do not annotate any corrections on a previous version. Please switch off the 'Track Changes' option in Microsoft Office files as these will appear in the published version.

Research data

This journal encourages and enables you to share data that supports your research publication where appropriate, and enables you to interlink the data with your published

articles. Research data refers to the results of observations or experimentation that validate research findings. To facilitate reproducibility and data reuse, this journal also encourages you to share your software, code, models, algorithms, protocols, methods and other useful materials related to the project.

Below are a number of ways in which you can associate data with your article or make a statement about the availability of your data when submitting your manuscript. If you are sharing data in one of these ways, you are encouraged to cite the data in your manuscript and reference list. Please refer to the "References" section for more information about data citation. For more information on depositing, sharing and using research data and other relevant research materials, visit the research data page.

Data linking
If you have made your research data available in a data repository, you can link your article directly to the dataset. Elsevier collaborates with a number of repositories to link articles on ScienceDirect with relevant repositories, giving readers access to underlying data that gives them a better understanding of the research described.

There are different ways to link your datasets to your article. When available, you can directly link your dataset to your article by providing the relevant information in the submission system. For more information, visit the database linking page.

For supported data repositories a repository banner will automatically appear next to your published article on ScienceDirect.

In addition, you can link to relevant data or entities through identifiers within the text of your manuscript, using the following format: Database: xxxx (e.g., TAIR: AT1G01020; CCDC: 734053; PDB: 1XFN).

Mendeley Data
This journal supports Mendeley Data, enabling you to deposit any research data (including raw and processed data, video, code, software, algorithms, protocols, and methods) associated with your manuscript in a free-to-use, open access repository. During the submission process, after uploading your manuscript, you will have the opportunity to upload your relevant datasets directly to *Mendeley Data*. The datasets will be listed and directly accessible to readers next to your published article online.

For more information, visit the Mendeley Data for journals page.

Data in Brief
You have the option of converting any or all parts of your supplementary or additional raw data into one or multiple data articles, a new kind of article that houses and describes your data. Data articles ensure that your data is actively reviewed, curated, formatted, indexed, given a DOI and publicly available to all upon publication. You are encouraged to submit your article for *Data in Brief* as an additional item directly alongside the revised version of your manuscript. If your research article is accepted, your data article will automatically be transferred over to *Data in Brief* where it will be editorially reviewed and published in the open access data journal, *Data in Brief*. Please note an open access fee of 500 USD is payable for publication in *Data in Brief*. Full details can be found on the Data in Brief website. Please use this template to write your Data in Brief.

MethodsX
You have the option of converting relevant protocols and methods into one or multiple MethodsX articles, a new kind of article that describes the details of customized research

methods. Many researchers spend a significant amount of time on developing methods to fit their specific needs or setting, but often without getting credit for this part of their work. MethodsX, an open access journal, now publishes this information in order to make it searchable, peer reviewed, citable and reproducible. Authors are encouraged to submit their MethodsX article as an additional item directly alongside the revised version of their manuscript. If your research article is accepted, your methods article will automatically be transferred over to MethodsX where it will be editorially reviewed. Please note an open access fee is payable for publication in MethodsX. Full details can be found on the MethodsX website. Please use this template to prepare your MethodsX article.

Data statement
To foster transparency, we encourage you to state the availability of your data in your submission. This may be a requirement of your funding body or institution. If your data is unavailable to access or unsuitable to post, you will have the opportunity to indicate why during the submission process, for example by stating that the research data is confidential. The statement will appear with your published article on ScienceDirect. For more information, visit the Data Statement page.

AFTER ACCEPTANCE

Online proof correction

Corresponding authors will receive an e-mail with a link to our online proofing system, allowing annotation and correction of proofs online. The environment is similar to MS Word: in addition to editing text, you can also comment on figures/tables and answer questions from the Copy Editor. Web-based proofing provides a faster and less error-prone process by allowing you to directly type your corrections, eliminating the potential introduction of errors.
If preferred, you can still choose to annotate and upload your edits on the PDF version. All instructions for proofing will be given in the e-mail we send to authors, including alternative methods to the online version and PDF.
We will do everything possible to get your article published quickly and accurately. Please use this proof only for checking the typesetting, editing, completeness and correctness of the text, tables and figures. Significant changes to the article as accepted for publication will only be considered at this stage with permission from the Editor. It is important to ensure that all corrections are sent back to us in one communication. Please check carefully before replying, as inclusion of any subsequent corrections cannot be guaranteed. Proofreading is solely your responsibility.

Offprints

The corresponding author will, at no cost, receive a customized Share Linkproviding 50 days free access to the final published version of the article on ScienceDirect. The Share Link can be used for sharing the article via any communication channel, including email and social media. For an extra charge, paper offprints can be ordered via the offprint order form which is sent once the article is accepted for publication. Both corresponding and co-authors may order offprints at any time via Elsevier's Webshop. Corresponding authors who have published their article gold open access do not receive a Share Link as their final published version of the article is available open access on ScienceDirect and can be shared through the article DOI link.