Computers & Security 88 (2020) 101640

Contents lists available at ScienceDirect

Computers & Security

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

More than the individual: Examining the relationship between culture and Information Security Awareness

Ashleigh Wiley[a,*], Agata McCormac[b], Dragana Calic[b]

[a] The University of Adelaide, SA 5005, Australia
[b] Defence Science & Technology Group, Third Ave, Edinburgh SA 5111, Australia

ARTICLE INFO

Article history:
Received 15 April 2019
Revised 18 September 2019
Accepted 7 October 2019
Available online 14 October 2019

Keywords:
Security culture
Organisational culture
Information Security Awareness (ISA)
Information Security (InfoSec)
Cyber security
Organisational behaviour

ABSTRACT

The relationship between security culture and Information Security Awareness (ISA) has received preliminary support; however, its interplay with organisational culture is yet to be empirically investigated. Therefore, this study explored the relationship between ISA, organisational culture, and security culture. A total of 508 working Australians completed an online questionnaire. ISA was measured using the Human Aspects of Information Security Questionnaire (HAIS-Q); organisational culture was measured using the Denison Organisational Culture Survey (DOCS); and security culture was assessed through the Organisational Security Culture Measure. Our results showed that while organisational culture and security culture were correlated with ISA, security culture played an important mediating relationship between organisational culture and ISA. This suggests that organisations should focus on security culture rather than organisational culture to improve ISA, saving time and resources. Future research could further extend current findings by also considering national culture.

1. Introduction

Human behaviour is largely determined by culture, affecting interactions in everyday social and work environments (Cronk and Salmon, 2017). Therefore, when attempting to understand and shape human behaviour, looking at an individual in isolation is problematic. It is also important to consider the group, the broader social and organisational systems, and their interactions (Tessem and Skaraas, 2005). This is important for information security, as people play a significant role in not only creating risks, but also preventing security breaches. In an organisational context, the primary cause of human error is non-compliance, or non-malicious unawareness, rather than malicious intent (Parsons et al., 2014).

Traditionally, information security has focused on technical solutions, and measures to mitigate risks. However, the importance of the human factor has become increasingly recognised, and it has been well established that technical solutions in isolation cannot sufficiently mitigate security breaches (e.g., Furnell and Clarke, 2012). The role of the human is crucial with humans being the weakest link in information security (Parsons et al., 2017; von Solms and van Niekerk, 2010).

Understanding and influencing these security behaviours is becoming increasingly important. Our increased reliance on technology in work and private lives has contributed to greater information security risks (Reid and van Niekerk, 2014). Risks often result in information security incidents, which are on the rise as more organisations are successfully targeted by cyber security attacks (Telstra Global, 2017). This represents a significant problem, with Chief Executive Officers reporting cyber risks as their greatest overall concern (Pricewaterhouse Cooper [PwC], 2018). The World Economic Forum has also listed major data breaches and cyber-attacks in the top five social risks of the next decade (The World Economic Forum, 2018). Over a two-year period more than 65% of Australian organisations experienced cyber-crime, with one in ten reporting losses greater than $1 million, and 9% reporting having had the confidentiality, integrity, or availability to sensitive data compromised (PwC, 2018). Further, the Australian Computer Emergency Response Team, found 3% of cyber security incidents involved systems of national interest and critical infrastructure (Australian Cyber Security Centre, 2017). As technical solutions alone are insufficient, and with the increase in information security risks, it is imperative we understand the broader factors contributing to ISA.

To further understand the role people play in information security, this study explores the relationship between employee Information Security Awareness (ISA), and organisational and security culture. These constructs have not been empirically studied in combination. In the following sections, we first introduce and de-

[*] Corresponding author.
E-mail addresses: a.wiley@live.com.au (A. Wiley), agata.mccormac@dst.defence.gov.au (A. McCormac), dragana.calic@dst.defence.gov.au (D. Calic).

https://doi.org/10.1016/j.cose.2019.101640

fine these constructs, and then provide a methodological outline of the study. We then present our findings, and discuss them in light of previous research, and in terms of practical implications and further research.

2. Background and related work

2.1. Information Security Awareness

Understanding ISA and its contributing factors is essential in mitigating information security risks. ISA refers to the extent to which employees understand the significance of their organisation's information security policies, rules, and guidelines, and the extent to which they behave in accordance with these policies, rules and guidelines (Siponen, 2000). The Knowledge-Attitude-Behaviour (KAB) model has been applied to the ISA context. Based on the model, as an employee's knowledge of security behaviours increases, their attitude improves, resulting in improved information security behaviours (Parsons et al., 2014; 2017).

To date, human aspects of information security research has primarily focused on understanding human vulnerabilities at the individual level, by exploring the specific characteristics that may relate to, and affect, information security behaviours (McCormac et al., 2017; 2018). This research has shown that ISA can, to an extent, be predicted by age, gender, resilience, job stress, education and some personality characteristics. For example, studies have found higher ISA is positively associated with age (i.e., ISA scores increase with age). Also, females, individuals who are more conscientious and agreeable, individuals who display greater resilience and lower levels of job stress, individuals with a higher education level, and those with a propensity to take fewer risks (McCormac et al. 2017, 2018; Öğütçü et al., 2016; Pattinson et al., 2016; Shropshire et al., 2006).

While research has focused on the individual factors that may predict ISA, limited empirical research has explored the relationship between ISA and culture. Although academics and industry practitioners recognise the importance of security culture (e.g., Da Veiga and Eloff, 2010; OECD, 2015) research in the area is still preliminary. Current literature posits that security culture should be part of organisational culture, as information is best protected when individuals understand, internalise and adhere to information security standards and best practices (van Niekerk and von Solms, 2005; Sanders, 2016). However, without empirical evidence industry practitioners risk providing advice that is below industry standards and expectations.

2.2. Organisational culture

The conceptualisation of organisational culture is highly contested; however, it is most colloquially referred to as 'the way things are done around here' (Lundy and Cowling, 1995, pp. 168). The most widely accepted formal definition of organisational culture has been developed by Schein:

A pattern of shared basic assumptions that the group learned as it solved its problems of external adaptation and internal integration… to be taught to new members as the correct way to perceive, think, and feel in relation to those problems (Schein, 1992, pp. 12).

Culture encompasses the norms a group shares about how the world operates; shaping their perceptions, thoughts, feelings and behaviours (Schein, 1992). Schein's theory of organisational culture conceptualises culture into three hierarchical levels: Artefacts, Espoused Values, and Basic Underlying Assumptions. His work is pivotal in understanding organisational culture and many theorists have based their culture models on this.

Building on the work of Schein, Denison's (1996) model and survey on organisational culture classifies culture into four sub-facets, with three nested subscales within each;

(1) Involvement (Subscales: Empowerment, Team Orientation, and Capability Development);
(2) Consistency (Subscales: Core Values, Agreement, and Coordination & Integration);
(3) Adaptability (Subscales: Creating Change, Customer Focus, and Learning);
(4) Mission (Subscales: Strategic Direction, Goals, and Objectives).

The four overarching sub-facets and their subscales interact to determine whether the organisation is internal or external facing, and whether the organisation has a preference for stability or flexibility. Due to its confirmed reliability, validity and demonstrated link to behavioural outcomes (e.g., Gillespie et al., 2008; Kotrba et al., 2012), the Denison Organisational Culture Survey (DOCS) is the most widely used measure for assessing organisational culture (Kokina and Ostrovska, 2013). Other measures also demonstrate similar reliability, however, they have not been linked as strongly to behaviour, are of a longer duration or are quite costly, with an inability to receive raw data (e.g., Cameron and Quinn, 2011; Cooke and Szumal, 1994; O'Reilly, Chatman and Caldwell, 1991).

The study and measurement of organisational culture is important due to its influence on individual and group behaviours and subsequent relationships with other organisational behaviours such as job satisfaction (Sempane et al., 2002) and job performance (Boyce et al., 2015). It should also be noted that the terms organisational culture and organisational climate are often used synonymously in the literature. Some distinctions including their conceptualisation and research methods had traditionally distinguished them (Schneider et al., 2017), however, now distinctions are primarily in interpretation (Denison, 1996).

2.3. Security culture

An understanding of organisational culture is fundamental when trying to understand and define security culture (Ruighaver et al., 2007). This is because effective security within an organisation is strongly entrenched within its organisational culture (Da Veiga and Martins, 2015). Consequently, security culture is often understood and explained as a sub-culture of organisational culture (Connolly et al., 2017). Therefore, it cannot be assessed in isolation. The focus on security culture is relatively new and in its infancy. Its growth in the literature is primarily attributed to our significant reliance on information systems and digitation of personal and work practices, coupled with the social and political environment surrounding the safeguarding of information. The current literature on security culture is primarily theoretical, with research focussing on conceptual models and frameworks.

The security culture literature draws on various disciplines including psychology, economics, behavioural sciences and management, with a focus on the organisational culture literature as a foundation (Hassan and Ismail, 2012; Nasir et al., 2019). The most extensive adaptations of Schein's (1985) organisational culture theory to security culture were developed by Da Veiga and Eloff (2010), and van Niekerk and von Solms (2010). Van Niekerk and von Solms (2010) adapted Schein's model to better reflect security culture, and also included an additional knowledge tier. Da Veiga and Eloff (2010) focus on the interaction between information security, behaviour and culture, across the individual, group and organisational levels.

While other theories exist, there is consensus that security culture incorporates the assumptions, attitudes, beliefs, values and knowledge that individuals use to interact with the organisation's systems, and conduct relevant procedures, daily tasks and activities. It is shaped through a combination of both the internal and external environments (Da Veiga and Martins, 2015). The internal environment consists of factors such as leadership and organisational structure, and the external environment includes factors ranging from the economic climate to the industry's technology intensity.

These result in certain behaviours that reflect the way things are habitually done in specific organisations (Da Veiga and Eloff, 2010; Schlienger and Teufel, 2003). A strong security culture exists when individuals are aware of security risks and preventative measures, and when they assume responsibility and take the required steps to improve the security of their information systems and networks (OECD, 2015). The primary objective of a strong security culture is to protect information assets by creating a work environment that encourages and supports employees to do the right thing.

Despite ample theoretical support, the measurement of security culture is limited. While security culture tools have been developed, a publicly available, comprehensive, validated and reliable security culture instrument was not available at the commencement of this study (e.g. Alhogail and Mirza, 2014; Da Veiga and Martins, 2015; Martins and Eloff, 2002; Schlienger and Teufel, 2003). An exploratory scale, developed by Parsons et al. (2015) has demonstrated promising reliability and acceptable face-validity; however, further validity testing is recommended.

Given the importance of organisational culture and security culture in determining secure behaviours, the following section will provide a brief overview of the limited empirical literature that has explored the relationship between culture and ISA.

2.4. Related work: culture and ISA

As previously explained, there is ample theoretical and anecdotal support for the relationship between organisational culture and security culture (Nosworthy, 2000), as well as between security culture and ISA (Da Veiga and Eloff, 2010; Schlienger and Teufel, 2003). Despite this, there is limited empirical support for these relationships, and in order to enable evidence-based-practice research is necessary (Coopamootoo and Gross, 2019).

For example, an exploratory quantitative study by Parsons et al. (2015) found a positive relationship between ISA and security culture. Employees from organisations with a better security culture were more likely to have the knowledge, attitudes, and behaviours in accordance with information security policies and procedures required to maintain good information security in the organisation. This is supported by D'Arcy and Greene's (2014) empirical study.

While previous literature has not specifically explored the relationship between ISA and organisational culture, components of culture that relate to ISA have received preliminary support. Strongest support was found for the effect of leadership support on information security management (Knapp et al., 2004) and the creation of a strong security culture (Zakaria et al., 2007). These studies emphasised the importance of leaders in encouraging positive security behaviours through strategic management and planning, communication, and transparent decision-making processes. It was also found that an organisation's security mission was strongly linked to a positive security culture (Ruighaver et al., 2007; Schlienger and Teufel, 2003). For example, a mission statement that outlined elements required for a strong security culture was more likely to translate to behaviours that reflected a positive security culture.

Involving employees in security management decision making provided them with a sense of ownership, and was found to improve both security behaviours and culture (Koh et al., 2005; Ruighaver et al., 2007). Similarly, people-oriented organisations were more likely to experience a positive-orientation to ISA, as a focus on solely tasks can create a conflict of interest between functionality and information security behaviours (Connolly et al., 2017). Lastly, while findings vary for the effects of punishment on ISA (Chen et al., 2012; Parsons et al., 2015), the importance of punishment expectancy and the perceived justice of punishment on ISA has been noted (Xue et al., 2011).

These findings provide preliminary empirical evidence to support the strong theoretical literature linking ISA, organisational culture and security culture. Nonetheless, even seemingly simple research to clearly establish relationships is important. Such research is foundational in guiding subsequent research and enabling industry practitioners to leverage evidence-based and best practice advice to organisations.

3. Current study

Given the strong theoretical link, and some empirical evidence linking organisational and security culture, and ISA, this study aims to empirically investigate the relationship and interplay between organisational culture and security culture, and ISA. Given the previous findings relating to demographic variables (e.g., age and gender) and their relationship to ISA (McCormac et al., 2017, 2018; Pattinson et al., 2016), the effect of these variables will also be analysed.

4. Method

Data collection involved an online survey, administered through the web-based survey platform Qualtrics. Data was collected over a two-week period in July 2018 and ethics approval was granted by the University of Adelaide.

4.1. Participants

A total of 508 (300 females, 207 males, 1 gender unspecified) working Australians completed the online questionnaire. Participants were well distributed across age categories. Approximately 28% of participants were between 18 and 29 years of age, and 28% were between 30 and 39 years of age. This left approximately 17% in the 40 to 49 age category, 15% in the 50 to 59 age category, and 12% of the cohort was 60 years and over. Participants were primarily casual or contracted workers ($n = 303$) as opposed to full time ($n = 138$) or part time ($n = 67$) workers, and were evenly distributed between management ($n = 255$) and non-management ($n = 253$) positions. Participants represented various industries and roles. Comparative to the Australian population (Australian Bureau of Statistics, 2016) our sample demographics were relatively representative.

Participants were required to be over the age of 18, currently employed, working within Australia, and spend some of their time at work on a computer. To ensure data quality, we followed the approach taken by Parsons et al. (2014), and excluded participants who declined to thoughtfully provide their best answers, who appeared to not be providing considered responses or provided answers that indicated a lack of content responsiveness. For example, this included participants who responded using only one response category, irrespective of reverse scoring and the specific questions being asked. Based on these criteria, we removed 17 participants.

Table 1
Correlations and descriptive statistics: gender, age, ISA, security culture, organisational culture ($N = 508$).

Variables	Gender	Age	ISA	Security culture	Organisational culture
Age	-0.13^{**}				
ISA	0.16^{**}	0.25^{**}			
Security Culture	0.10^{*}	0.11^{*}	0.55^{**}		
Organisational Culture	0.03	0.01	0.25^{**}	0.50^{**}	
Mean	^^^	^^^	259.33	3.57	3.59
SD	^^^	^^^	35.71	0.64	0.59

Note. $^{*}p < 0.05$; $^{**}p < 0.001$: ^^^Mean and SD scores for gender and age are unavailable, as gender is a nominal variable, and age range, rather than exact ages, were provided by participants.

4.2. Measures

4.2.1. Demographic information

The participants were asked to provide individual demographics including their age and gender, as well as organisational demographics, including; employment status, position level, industry sector, organisation size, frequency of using technology at work, and information security education.

4.2.2. Information security awareness: the human aspects of information security awareness questionnaire (HAIS-Q)

The HAIS-Q measures an individual's ISA based on their knowledge, attitude and behaviour in relation to good security behaviours (Parsons et al., 2017). The tool consists of 63 statements answered on a 5-point Likert scale, ranging from 1 = 'Strongly Disagree' to 5 = 'Strongly Agree'. In this study, Cronbach's alpha score was 0.96 for ISA. This is consistent with alpha levels reported in previous studies (e.g., McCormac et al., 2016, 2017). For detailed validity and reliability assessments of the HAIS-Q, refer to Parsons et al. (2017) and McCormac et al. (2016). Sample items as part of the Social Media Use focus area are "*I can't be fired for something I have posted on social media*" (Knowledge), "*It's risky to post certain information about my work on social media*" (Attitude), and "*I post whatever I want about my work on social media*" (Behaviour).

4.2.3. Organisational culture: DOCS Denison Organisational Culture Survey

The DOCS (Denison et al., 2006) measures organisational culture by focusing on the following four sub-facets: involvement, consistency, adaptability and mission. The 60-item tool utilises a 5-point Likert scale, ranging from 1 = 'Strongly Disagree' to 5 = 'Strongly Agree'. This study yielded an overall Cronbach's alpha of 0.97, which is consistent with previous studies (Kotrba et al., 2012). A sample item is; "*There is a long-term purpose and direction*".

For the purposes of our study, and consistent with the approach of Boyce et al. (2015), we derived an overall index of organisational culture by taking the mean across the four sub-facets. While this approach is not sensitive to potential sub-facet differences, given the exploratory nature of our study and the focus on organisational culture overall, this method was deemed most suitable.

4.2.4. Security culture: Organisational Security Culture Measure

The Organisational Security Culture Measure assesses an organisation's security culture (Parsons et al., 2015) using six statements measured on a 5-point Likert scale ranging from 1 = 'Strongly Disagree' to 5 = 'Strongly Agree'. An alpha level of 0.71 has been previously reported (Parsons et al., 2015), and the results of this study found the measure to have an alpha value of 0.69. A sample item is, "*Most of my colleagues generally behave in a secure manner when they are using a computer.*"

5. Results

Preliminary analyses were conducted to ensure there was no violation of the assumptions of normality, linearity, multicollinearity and homoscedasticity. As no major violations were identified, several parametric tests were used. These statistical methods were most appropriate for the aims of this study. We calculated descriptive statistics to obtain a general summary of the data and the main variables of interest. Following this correlation analyses were conducted to determine the strength of the linear relationship between the main variables. Hierarchical regression analysis was then used to assess the extent to which organisational culture and security culture predicted ISA, and finally, mediation analysis further examined the relationship between ISA, organisational culture and security culture. A detailed overview of the main results is presented in the following sections.

5.1. Demographic variables, organisational culture, security culture, ISA

Table 1 presents a correlation matrix, including mean and standard deviation scores, to examine the relationship between organisational culture, security culture, ISA, gender, and age. Organisational demographic variables relating to position level, employment sector, industry, and organisation size were also examined. There were no significant relationships between these organisational variables and organisational culture, security culture, and ISA.

5.2. ISA, age, gender

A two-way between-groups ANOVA was conducted to explore the effect of gender and age on ISA. While the interaction effect between gender and age was not statistically significant, $F\ (5,\ 495) = 1.313$, $p = .26$, there was a statistically significant main effect for age, $F\ (5,\ 495) = 7.67$, $p < .001$, partial $\eta^2 = 0.07$. Post-hoc comparisons using the Tukey HSD test indicated that the mean ISA scores for the 20–29 age group ($M = 248.62$, $SD = 39.49$) was significantly different from the 40–49 age group ($M = 265.13$, $SD = 33.99$), the 50–59 age group ($M = 268.05$, $SD = 33.30$), and the 60+ age group ($M = 272.73$, $SD = 25.76$). The mean score for the <19 age group ($M = 241.32$, $SD = 34.28$) was also significantly different from the 60+ age group.

The main effect for gender, $F\ (2,\ 495) = 4.44$, $p = .12$, did not reach statistical significance. There was a trend for ISA to be higher for female participants, when compared to male participants (except for <19 years of age); however, examination of the raw data showed that these gender differences reduced in older age brackets, consistent with previous findings (e.g., McCormac et al., 2017).

5.3. Organisational culture, security culture, ISA

A three-stage hierarchical regression, summarised in Table 2, was used to investigate the extent to which organisational cul-

Table 2
Summary of the hierarchical regression analysis for organisational culture, security culture, age, and gender predicting ISA ($N = 508$).

Variable	β (standardised)	t	p
Stage 1	$F_{(2,\ 507)} = 27.43$, adjusted $R^2 = 0.10^{**}$		
Age	6.88	6.41	<0.001
Gender	13.88	4.52	<0.001
Stage 2	$F_{(3,\ 507)} = 30.97$, adjusted $R^2 = 0.15^{**}$		
Age	6.80	6.55	<0.001
Gender	13.39	4.50	<0.001
Organisational Culture	14.53	5.87	<0.001
Stage 3	$F_{(4,\ 507)} = 68.78$, adjusted $R^2 = 0.35^{**}$		
Age	5.21	5.67	<0.001
Gender	9.60	3.66	<0.001
Organisational Culture	−1.02	−0.41	0.68
Security Culture	28.88	12.41	<0.001

Note. $^{*}p < 0.05$; $^{**}p < 0.001$.

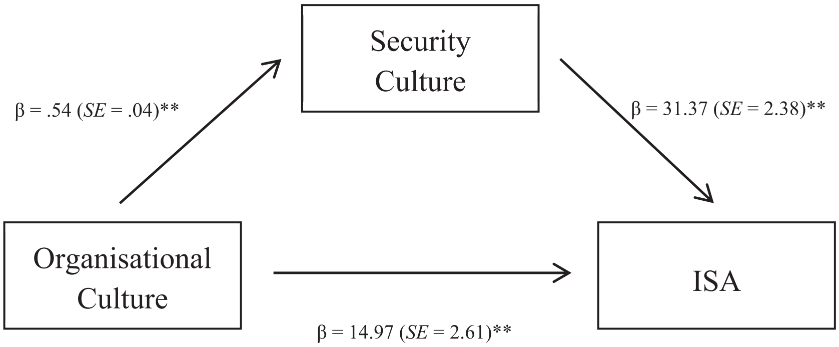

Fig. 1. Mediation analysis: Security culture mediates the relationship between organisational culture and ISA.

ture and security culture predicted ISA. To control for the effects of age and gender, which were previously found to predict ISA (e.g., McCormac et al. 2017), these variables were entered at Stage 1. Strong theoretical literature highlights the effect of organisational culture on individual and group behaviours (Boyce et al., 2015; Cronk and Salmon, 2017). Therefore, this variable was entered at Stage 2, and explained an additional 5% of the variance. As security culture is often conceptualised as a sub-component of organisational culture (e.g., Connolly et al., 2017; Ruighaver et al., 2007), it was entered at Stage 3, and explained an additional 20% of variance. The final model explained a total of 35% variance in ISA. Interestingly, despite the initial contribution and significant correlation with ISA, the contribution of organisational culture was not significant in the final model. To further investigate this, a mediation analysis was conducted, examining the relationship between ISA, organisational culture and security culture.

To examine the mediation effect of security culture between the relationship of organisational culture and ISA, the Sobel test was conducted (Baron and Kenny, 1986). As shown in Fig. 1, the unstandardised regression coefficients were statistically significant, and the statistic for the Sobel test was 9.43, $SE = 1.80$, $p < .001$, indicating that the overall effect of organisational culture on ISA is significantly affected by security culture. This result has applied implications, discussed in the following sections.

6. Discussion

The aim of this study was to empirically examine the relationship between organisational culture, security culture, and ISA. Our main finding, not previously reported was that security culture mediates the relationship between organisational culture and ISA. The following sections will discuss the study's findings and link them to appropriate applications, address some of the main limitations, and propose possible future directions for this promising research.

6.1. Findings and implications

We found a significant positive relationship between organisational culture, security culture, and ISA. Furthermore, after controlling for age and gender, in the regression analyses, organisational culture and security culture predicted an additional 25% of the variance in ISA. A strong positive linear relationship was found between organisational culture and security culture; as organisational culture increased, so did security culture. This relationship is supported by previous literature (Da Veiga and Martins, 2015) and is in line with theoretical arguments suggesting that security culture is a sub-component or a sub-facet of organisational culture (Connolly et al., 2017; Nasir et al., 2019; van Niekerk and von Solms 2005).

A significant positive linear relationship was also found between security culture and ISA, consistent with the theoretical (Da Veiga and Eloff, 2010) and preliminary empirical literature (D'Arcy and Greene, 2014; Parsons et al., 2014). As security culture increased, so did ISA. Essentially, individuals from organisations with a stronger security culture were more likely to have better ISA.

Despite these linear relationships, the study found a more complex relationship which explained the interplay between organisational culture, security culture and ISA. Our findings show that security culture mediates the relationship between organisational culture and ISA. This means that while a relationship between organisational culture and ISA exists, it is strongly affected by security culture. This suggests that irrespective of an organisation's overall culture, a strong security culture may be a better predictor of employee ISA. Therefore, organisation-wide improvements in ISA may be best achieved by focusing on security culture, rather than organisational culture more broadly.

Relationships between ISA and demographic variables were also found. A positive linear relationship between age and ISA was found, with ISA being higher as age increased. However, the distinction between age brackets began to plateau as age increased (>40 years). Similar findings were also reported by McCormac et al. (2017, 2018). Further support for age-related ISA differences have also been found in phishing studies (Sheng et al., 2010). Inconsistent with previous research (McCormac et al., 2017, 2018), a significant main effect was not found between male and female ISA scores.

6.1.1. Applied implications

Our findings have both theoretical and practical implications. The results contribute to the theoretical literature by providing initial empirical support for the relationship between organisational culture, security culture, and ISA. Similarly, the current study also provides initial empirical support and confirms the relationship between security culture and ISA, which to date has been primarily theoretical (Da Veiga and Eloff, 2010; van Niekerk and von Solms, 2010). Finally, we found that the relationship between organisational culture and ISA is mediated by security culture.

Organisational culture is deeply ingrained within an organisation and can be difficult to change (Schein, 2004). However, as security culture is a sub-component of organisational culture (van Niekerk and von Solms, 2005), and is more focussed, it may be easier to manage and change. This is important from a practical perspective, organisations would more effectively utilise their time and resources by focusing on what is required to understand and modify security culture to improve employee ISA. Changing culture more broadly would require greater resources, making it more time-consuming and costly. In addition, positive cultural changes that improve ISA may also result in improvements in overall organisational culture. It is therefore recommended that organisations hoping to improve ISA should focus on security culture through, for example, infrastructure (e.g., technical and procedural) and group norms (e.g., mechanisms such as management support) rather than overall organisational cultural change.

This study provides an important contribution to security research. Current findings can be used to further examine other related variables and interaction effects. For example, it may be beneficial to explore the relationship between security culture and other variables relevant to information security, such as work engagement, resilience and barriers to information security compliance. More importantly, this study also provides an applied contribution. Industry practitioners can rely on sound empirical evidence to guide their recommendations and advice to organisations.

6.2. Limitations and future direction

This study has clear theoretical and applied contributions; however, some limitations are noted. As culture is a multifaceted and multilayered construct, quantitative methods alone may be unlikely to provide a thorough understanding and assessment of organisational culture (Tucker et al., 1990). However, this method allows for the identification and measurement of culture across organisations (Schein, 2004). In addition, self-report is prone to common method variance and social desirability (Spector, 1994), yet it allows for systemisation, repeatability, comparability and convenience (Tucker et al., 1990).

This was an exploratory study; therefore, using a survey-based, self-report, quantitative method was justified. In addition, to reduce the previously mentioned effects, this study also implemented quality control measures, and guaranteed confidentiality and anonymity to all participants. Nonetheless, to offset some of these weaknesses and to provide a greater breadth of understanding, where possible future studies should employ a mixed methods design.

The measurement tools used in this study may also present a limitation. A short security culture measurement tool was used. At the time of data collection, a comprehensive, valid and reliable measure of security culture was yet to be published. However, the 6-item tool used demonstrated sound reliability, and due to the exploratory nature of this study was deemed sufficient. Given the findings of this study, and the recent development of the Information security culture Assessment (ISCA) diagnostic instrument (questionnaire) (Da Veiga, 2018), further exploration, and even a replication, using this measure is warranted. In addition, the DOCS organisational culture tool has shown considerable reliability and validity, and is the most widely used organisational culture assessment tool (Kokina and Ostrovska, 2013). However, one limitation is that the sub-facets are highly correlated, (Denison et al., 2006), meaning it is difficult to ascertain whether the sub-facets are distinct areas of culture that can be compared. This means it is difficult to compare whether certain sub-facets were more predictive of security culture and ISA than others. This is something that needs to be considered in future studies.

While this study has focussed on the relationship between organisational culture, security culture and ISA, there are other aspects that may predict ISA including national culture, and other individual, group, and organisational differences. While the DOCS model is applicable for assessing organisational culture globally (Denison et al., 2006), the effect of national culture on organisational culture, security culture and ISA could also be explored. For example, Hofstede et al. (2010), and Schein (2004) found that Western and Asian countries have profoundly different national and organisational cultures. Given the relationship between national culture and organisational culture, a global sample would contribute to the understanding of this relationship. While considerable research has documented the relationship between individual differences and ISA (e.g. McCormac et al., 2018; Pattinson et al., 2016), incorporating these into a more comprehensive model with culture could be insightful, especially given the global and cross-cultural dispersion of many organisations. This would give organisations and industry practitioners a greater understanding of the factors contributing to ISA of their employees. In turn, this could inform and guide the development of appropriate intervention initiatives such as cyber communications and training programs, strategy development, risk analysis modelling and culture change.

6.3. Conclusion

This study empirically examined the relationship between organisational culture, security culture, and ISA. Our main finding, not previously reported, was that security culture mediates the relationship between organisational culture and ISA. These findings have important theoretical and applied implications. Theoretically, the results of this study can be explored further in future research to more comprehensively, using different methodological approaches and measures, investigate these relationships. This finding is also practically important and seems to demonstrate that rather than focussing on the broader organisational culture which may be time consuming and resource intensive, organisations may achieve greater employee ISA by focussing on understanding, developing and strengthening their organisation's security culture.

Declaration of Competing Interest

None.

References

Alhogail, A., & Mirza, A. (2014). A proposal of an organizational information security culture framework. In Proceedings of the *Information, Communication Technology and System (ICTS), 2014 International Conference* (pp. 243-250). Surabaya: Indonesia.

Australian Bureau of Statistics. (2016). *2016 Census QuickStats*. Retrieved from quickstats.censusdata.abs.gov.au/census_services/getproduct/census/2016/quickstat/036.

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

Baron, R., Kenny, D., 1986. The moderator–mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations. J. Pers. Social Psychol. 51 (6), 1173.

Boyce, A., Nieminen, L., Gillespie, M., Ryan, A., Denison, D., 2015. Which comes first, organizational culture or performance? A longitudinal study of causal priority with automobile dealerships. J. Organ. Behav. 36 (3), 339–359.

Cameron, K., Quinn, R.E., 2011. Diagnosing and Changing Organizational Culture: Based on the Competing Values Framework, (3rd ed.) Jossey-Bass, San Francisco, CA.

Chen, Y., Ramamurthy, K., Wen, K., 2012. Organizations' information security policy compliance: stick or carrot approach. J. Manage. Inf. Syst. 29 (3), 157–188.

Connolly, L., Lang, M., Gathegi, J., Tygar, D., 2017. Organisational culture, procedural countermeasures, and employee security behaviour: a qualitative study. Inf. Comput. Secur. 25 (2), 118–136.

Cooke, R., Szumal, J., 1994. The impact of group interaction styles on problem-solving effectiveness. J. Appl. Behav. Sci. 30 (4), 415–437.

Coopamootoo, K., Gross, T., 2019. A systematic evaluation of evidence-based practice methods in cyber security user studies (Technical report no. CS-TR-1528). Retrieved from https://www.ncl.ac.uk/media/wwwnclacuk/schoolofcomputingscience/files/trs/1528.pdf.

Cronk, L., Salmon, C., 2017. Culture's influence on behavior: steps toward a theory. Evol. Behav. Sci. 11 (1), 36–52.

D'Arcy, J., Greene, G., 2014. Security culture and the employment relationship as drivers of employees' security compliance. Inf. Manage. Comput. Secur. 22 (5), 474–489.

Da Veiga, A, 2018. An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. Inf. Comput. Secur. 26 (5), 584–612.

Da Veiga, A, Eloff, J, 2010. A framework and assessment instrument for information security culture. Comput. Secur. 29 (2), 196–207.

Da Veiga, A, Martins, N., 2015. Information security culture and information protection culture: a validated assessment instrument. Comput. Law Secur. Rev. 31 (2), 243–256.

Denison, D., 1996. What "IS" the difference between organizational culture and organizational climate? A native's point of view on a decade of paradigm wars. Acad. Manage. Rev. 21 (3), 619.

Denison, D., Janovics, J., Young, J., Cho, H., 2006. *Diagnosing Organizational Cultures: Validating a Model and Method* (Vol. 304) Ann Arbor, MI.

Furnell, S., Clarke, N., 2012. Power to the people? The evolving recognition of human aspects of security. Comput. Secur. 31 (8), 983–988.

Gillespie, M., Denison, D., Haaland, S., Smerek, R., Neale, W., 2008. Linking organizational culture and customer satisfaction: results from two companies in different industries. Eur. J. Work Organizational Psychol. 17 (1), 112–132.

Hassan, N., Ismail, Z., 2012. A conceptual model for investigating factors influencing information security culture in healthcare environment. Procedia - Social Behav. Sci. 65, 1007–1012.

Hofstede, G., Hofstede, Gert Jan, Minkov, Michael, 2010. Cultures and organizations: Software of the mind: Intercultural cooperation and Its Importance For Survival / By Geert Hofstede, Gert Jan Hofstede, and Michael Minkov, 3rd ed McGraw-Hill, New York; Sydney Rev. and expanded.

Knapp, K., Marshall, T., Rainer, R., Morrow, D., 2004. Top ranked information security issues. In: Proceedings of *The 2004 International* Information *Systems* Security *Certification* Consortium *(ISC) 2 Survey Results*. Auburn, Alabama: United States.

Koh, K., Ruighaver, A.B., Maynard, S., Ahmad, A., 2005. Security governance: its impact on security culture. In: Proceedings *of the 3rd Australian Information Security Management Conf*erence: *AISM*. Perth, Western Australia.

Kokina, I., Ostrovska, I., 2013. The analysis of organizational culture with the Denison model: (the case study of Latvian municipality. Eur. Sci. J. 1 (1), 362.

Kotrba, L., Gillespie, M., Schmidt, A., Smerek, R., Ritchie, S., Denison, D., 2012. Do consistent corporate cultures have better business performance? Exploring the interaction effects. Hum. Relat. 65 (2), 241–262.

Lundy, O., Cowling, A., 1995. *Strategic Human Resource Management/Olive Lundy and Alan Cowling*. Routledge, New York.

Martins, A., Eloff, J., 2002. Information security culture. *Paper* Presented *at the 17th International* Conference On Information *Security*. Cairo, Egypt.

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. Inf. Comput. Secur. 26 (3), 277–289.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M., 2017. Individual differences and information security awareness. Comput. Hum. Behav. 69, 151–156.

Nasir, A., Arshah, R.A, Hamid, M.R, Fahmy, S, 2019. An analysis on the dimensions of information security culture concept: a review. J. Inf. Secur. Appl. 44, 12–22.

Nosworthy, J., 2000. Implementing information security in the 21st century — do you have the balancing factors? Comput. Secur. 19 (4), 337–347.

Öğütçü, M., Testik, Ö., Chouseinoglou, O., 2016. Analysis of personal information security behavior and awareness. Comput. Secur. 56, 83–93.

O'Reilly, C., Chatman, J., Caldwell, D., 1991. People and organisational culture: a profile comparison approach to assessing person-organization fit. Acad. Manage. J. 34 (3), 487–516.

Organisation for Economic Co-operation and Development [OECD]. (2015). *Principles of corporate governance*. Retrieved from oecd.org/daf/ca/Corporate-Governance-Principles-ENG.pdf.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T., 2017. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Comput. Secur. 66, 40–51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C., 2014. Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Comput. Secur. 42, 165–176.

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M., Jerram, C., 2015. The influence of organisational information security culture on cybersecurity decision making. J. Cognit. Eng. Decis. Making 9 (2), 117–129.

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., Calic, D., 2016. Assessing information security attitudes: a comparison of two studies. Inf. Comput. Secur. 24 (2), 228–240.

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.

Reid, R., van Niekerk, J., 2014. Brain-compatible, web-based information security education: a statistical study. Inf. Manage. Comput. Secur. 22 (4), 371–381.

Ruighaver, A., Maynard, S., Chang, S., 2007. Organisational security culture: extending the end-user perspective. Comput. Secur. 26 (1), 56–62.

Sanders, J., 2016. Defining terms: data, information and knowledge. In: SAI Computing Conference (SAI), 2016, pp. 223–228.

Schein, E., 1985. Organizational Culture and Leadership, (1st ed.) Jossey-Bass Business & Mangement Series, San Francisco, CA.

Schein, E., 1992. Organizational Culture and Leadership, (2nd ed.) Jossey-Bass Business & Management Series, San Francisco, CA.

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

Schlienger, T., Teufel, S., 2003. Analyzing information security culture: increased trust by an appropriate information security culture. In: *Database and Expert* Systems *Applications, 2003. Proceedings. 14th International Workshop*. Prague: Czech Republic, pp. 405–409.

Schneider, B., González-Romá, V., Ostroff, C., West, M., Chen, G., 2017. Organisational climate and culture: reflections on the history of the constructs in the journal of applied psychology. J. Appl. Psychol. 102 (3), 468–482.

Sempane, M., Rieger, H., Roodt, G., 2002. Job satisfaction in relation to organisational culture. SA J. Ind. Psychol. 28 (2), 23–30.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., Downs, J., 2010. Who falls for phishing? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: *Proceedings of the SIGCHI Conference on Human* Factors *in Computing* Systems. ACM, Atlanta, Georgia: USA, pp. 373–382.

Shropshire, J., Warkentin, M., Johnston, A., Schmidt, M., 2006. Personality and it security: an application of the five-factor model. In: AMCIS 2006 Proceedings, p. 415.

Siponen, M., 2000. A conceptual foundation for organizational information security awareness. Inf. Manage. Comput. Secur. 8 (1), 31–41.

Spector, P., 1994. Using self-report questionnaires in OB research: a comment on the use of a controversial method. J. Organ. Behav. 15 (5), 385–392.

Telstra Corporation. (2017). *Telstra cyber security report 2017*. Retrieved from telstraglobal.com/images/assets/insights/resources/Telstra_Cyber_Security_Report_2017_-_Whitepaper.pdf.

Tessem, M., Skaraas, K., 2005. Creating a security culture. Telektronikk 101 (1), 15–22.

Tucker, R., Mccoy, W., Evans, L., 1990. Can questionnaires objectively assess organisational culture? J. Manage. Psychol. 5 (4), 4–11.

Van Niekerk, J., von Solms, R., 2005. A holistic framework for the fostering of an information security sub-culture in organizations. ISSA 1 (13).

Van Niekerk, J., von Solms, R., 2010. Information security culture: a management perspective. Comput. Secur. 29 (4), 476–486.

World Economic Forum. (2018). *World economic forum annual meeting: creating a shared future in a fractured world*. Retrieved from www3.weforum.org/docs/WEF_Annual_Report_2017-2018.pdf.

Xue, Y., Liang, H., Wu, L., 2011. Punishment, justice, and compliance in mandatory IT settings. Inf. Syst. Res. 22 (2), 400–414 416-417.

Zakaria, O., Gani, A., Moh Nor, M, Badrul Anuar, N, 2007. Reengineering information security culture formulation through management perspective. *Paper* Presented *at the International* Conference *on* Electrical Engineering and *Informatics*, Bandung: Indonesia.

Ashleigh Wiley. *The University of Adelaide***.** Ashleigh Wiley is a psychologist, who has recently completed the Master of Psychology (Organisational and Human Factors) degree at the University of Adelaide. She spent the last year working with the Defence Science and Technology Group examining the human aspects of cybersecurity. Her previous research explored aspects relating to culture and climate, specifically looking at the Psychosocial Safety Climate.

Agata McCormac. *Defence Science and Technology (DST) Group*. Agata McCormac is a research scientist with the Defence Science and Technology (DST) Group, where her research involves examining the human aspects of cybersecurity. She completed a Master of Psychology (Organisational and Human Factors) at the University of Adelaide in 2005. She is an organisational psychologist and Adjunct Lecturer within the School of Psychology at The University of Adelaide.

Dragana Calic. *Defence Science and Technology (DST) Group*. Dragana Calic is a research scientist with the Defence Science and Technology (DST) Group, where her research is concerned with the human aspects of cybersecurity. In 2013, she completed a PhD in Psychology at the University of Adelaide on the human performance in face matching. She is also a Visiting Research Fellow in the School of Psychology at The University of Adelaide.