Culture and Information Security Awareness: Examining the Role of Organisational and Security Culture

Ashleigh Wiley

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 2018

Literature Review Word Count: 4, 928

Research Report Word Count: 5, 444

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.

Ashleigh Morgan Wiley

[redacted]

October 2018

Acknowledgements

To my supervisors Agata McCormac and Dragana Calic, you generously shared your knowledge, support and time. I cannot thank either of you enough for your expertise, approachability and warmth. I am grateful to have had you both as supervisors.

Also to the other members of the Human Aspects of Cyber Security (HACS) team: Kathryn Parsons, Marcus Butavicius, (DST Group), and Malcolm Pattinson (The University of Adelaide). Thank you for your continuous feedback and help. I have enjoyed working with such a wonderful team.

Thank you to Neil Kirby for your assistance as secondary supervisor and as the Master of Psychology (OHF) Program Coordinator.

To my parents, siblings and Paul, thank you for your continuous love and support. I could not have come so far without you.

To my classmates, thank you for your support and encouragement. You have made the last two years more enjoyable than I could have asked for.

List of Tables

Literature Review

Research Report

List of Figures

Literature Review

Word count: 4, 928

Abstract

This review provides an initial assessment of the literature on Information Security Awareness (ISA), organisational culture and security culture. The relationship between aspects of organisational culture, security culture and ISA has received theoretical support. However, there is a lack of empirical research examining this relationship; therefore an empirical investigation is warranted. Given the findings of this review, future research should empirically examine the interplay between ISA, organisational culture and security culture.

Keywords: Security Culture, Organisational Culture, ISA, Cyber, Review

Introduction

Human behaviour is largely determined by culture, which affects both social and work interactions (Cronk & Salmon, 2017). Therefore, to understand and influence behaviour, looking at an individual in isolation is problematic. It is important to consider the group, the infrastructure and their interaction (Grant, 2005; Tessem & Skaraas, 2005). This is important for information security, as humans 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; Pfleeger & Caputo, 2012; Wood & Banks, 1993). To further understand the role humans play in information security within an organisational context, this review will explore the literature on employee Information Security Awareness (ISA), organisational culture and security culture. These constructs have not previously been explored together.

Information security research has traditionally been approached from a computer science perspective, with technical measures being implemented to mitigate risks (Aurigemma & Panko, 2012). While information security and cyber security are often used synonymously in the literature, cyber security is one component of information security (von Solms & van Niekerk, 2013). Therefore, as information security encompasses cyber security, this review will use the term information security, unless referring to specific cyber security statistics. Irrespective, the importance of the human factor in information security is increasingly recognised (e.g., Herath & Rao, 2009; Metalidou et al., 2014; Vroom & von Solms, 2004). It has been well established that technical solutions, alone, cannot safeguard against all information security threats (e.g., Furnell & Clarke, 2012; Furnell et al., 2006; Pfleeger & Caputo, 2012). The role of the human is crucial as humans are often referred to as the first line of defence against information security threats (von Solms & van Niekerk, 2010; Pricewaterhouse Cooper [PwC], 2016, 2018; Schlienger & Teufel, 2003).

It has become increasingly important to not only understand, but to also influence security behaviours. Our increased reliance on technology in work and private lives has contributed to greater information security risks (Crossler et al., 2013; Reid & Niekerk, 2014; Thomson, von Solms & Louw, 2006). These risks often result in security incidents, which are on the rise with more organisations successfully being targeted through cyber-attacks (Telstra Global, 2017). This represents a significant problem, with Chief Executive Officers reporting cyber risks as their greatest overall concern (PwC, 2018). The World Economic Forum has also listed cyber-attacks and major data breaches 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 due to a cyber-attack (PwC, 2018). Further, the Australian Computer Emergency Response Team (ACSC, 2017) found 3% of cyber security incidents involved systems of national interest and critical infrastructure. As technical solutions alone are insufficient, it is important to more thoroughly examine the factors contributing to employee awareness.

Given the influence of culture on human behaviour (Cronk & Salmon, 2017) and the importance of human factors in information security (Metalidou et al., 2014; Parsons et al., 2014; Vroom & von Solms, 2004); this literature review will examine the constructs of ISA, organisational culture and security culture, including the relationships between them. Throughout the following sections, we provide a thorough review of the relevant ISA, organisational and security culture literature.

Information Security Awareness

Understanding Information Security Awareness (ISA) and its contributing factors is essential in mitigating information security risks. ISA refers to the degree to which employees understand the importance of their organisations' information security policies, rules, and guidelines, and the degree to which they behave in accordance with these (Bulgurcu, Cavusoglu & Benbasat, 2010; Kruger & Kearney, 2006; Siponen, 2000).

The human aspects of information security research has focused primarily on understanding human vulnerabilities at the individual level, through exploring the specific characteristics affecting information security behaviours (McCormac et al., 2017a, 2018; Shropshire et al., 2006). This research has shown ISA can, to an extent, be predicted by age, gender, resilience, job stress, education and some personality characteristics. Studies have found higher ISA to be positively associated with age (i.e., ISA scores increasing with age), gender (i.e., females have higher ISA scores than males), and education (i.e., ISA scores increasing with education level). It has also been found that individuals who are more conscientious and agreeable, have a propensity to take fewer risks, possess greater resilience, and also have higher ISA (McCormac et al., 2017a; 2018; Öğütçü, Testik & Chouseinoglou, 2016; Pattinson et al., 2016).

While substantial research has focussed on individual factors predicting ISA, limited empirical research has explored the relationship between ISA and culture, despite academics and industry practitioners recognising the importance (Da Veiga & Eloff, 2010; Schlienger & Teufel, 2003; OECD, 2004, 2015). The literature suggests a security culture should form part of an organisation's culture (Schlienger & Teufel, 2003; von Solms, 2000), as information is best protected when individuals understand, internalise and behave to information security standards (van Niekerk & von Solms, 2005; Sanders, 2016; Thomson, von Solms & Louw, 2006).

Theories & Frameworks

The Knowledge-Attitude-Behaviour (KAB) model is often applied to the ISA context. The model purports that, as an employee's knowledge of security behaviours increases, their attitude improves, resulting in improved information security behaviours (Kruger & Kearney, 2006; Parsons et al., 2014; Siponen, 2000). While this model has been criticised by some researchers, evidence of its validity is well established (Bettinghaus, 1986; Van der Linden, 2012), and its use supported (McGuire, 1969).

Measurement & Methods

Despite the importance of assessing employee ISA, little effort has been put into trying to measure ISA in a holistic manner (Öğütçü, Testik & Chouseinoglou, 2016). Although security breaches and their corresponding consequences are often measured in organisations (e.g. PwC, 2018), the impact of employee ISA is rarely considered. Additionally, specific aspects of ISA have been researched within the literature (e.g. Stanton et al., 2005; Utz, 2009); however overall ISA was not measured. Behavioural models, such as the Theory of Planned Behaviour (Bulgurcu, Cavusoglu & Benbasat, 2010), and the General Deterrence Theory (D'Arcy, Hovav & Galletta, 2009; Fan & Zhang, 2011), have also been applied to understand aspects of ISA. However, this approach is also limited, as an indication of overall ISA was not provided (Karjalainen & Siponen, 2011; Parsons et al., 2017).

More recently, research has focussed on developing a measure of ISA. These measures are at various stages of development and many still require further reliability and validation testing. For example, The Users' Information Security Awareness Questionnaire (UISAQ), measures risk behaviour, level of ISA, beliefs about information security and the quality and security of passwords (Solic, Velki & Galba, 2015; Velki, Solic & Ocevcic, 2014). The Security Behaviour Intentions Scale (SeBIS) (Egelman & Peer, 2015) focusses on adherence to computer security advice, exploring device securement, password generation, and proactive awareness and staying up-to-date. The measure has undergone preliminary reliability and validity testing (Egelman, Harbach & Peer, 2016). Öğütçü, Testik, and Chouseinoglou (2016) developed four scales to measure the security behaviours and awareness of individuals; Risky Behaviour Scale (RBS), Conservative Behaviour Scale (CBS), Exposure to Offence Scale (EOS) and Risk Perception Scale (RPS). The scales found promising results, however, as preliminary testing has only been conducted for several of these measures, further validity and reliability testing with a more generalisable sample is needed.

The Human Aspects of Information Security Questionnaire (HAIS-Q) has the most theoretical support (Parsons et al., 2014, 2017) and builds on the Knowledge-Attitude-Behaviour model (KAB). It proposes that as employee information security knowledge increases, attitude improves, resulting in improved behaviours (Bulgurcu, Cavusoglu & Benbasat , 2010; Kruger & Kearney, 2006; Parsons et al., 2014; Siponen, 2000). It was developed through a review of information security policies and standards, and through consultation with managers and information technology professionals (Parsons et al., 2017). The HAIS-Q measures an individual's ISA based on their knowledge, attitude and behaviour towards information security behaviours. The measure has undergone sufficient reliability and validity testing on diverse populations (Hadlington & Parsons, 2017; McCormac et al., 2016, 2017b; Parsons et al., 2017).

Given the influence of culture on human behaviour (Cronk & Salmon, 2017) and the importance of the human factor in information security (Metalidou et al., 2014; Parsons et al., 2014; Vroom & von Solms, 2004); the following sections will explore culture, by considering both organisational and security culture, and their relationship to ISA.

Organisational Culture

The conceptualisation of organisational culture is highly contested, however, it is colloquially referred to as 'the way things are done around here' (Lundy & 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, that has worked well enough to be considered valid and, therefore, 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 is developed based on the culmination of activities, the vision and employee behaviour at the individual, group and organisational level (Hellriegel et al., 1998; Robbins, 2001). It encompasses the norms a group shares about how the world operates; shaping their perceptions, thoughts, feelings and behaviours (Schein, 1986, 1990). The study of culture is important due to its influence on individual and group behaviours, and subsequent relationship to organisational behaviours such as job satisfaction (Fey & Denison, 2003; Schneider & Snyder, 1975; Sempane, Rieger & Roodt, 2002) and job performance (Boyce et al., 2015; Hartnell, Ou & Kinicki, 2011).

The notion of culture has a long history in anthropology and sociology (Alyesson & Berg, 1992; Berthon, Pitt & Ewing, 2001; Cameron & Ettington, 1988). The concept of organisational culture was initially discussed in 1962 (Blau & Scott), however, it was another decade later before the first major analysis of the informal dimension of organisational culture gained attention in mainstream organisational theory literature (Peters, 1978; Pettigrew, 1979).

The terms organisational *culture* and organisational *climate* are often used synonymously in the literature, despite some distinctions (Schneider et al., 2017; Schwartz & Davis, 1981; Wallace, Hunt & Richards, 1999). Organisational culture was initially conceptualised as the collection of fundamental values and belief systems that give meaning to organisations (Geertz, 1973; Mohr, 1982; Schein, 1985), and was almost exclusively measured qualitatively through ethnographic research, including case studies (Rousseau, 1990; Schein, 2004; Schneider, Ehrhart & Macey, 2011). Organisational climate, however, placed greater emphasis on factors closer to the surface of organisational life that are easier to decipher (Guion, 1973; James & Jones, 1974), focussing on the impact organisations have on groups and individuals (Ekvall, 1987; Joyce & Slocum, 1984; Koys & DeCotiis, 1991). It was derived from the Lewin field theory (Drexler, 1977; Lewin, 1951; Lewin, Lippit & White, 1939) and quantitative observation (Barker, 1965; Likert, 1961; O'Driscoll & Evans, 1988). Currently distinctions are primarily in interpretation rather than the phenomenon itself (Denison, 1996; Moran & Volkwein, 1992).

Theories & Frameworks

One of the most cited theories is Edgar Schein’s (1985, 1992, 2004) theory of organisational culture (Buchanan & Huczynski, 2016). Schein conceptualises culture into three hierarchical levels: Artefacts, Espoused Values, and Basic Underlying Assumptions. The Artefacts level consists of overtly apparent, visible, organisational features (e.g., staff uniforms). The Espoused Values level encompasses the elements and guiding principles essential to inform artefacts and govern employee behaviour (e.g., mission statement). Lastly, Basic Underlying Assumptions shape the core of the organisations culture; they are held implicitly and are not readily observable (e.g., how employees perceive others' behaviour). Other prominent researchers also dominate the field of organisational culture, each offering a unique perspective. Table 1 summarises the most notable theories.

Table 1.

Prominent Organisational Culture Theories

Theorist	Theory Title
Cameron, & Quinn *(2011)*	Competing Values Framework
Cooke & Szumal *(1994)*	Organisational Culture
Deal & Kennedy *(1982)*	Deal & Kennedy Culture Types
Denison *(1990, 1996)*	Denison Model Of Organisational Culture (DOCS)
Flamholtz *(2011)*	Organisational Culture Components
Grant *(2012)*	Norms of Reciprocity
Hampden-Turner & Trompenaars *(1997)*	Cultural Dimensions
Handy *(1986)*	Organisational Culture
Harris *(1994)*	In-Organisation Schema
Harrison *(1972, 1975)*	Typologies of Organisational Culture
Hofstede *(1990)*	Cultural Dimensions Theory
Johnson & Scholes *(1997)*	Cultural Web
O'Reilly, Chatman & Caldwell *(1991)*	Organisational Cultural Profile (OCP)
Schein *(1985, 1992, 2004)*	Organisational Culture
Schneider *(1985)*	Schneider Culture Model

These organisational culture theories vary in their complexity, applicability and empirical support. Numerous theories categorise organisational culture based on, for example, competence or productivity, hierarchical structure or a collaboration focus (Cameron & Quinn, 2011; Deal & Kennedy, 1982; Handy, 1986; Harrison, 1972, 1975; Schneider, 1985; Quinn & Rohrbaugh, 1983). While the approach of exploring culture through fixed overarching categories, rather than on a spectrum, allows for ease in comparing groups, it can be limiting when attempting to understand the deeper level of culture and the reasoning behind employee behaviour.

O'Reilly, Chatman, and Caldwell's (1991) approach focusses on person-environment-fit. Johnson's Cultural Web (1997) assesses organisational culture through six domains; while it is useful for cultural change, it is less beneficial in research settings where the aim is to compare organisations. Other organisational culture theories explore a specific aspect of culture, rather than devising an all-encompassing theory (Grant, 2012; Harris, 1994; Hofstede, 1990; Martin & Siehl, 1983; Trompenaars & Hampden-Turner, 1997).

Denison’s (1996) model of organisational culture classifies culture into four sub-facets (traits), with three subscales nested within each; Involvement (Empowerment, Team Orientation, and Capability Development), Consistency (Core Values, Agreement, and Coordination & Integration), Adaptability (Creating Change, Customer Focus, and Learning), and Mission (Strategic Direction, Goals, and Objectives). The four overarching traits 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. Additionally, the traits can be applied to predict behavioural outcomes linked to performance, satisfaction, and innovation. Denison’s model and the associated instrument is the most widely used for assessing organisational culture (Kokina & Ostrovska, 2013; Sackmann, 2011; Schneider, Ehrhart, & Macey, 2011).

Recently there has been a shift from conceptualising organisational culture toward quantitatively measuring culture, partially due to the recognition of the importance of culture and its relationship with organisational performance (Boyce et al., 2015; Hartnell, Ou & Kinicki, 2011; Sackmann, 2011). This has meant that industry is placing a greater focus on culture, relying on measurement methods for comparison and improvement.

Measurement & Methods

The ease of application and the systemisation, repeatability, generalisability and comparability of quantitative measures has led to the development of many organisational culture measures in academia and in practice (Ashkanasy, et al., 2000; Ott, 1989; Schein, 2004; Tucker, McCoy & Evans, 1990). As organisational culture measures vary considerably in terms of their theoretical basis, validity and reliability, a degree of caution should be exercised when choosing a measure.

Several organisational culture measures currently exist. Table 2 lists several of the most common ones. The reason for the popularity of these tools is primarily due to their stronger theoretical underpinning, psychometric properties and ease of application. Additionally, it is important to note that uptake of measures is often dependent on whether there is an associated cost, whether raw data can be obtained by the researcher, and the survey duration.

Table 2.

Organisational Culture Measures

Theorist	Measure	Properties
Cameron & Quinn (2011)	Organisational culture Assessment Instrument (OCAI)	Reliability: Cronbach Alpha .70-.90 Confirmatory Factor Analysis: Good model fit
Cooke & Lafferty (1983)	Organisational culture Inventory (OCI)	Reliability: Cronbach Alpha .67-.92
Denison (2006)	Denison Organisational culture Survey (DOCS)	Reliability: Cronbach Alpha .80-.97 Confirmatory Factor Analysis: Good model fit Criterion-related validity: Job satisfaction, .42-.79
O’Reilly, Chatman, Caldwell (1991)	Organisational Cultural Profile (OCP)	Reliability: Cronbach Alpha .85-.96 Exploratory Factor Analysis: 75% of variance

Of these, the DOCS is the most widely used organisational culture measure (Kokina & Ostrovska, 2013; Sackmann, 2011; Schneider, Ehrhart & Macey, 2011), due to its confirmed reliability, validity and demonstrated link to behavioural outcomes (e.g., Gillespie et al., 2008; Kotrba et al., 2012; Yilmaz & Ergun, 2008). The DOCS (Denison et al., 2006) follows the same categorisation as Denison’s culture theory, measuring four traits of organisational culture, with three nested indexes.

Security Culture

An understanding of organisational culture is fundamental to understanding security culture. This is because effective security culture is strongly entrenched within organisational culture (Da Veiga & Martins, 2015) and cannot be assessed in isolation. The focus on security culture is relatively new. Its growth in the literature is primarily attributed to our significant reliance on information systems and digital devices, coupled with the social and political environment surrounding the safeguarding of information. The implementation of solely technological solutions is inadequate in preventing security breaches (Borck, 2000; Pfleeger, 1997). Therefore, focussing on the human aspects at the group level, by measuring culture, could provide a more comprehensive understanding. Security culture is often explained as a sub-culture of organisational culture (Borck, 2000; Chia, Maynard, & Ruighaver, 2003; Connolly et al., 2017). It is shaped through a combination of both internal and external environments (Da Veiga & Martins, 2015; Thompson, von Solms & Louw, 2006). The internal environment consists of factors such as leadership and organisational structure. Whereas, the external environment, includes factors ranging from the economic climate to an industry’s technology use.

Security culture incorporates the assumptions, attitudes, beliefs, values and knowledge that individuals use to interact with the organisation’s systems, procedures, daily tasks and activities. These result in certain behaviours that reflect the way things are habitually done in specific organisations (Da Veiga & Eloff, 2010; Mahfuth et al., 2017; Schlienger & Teufel, 2003). A strong security culture exists when individuals are aware of security risks and preventative measures, assume responsibility, and take the required steps to improve the security of their information systems and networks (OECD, 2004). The primary objective of a strong security culture is to protect information assets by influencing employees. This can be achieved through increasing ISA in order to improve the security behaviour of employees (Furnell, 2007).

Theories & Frameworks

The current literature on security culture is primarily theoretical, with research focussing on conceptual models and frameworks. While some researchers have argued that security culture is too complex to be summarised in a single model (Ruighaver, Maynard, & Chang; 2007), others have developed theoretical frameworks based on organisational culture theories (Schlienger & Teufel, 2003; Vroom & von Solms, 2004).

The security culture literature draws on various disciplines including psychology, economics, behavioural sciences and management. However, the literature primarily focusses on extending Schein's three-tier organisational culture model of Assumptions, Espoused Values and Artefacts (Schlienger & Teufel, 2003). Van Niekerk and von Solms (2010) adapted Schein's (1985) three-tier model by including an additional tier, Information Security Knowledge. The addition of the knowledge tier is paramount, as behaviour is guided by knowledge (Mahfuth et al., 2017; Parsons et al., 2017). While it is assumed individuals have the knowledge to undertake their core role successfully, the same assumption cannot be made for having sufficient knowledge of information security. The contents of Schein's (1985) other dimensions were also marginally altered to better reflect the security culture context.

Da Veiga and Eloff (2010) also adapted Schein's (1985) organisational culture theory. They focus on the interaction between information security, behaviour and culture, across the individual, group and organisational levels. They suggest that information security policies, procedures and practices influence information security behaviour, which in turn cultivates a security culture. This model has suggested a slightly different causal direction than most culture research. Due to the difficulty in determining causation, they suggested culture and behaviour can each exert influence over the other.

Several others propose a security culture framework, either by using the organisational culture literature as a foundation (D'Arcy, Hovav & Galletta, 2009; Hassan, & Ismail, 2012; Knapp et al., 2006; Ruighaver, Maynard, & Chang, 2007) or by summarising the existing security culture literature (Alhogail, 2015; Tang, Li & Zhang, 2016). However, this work is less comprehensive than the work of van Niekerk and von Solms (2010) and Da Veiga and Eloff (2010).

Measurement & Methods

Despite ample literature, measurement of security culture is limited. A publicly available, comprehensive, validated and reliable security culture instrument is not currently available. A number of other security culture tools have been developed. Unfortunately, some of these measures either demonstrated poor psychometric properties, have not been well validated, or have not been released for public use (Al-Mayahi & Mansoor, 2013; Alhogail & Mirza, 2014; Ashenden, 2008; Da Veiga & Martins, 2015; Flores & Ekstedt, 2016; Karlsson, Åström & Karlsson, 2015; Martins & Eloff, 2002; Schlienger & Teufel, 2003). This means organisations are unable to accurately and objectively measure their security culture. This affects their ability to measure risk and monitor change.

An exploratory scale, developed by Parsons et al. (2015) seeks to measure security culture through six statements. This measure has demonstrated promising reliability and acceptable face-validity. However, further validity testing is needed. Given the importance of organisational culture and security culture in determining secure behaviours, the following section will address the empirical literature that has explored the relationship between aspects of culture and information security.

Previous Research: ISA, Organisational Culture, Security Culture

Although research has not specifically explored the relationship between ISA, organisational culture, and security culture, some aspects of culture and ISA have been studied. For example, an exploratory quantitative study by Parsons et al. (2015) found a positive relationship between decision making and information security culture. Employees from organisations with better information security culture were more likely to have knowledge, attitudes, and behaviours in accordance with information security policy and procedures. These findings were supported by D'Arcy and Greene (2014).

Despite these exploratory findings, most information security literature has explored only some aspects of culture (e.g., organisation's mission, leadership, structure and style) and ISA, rather than measuring culture as a holistic construct. These components and others are discussed in relation to ISA.

A mixed-methods study by Schlienger and Teufel (2003) found support for an organisation's security mission in influencing an information security culture. It is suggested that effective organisational security policy should incorporate clear definitions of responsibilities to guide employees' understanding of acceptable and responsible security behaviour (Höne & Eloff, 2002; Schlienger & Teufel, 2003). The importance of an organisation's mission was supported by Ruighaver, Maynard, and Chang (2007), who found that long-term security policies and procedures were crucial to maintaining a strong security culture.

Employing a combination of field studies and structured surveys, Fourie (2003) found management support as the most significant factor affecting information security management activities. This was best achieved by defining and communicating a security policy, allocating specific responsibilities, making resources readily available for continual upkeep and control, monitoring and reviewing information security effectiveness, and supporting the establishment of a security culture. Other studies have found similar results and have emphasised the importance of senior management in encouraging good security behaviours through strategic management and planning, communication, and decision making (Stewart, 2005; Zakaria et al., 2007).

The influence of management on ISA is further supported by an industry based global survey that determined leadership support as the largest contributing factor to information security, above training and technical controls (Knapp et al., 2004). Management's preference for control or autonomy has also received preliminary support in relation to ISA. A self-report survey of 87 senior managers in Taiwan found a relationship between organisational culture and information security management control (Ernest Chang & Lin, 2007). It was found organisations with a control focussed culture were conducive to the development of information security management, with higher control indirectly discouraging information sharing among staff.

Further literature exploring individual autonomy and control has linked ISA and security behaviours to punishment. The literature suggests that constant monitoring and enforcement of individual employees' behaviours will influence compliance with policy. This suggests that individuals can be motivated to adopt security behaviour through drills and threats of punishment to non-compliance (Adams & Sasse, 1999). However, this study also noted employees typically required a perceived need for these behaviours. This is further supported by Xue, Liang, and Wu (2011) who found the effect of punishment expectancy on IT compliance was overshadowed by the perceived justice of punishment. This suggests that compliance is more strongly related to the shared attitudes concerning punishment. A more recent study suggests that an influencing strategy, including education and individual accountability, may be more effective than an enforcing one (Guo & Yuan, 2012). However, inconsistent punishment findings exist (Chen, Ramamurthy & Wen, 2012; Parsons et al. 2015; Sasse, Brostoff & Weirich, 2001), with Siponen and Vance (2012) suggesting punishment may only provide short-term benefits.

The style preference of an organisation is another aspect of culture that has received preliminary support. To date, ISA research has explored the comparison between people-oriented and task-oriented organisations. Connolly et al. (2017) found organisations that focussed more on developing people rather than measuring productivity were more likely to see greater compliance with information security. They were also more likely to have a positive-orientation to security behaviours. Additionally, high task-orientation was related to greater work pressure, which is linked to a negative-orientation to security behaviours, and a decreased likelihood of information security rule adherence. These findings were supported by Albrechtsen (2007) who found high information security workload can create a conflict of interest between functionality and information security behaviours.

A review by Chipperfield and Furnell (2010) found that flatter structures enabled better information security as the organisations could adapt to the external environment quicker, involved less bureaucracy, and received greater employee support. Having a structure that allows for collaboration has also received empirical support. Ruighaver, Maynard, and Chang (2007) also analysed security governance processes and structures, and showed that a lack of collaboration with stakeholders in daily decision-making negatively affected motivation and work orientation, leading to a narrow security focus. Koh et al. (2005) also found that collaboration in the security decision making process can be beneficial. This is because collaboration ensures employees feel responsible for their workplace security, and have a sense of ownership (Freeman, 2000; Ruighaver, Maynard & Chang, 2007).

Despite the positive influence of collaboration on security culture, it is imperative this is done in a structured and secure way. This is primarily because informal and social organisations have been linked to a negative-orientation to security behaviours due to mediocracy, consensus, and group think (Connolly et al., 2017). Additionally, it has been found that cooperativeness is negatively related to confidentiality, highlighting the difficulty in holding information secure, in an information sharing environment (Ernest Chang & Lin, 2007).

While these findings are limited, Crossler et al. (2013) and Shinn (2000) note that as our reliance on technology increases, change should be carefully managed as security is never guaranteed and organisations must ensure their security posture is not static. While these are the only studies that suggest flexible organisations display greater information security behaviours, adapting to the external environment is an important aspect of information security, due to the constant evolution of technology. These results have implications, discussed in the following section.

Discussion

In this review, we provide a detailed overview of the ISA, organisational culture and security culture literature, as well as the literature on the relationship between ISA and aspects of culture. In this section, we briefly discuss the theoretical and applied implications of this review, and propose a way forward.

Implications

The link between organisational culture and security culture has strong theoretical support (Martins & Eloff, 2002; Schlienger & Teufel, 2003), with both constructs sharing the basic underlying principles and structures proposed by Schein (1985). As discussed in this review, the relationship between aspects of organisational culture and ISA has received theoretical support. Although this is promising, there is a clear gap in the literature, due to the lack of empirical research examining this relationship.

Theoretically, this review provides a starting point for information security researchers. It has brought together multidisciplinary literature to provide a succinct summary of the problem space. This means it can be used to guide further theoretical developments and much needed empirical research. From an applied perspective, this review provides a summary of valid and reliable measurement instruments, that organisations can implement to assess their baseline level of organisational and security culture, and ISA.

Limitations & Future Research Directions

Security culture is a multi-disciplinary field, drawing on myriad of research methods, analyses and interpretations. Nonetheless, most studies rely on self-report (e.g. quantitative questionnaires, interviews, and focus groups). Although self-report is prone to common method variance and social desirability (Austin et al., 1998; Podsakoff & Organ, 1986; Spector, 1994), it enables systemisation, repeatability, comparability and convenience (Tucker, McCoy & Evans, 1990). Therefore, using valid and reliable self-report measures is recommended, particularly for exploratory research. Once empirical support has been established, mixed-method designs combining self-report, observational sampling, and case studies will increase the breadth of understanding (Workman et al., 2008). To reduce the effects of bias and enable generalisability of results (Faber & Fonseca, 2014), it is also recommended that future sample sizes are of a sufficient size.

While preliminary support exists for the relationship between ISA, organisational culture, and security culture; a study is yet to empirically explore all three. This literature review has identified a gap in the research and emphasises that an empirical examination is warranted. Based on these findings, future research should empirically examine the relative contribution of organisational culture and security culture on ISA, including the interplay between the three variables. Also, the extent to which security culture is a sub-component of organisational culture, as has been argued in the literature.

References

Adams, A., & Sasse, M. (1999). Users are not the enemy. *Communications of the ACM,42*(12), 40-46.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289.

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567-575.

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.

Al-Mayahi, I., & Mansoor, S. (2013). Information security culture assessment: Case study. In Proceedings of the *Information Science and Technology (ICIST), 2013 International Conference* (pp. 789-792). Yangzhou: China.

Alvesson, M., & Berg, P. (1992). *Corporate Culture and Organizational Symbolism: An Overview*. Berlin, New York: de Gruyter.

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report, 13*(4), 195-201.

Ashkanasy, N., Wilderom, C., & Peterson, M. (2000). *Handbook of organizational culture & climate.* Thousand Oaks, Calif, London: Sage Publications.

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.

Austin, E., Deary, I., Gibson, G., Mcgregor, M., & Dent, J. (1998). Individual response spread in self-report scales: Personality correlations and consequences. *Personality and Individual Differences, 24*(3), 421-438.

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

Barker, R. (1965). Explorations in ecological psychology. *American Psychologist, 20,* 1-14.

Baron, R. & Kenny, D. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology, 51*(6), 1173.

Berthon, P., Pitt, L., & Ewing, F. (2001). Corollaries of the collective: The influence of organizational culture and memory development on perceived decision-making context. *Journal of the Academy of Marketing Science, 29*(2), 135-150.

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

Blau, P., & Scott, W. (1962). *Formal Organizations: A Comparative Approach.* Toronto, Ontario: Chandler.

Borck, J. (2000). Keys to the privacy-enabled enterprise - Building trust across computing environments requires a combination of firewalls, VPNs, SSL, PKI, digital certificates.(Industry Trend or Event). *InfoWorld, 22*(37), 58-60.

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. *Journal of Organizational Behavior, 36*(3), 339-359.

Buchanan, D., & Huczynski, A. (2016). *Organizational Behaviour*. Harlow: Pearson Education Limited.

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.

Calic, D., Pattinson, M., Parsons, K., Butavicius, M. & McCormac, A. (2016). Naïve and accidental behaviours that compromise information security: what the experts think, In Furnell, S.M. and Clarke, N.L. (Eds), *Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance (HAISA 2016).* Frankfurt: Germany.

Cameron, K., & Quinn, Robert E. (2011). *Diagnosing and changing organizational culture: Based on the competing values framework (Third ed.).* San Francisco, CA: Jossey-Bass.

Cameron, K., & Ettington, D. (1988). *The Conceptual Foundations of Organizational Culture*. In Smart, J.C., ed. Higher Education: Handbook of Theory and Research. New York: Agathon.

Chen, Y., Ramamurthy, K., & Wen, K. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems,29*(3), 157-188.

Chia, P., Maynard, S., & Ruighaver, A. (2003). *Understanding organizational security culture*. In M. Hunter & K. Dhanda (Eds.), Information systems: The challenges of theory and practice (pp. 335–365). Las Vegas, USA: Information Institute.

Chipperfield, C., & Furnell, S. (2010). From security policy to practice: Sending the right messages. *Computer Fraud & Security, 2010*(3), 13-19.

Connolly, L., Lang, M., Gathegi, J., & Tygar, D. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information and Computer Security, 25*(2), 118-136.

Cooke, R., & Lafferty, J. (1983). *Level V: Organizational cultural inventory-form I.* Plymouth, MI: Human Synergistics.

Cooke, R., & Szumal, J. (1994). The Impact of Group Interaction Styles on Problem-Solving Effectiveness. *The Journal of Applied Behavioral Science, 30*(4), 415-437.

Cronk, L., & Salmon, C. (2017). Culture’s Influence on Behavior: Steps Toward a Theory. *Evolutionary Behavioral Sciences, 11*(1), 36-52.

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101.

Da Veiga, A., & Eloff, J. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207.

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.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees’ security compliance. *Information Management & Computer Security,22*(5), 474-489.

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*(1), 79-98.

Deal, T., & Kennedy, A. (1982). *Corporate cultures: The rites and rituals of corporate life.* Reading, Mass: Addison/Wesley.

Denison, D. (1990). *Corporate Culture and Organisational Effectiveness.* New York: John Wiley & Sons

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. *The Academy of Management Review,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.

Drexler, J. (1977). Organizational climate: Its homogeneity within organizations. *Journal of Applied Psychology, 62*(1), 38-42.

Egelman, S., & Peer, E. (2015). Predicting privacy and security attitudes. *ACM SIGCAS Computers and Society, 45*(1), 22-28.

Egelman, S., Harbach, M., & Peer, E. (2016) Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS). In Proceedings of the *SIGCHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA.

Ekvall, G. (1987). *The Climate Metaphor in Organization Theory*. In: Bass, B. and Drenth, P., Eds., Advances in Organizational Psychology pp 177-190. Beverly Hills: Sage.

Ernest Chang, S., & Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458.

Faber, J., & Fonseca, L. (2014). How sample size influences research outcomes. *Dental Press Journal of Orthodontics, 19*(4), 27-29.

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.

Fey, C., & Denison, D. (2003). Organizational culture and effectiveness: Can American theory be applied in Russia? *Organization Science, 14*(6), 686-706.

Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*(C), 26-44.

Fourie, L. (2003). The management of Information Security- A South Africa case study. *South Africa Journal of Business Management, 34*(2), 19-29.

Furnell, S., Jusoh, A., Katsabas, D. & Dowland, P. (2006). Considering the Usability of End-User Security Software. In Proceedings of the *21st IFIP International Information Security Conference (IFIP SEC 2006)*. Karlstad: Sweden.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(8), 983-988.

Furnell, S. (2007). IFIP workshop – Information security culture. *Computers & Security, 26*(1), 35.

Geertz, C. (1973). *The interpretation of cultures : Selected essays / by Clifford Geertz*. New York: Basic Books.

Gillespie, M., Denison, D., Haaland, S., Smerek, R., & Neale, W. (2008). Linking organizational culture and customer satisfaction: Results from two companies in different industries. *European Journal of Work and Organizational Psychology,17*(1), 112-132.

Grant, A (2012). Leading with meaning: Beneficiary contact, prosocial impact, and the performance effects of transformational leadership. *Academy of Management Journal 55*(2), 458-476.

Grant, G. (2005). Information sharing key to U.S. security. *Computerworld, 39*(27), 6.

Guion, R. (1973). A note on organizational climate. *Organizational Behavior and Human Performance, 9*(1), 120-125.

Guo, K., & Yuan, Y. (2012). The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model. *Information & Management, 49*(6), 320–326.

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

Hampden-Turner, C., & Trompenaars, F. (1997). Response to Geert Hofstede. *International Journal of Intercultural Relations, 21*(1), 149-159.

Handy, C. (1986). *Understanding organisations.* Harmondsworth: Penguine Books.

Harris, S. (1994). Organizational Culture and Individual Sensemaking: A Schema-Based Perspective. *Organization Science. 5*(3), 289-477.

Harrison, R. (1975). "Diagnosing organization ideology", in Jones, J.E. and Pfeiffer, J.W. (Eds), The 1975 Annual Handbook for Group Facilitators, University Associates, La Jolla, CA, pp. 101-7.

Harrison, R. (1972). Understanding your organisation's character. *Harvard Business Review, 50*(3), 119-128.

Hartnell, C., Ou, A., & Kinicki, A. (2011). Organizational culture and organizational effectiveness: A meta-analyticinvestigation of the competing values framework's theoretical suppositions. *Journal of Applied Psychology, 96*, 677–694.

Hassan, N., & Ismail, Z. (2012). A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment. *Procedia - Social and Behavioral Sciences, 65,* 1007-1012.

Hellriegel, D., Slocum, J.W. & Woodman, R.W. (1998) Organizational Behavior, 8th ed., South-Western College, Cincinnati, OH.

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

Höne, K., & Eloff, J. (2002). Information security policy — what do international information security standards say? *Computers & Security, 21*(5), 402-409.

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

James, L., & Jones, A. (1974). Organizational climate: A review of theory and research. *Psychological Bulletin, 81*(12), 1096-1112.

Johnson, G., & Scholes, K. (1997). *Exploring corporate strategy: Text and cases*. Prentice Hall, London: Financial Times.

Joyce, W., & Slocum, J. (1984). Collective Climate: Agreement as a Basis for Defining Aggregate Climates in Organizations. *The Academy of Management Journal*, *27*(4), 721-742.

Karjalainen, M., & Siponen, M. (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. *Journal of the Association for Information Systems, 12*(8), 518-555.

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013. *Information & Computer Security*, *23*(3), 246-285.

Knapp, K., Marshall, T., Rainer, R., & Morrow, D. (2006). The Top Information Security Issues Facing Organisations: What Can Government do to Help? *EDPACS, 34*(4), 1-10.

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, AB., Maynard, S., & Ahmad, A. (2005). Security Governance: Its Impact on Security Culture. *Proceedings of the 3rd Australian Information Security Management Conference: AISM*. Perth, Western Australia.

Kokina, I., & Ostrovska, I. (2013). The analysis of organizational culture with the Denison model: (the case study of Latvian municipality. *European Scientific Journal: Special Edition, 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. *Human Relations*, *65*(2), 241–262.

Koys, D., & Decotiis, T. (1991). Inductive measures of psychological climate. *Human Relations, 44,* 265-285.

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

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review, 37*(12), 1049-1092.

Lewin, K. (1951). *Field theory in social science: selected theoretical papers*. Oxford, England: Harpers.

Lewin, K., Lippitt, R., & White, R. (1939). Patterns of aggressive behavior in experimentally created social climates. *Journal of Social Psychology, 10*(2), 271.

Likert, R. (1961). *New Patterns of Management.* New York: McGraw-Hill.

Lundy, O., & Cowling, A. (1995). *Strategic human resource management / Olive Lundy and Alan Cowling.* New York: Routledge.

Mahfuth, A., Yussof, S., Baker, A., & Ali, N. (2017). A systematic literature review: Information security culture. In Proceedings of the *5th International Conference on Research and Innovation in Information Systems: Social Transformation through Data Science,* ICRIIS 2017, IEEE Computer Society. Langkawi Island: Malaysia.

Martin, J., & Siehl, C. (1983). Organizational Culture and Counterculture: An Uneasy Symbiosis. *Organizational Dynamics, 12,* 52-64.

Martins, A., & Eloff, J. (2002). Information Security Culture. *Paper presented at the 17th International Conference on Information Security.* Cairo, Egypt.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2017a). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156.

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

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 & Computer Security, 26*(3), 277-289.

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

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences, 147*, 424-428.

Mohr, L. (1982). *Explaining organizational behavior*. San Francisco: Jossey-Bass.

Moran, E., & Volkwein, J. (1992). The Cultural Approach to the Formation of Organizational Climate. *Human Relations, 45*(1), 19-47.

Mowday, R., & Sutton, R. (1993). Organizational Behavior: Linking Individuals and Groups to Organizational Contexts. *Annual Review of Psychology, 44*(1), 195-229.

Nosworthy, J. (2000). Implementing Information Security In The 21st Century — Do You Have the Balancing Factors? *Computers & Security, 19*(4), 337-347.

O'Driscoll, M., & Evans, R. (1988). Organizational Factors and Perceptions of Climate in Three Psychiatric Units. *Human Relations, 41*(5), 371-388.

Öğütçü, M., Testik, Ö., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93.

O'Reilly, C., Chatman, J., & Caldwell, D. (1991). People and Organisational Culture: A profile comparison approach to assessing person-organization fit. *Academy of 233 Management Journal, 34*(3), 487-516.

Organisation for Economic Co-operation and Development [OECD]. (2004). *Principles of Corporate Governance.* Retrieved from oecd.org/corporate/ca/corporategovernanceprinciples/31557724.pdf

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

Ott, J. (1989). *The organizational culture perspective*. Chicago, Ill: Dorsey Press.

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

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176.

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M., & Jerram, C. (2015). The Influence of Organisational Information Security Culture on Cybersecurity Decision Making. *Journal of Cognitive Engineering and Decision Making: Special Issue on Cybersecurity Decision Making, 9*(2), 117-129.

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: A comparison of two studies. *Information and Computer Security,24*(2), 228-240.

Peters, T. (1978) Symbols, patterns and settings. *Organizational Dynamics, 9*(2), 3-23.

Pettigrew, A. (1979). On studying organizational cultures. *Administrative Science Quarterly, 24,* 570-81.

Pfleeger, C. (1997). The fundamentals of information security. *Software, IEEE, 14*(1), 15-16.

Pfleeger, S., & Caputo, D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611.

Podsakoff, P., & Organ, D. (1986). Self-Reports in Organizational Research: Problems and Prospects. *Journal of Management, 12*(4), 531-544.

Pricewaterhouse Coopers. (2016). *Key findings from the global state of information security survey 2016. Turnaround and transformation in cyber security.* Retrieved from pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf

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

Quinn, R., & Rohrbaugh, J. (1983). A Spatial Model of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Analysis. *Management Science, 29*(3), 363-377.

Reid, R., & van Niekerk, J. (2014). Brain-compatible, web-based information security education: A statistical study. *Information Management & Computer Security, 22*(4), 371-381.

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

Rousseau, D. (1990). Normative Beliefs in Fund-Raising Organizations: Linking Culture to Organizational Performance and Individual Responses. *Group & Organization Management, 15*(4), 448-460.

Ruighaver, A., Maynard, S., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.

Ryder, P., & Southey, G. (1990). An exploratory study of the Jones and James organisational climate scales. *Asia Pacific Journal of Human Resources Management*, *28*(3). 45-52.

Sackmann, S. (2011). *Culture and performance*. In N. Ashkanasy, C. Wilderom, & M. Peterson (Eds.), The handbook oforganizational culture and climate (2nd edn., pp. 188–224). Thousand Oaks, CA: Sage Publications.

Sanders, J. (2016). Defining terms: Data, information and knowledge. *SAI Computing Conference (SAI), 2016*, 223-228.

Sasse, A., Brostoff, AMR., & Weirich, D. (2001). Transforming the 'weakest link' - a human-computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122 - 131.

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

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

Schein, E. (1999). Empowerment, coercive persuasion and organizational learning: Do they connect? *The Learning Organization, 6*(4), 163-172.

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

Schein, E. (1986). What you need to know about organizational culture. *Training and Development Journal, 40*(1), 30-34.

Schein, E. (1990). Organizational culture. *American Psychologist, 45,* 109-19.

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

Schneider, B. (1985). Organizational behavior. *Annual Review of Psychology, 36*(1), 573-611.

Schneider, B., Ehrhart, M., & Macey, W. (2011). Perspectives on organizational climate and culture. *APA handbook of industrial and organizational psychology, 1,* 373-414.

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. *Journal of Applied Psychology*, *102*(3), 468-482.

Schneider, B., & Snyder, R. (1975). Some relationships between job satisfaction and organization climate. *Journal of Applied Psychology*, *60*(3), 318-328.

Schulz, D. (2005). *Bureau of Industry and Security*. Encyclopedia of Law Enforcement, 566-568.

Schwartz, H., & Davis, S. (1981). Matching Corporate Culture and Business Strategy. *Organizational Dynamics, 10,* 30-48.

Sempane, M., Rieger, H., & Roodt, G. (2002). Job Satisfaction In Relation To Organisational Culture. *SA Journal of Industrial Psychology, 28*(2), 23-30.

Shinn M. (2000). Security for your e-business. *Enterprise Systems Journal, 15*(8), 18.

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. *AMCIS 2006 Proceedings*. 415. aisel.aisnet.org/amcis2006/415. Acapulco: México.

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

Siponen, M., & Vance, A. (2012). IS Security Policy Violations: A Rational Choice Perspective. *Journal of Organizational and End User Computing (JOEUC), 24*(1), 21-41.

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.

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.

Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Stewart, A. (2005). Information security technologies as a commodity input. *Information Management & Computer Security, 13*(1), 5-15.

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information Technology and Management, 17*(2), 179-186.

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.

Thomson, K., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security, 2006*(10), 7-11.

Tucker, R., Mccoy, W., & Evans, L. (1990). Can Questionnaires Objectively Assess Organisational Culture? *Journal of Managerial Psychology, 5*(4), 4-11.

Utz, S. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 3*(2).

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

Van Niekerk, J., & von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486.

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

Velki, T., Solic, K., & Ocevcic, H. (2014). Development of Users' Information Security Awareness Questionnaire (UISAQ); Ongoing work. *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on,*1417-1421. Opatija: Croatia.

Von Solms, B. (2000). Information security - the third wave. *Computers & Security, 19*(7), 615-620.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

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

Wallace, J., Hunt, J., & Richards, C. (1999). The relationship between organisational culture, organisational climate and managerial values. *International Journal of Public Sector Management, 12*(7), 548-564.

Workman, M., Bommer, W., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

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. *Information Systems Research, 22*(2), 400-414,416-417.

Yilmaz, C., & Ergun, E. (2008). Organizational culture and firm effectiveness: An examination of relative effects of culture traits and the balanced culture hypothesis in an emerging economy. *Journal of World Business, 43*(3), 290-306.

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.

Research Report

Word count: 5. 444

Culture and Information Security Awareness: Examining the Role of Organisational and Security Culture

Ashleigh Wiley

Affiliation: The University of Adelaide

Postal Address: The University of Adelaide
SA 5005
AUSTRALIA

Email Address: [redacted]

Declarations of interest: none

Abstract

The relationship between security culture and ISA has received preliminary support; however, its interplay with organisational culture is yet to be empirically explored. Therefore, this study examined 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 mediated the relationship between organisational culture and ISA. This finding has important applied implications. Organisations can improve ISA by focussing on security culture rather than organisational culture, saving them time and resources. Future research could further extend current findings by also considering national culture.

Keywords: Security Culture, Organisational Culture, ISA, Cyber

1. Introduction

Human behaviour is largely determined by culture, affecting interactions in social and work environments (Cronk & 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 infrastructure and their interaction (Grant, 2005; Tessem & Skaraas, 2005). This is important for information security, as humans 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; Pfleeger & Caputo, 2012; Wood & Banks, 1993). To further understand the role humans play in information security, this study explores the relationship between employee Information Security Awareness (ISA)[1], and organisational and security culture. These constructs have not been empirically studied in combination.

Traditionally, information security has been approached from a computer science perspective, focussing solely on technical measures to mitigate risks (Aurigemma & Panko, 2012). However, the importance of the human factor has become increasingly recognised (e.g., Herath & Rao, 2009; Metalidou et al., 2014; Vroom & von Solms, 2004). It has been well established that technical solutions in isolation cannot sufficiently mitigate security breaches (e.g., Furnell & Clarke, 2012; Pfleeger & Caputo, 2012; Schulz, 2005). The role of the human is crucial with humans being the weakest link in information security (IBM, 2014; Schlienger & Teufel, 2003; von Solms & 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 (Crossler et al., 2013; Reid & Niekerk, 2014; Thomson,

[1] ISA: Information Security Awareness

von Solms & Louw, 2006). 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], 2016, 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 (ACSC, 2017). As technical solutions alone are insufficient, and with the increase in information security risks, it is important we understand the factors contributing to ISA. The current study will examine the relationships between ISA, organisational culture, and security culture. These constructs will be discussed in the following sections.

1.1 Information Security Awareness

Understanding Information Security Awareness (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 organisations information security policies, rules, and guidelines, and the extent to which they behave in accordance with these policies, rules and guidelines (Bulgurcu, Cavusoglu & Benbasat, 2010; Kruger & Kearney, 2006; 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 (Bulgurcu, Cavusoglu & Benbasat, 2010; Kruger & Kearney, 2006; Parsons et al., 2014; Siponen, 2000). While this model has been criticised by some researchers, evidence of its validity has been established (Bettinghaus, 1986; Van der Linden, 2012), and its use supported (McGuire, 1969).

The KAB model underpins the Human Aspects of Information Security Questionnaire (HAIS-Q). The HAIS-Q has received significant theoretical support (Parsons et al., 2014, 2017) and has undergone sufficient reliability and validity testing on diverse populations (Hadlington & Parsons, 2017; McCormac et al., 2016, 2017b; Parsons et al., 2017). Other attempts to measure ISA have been limited by either focussing on information security breaches or aspects of ISA (D'Arcy, Hovav & Galletta, 2009; PwC, 2018; Stanton et al., 2005), and require further reliability and validity testing (Egelman, Harbach & Peer, 2016; Öğütçü, Testik & Chouseinoglou, 2016; Solic, Velki & Galba, 2015; Velki, Solic & Ocevcic, 2014).

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 affect information security behaviours (McCormac et al., 2017a, 2018; Shropshire et al. 2006). 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), females, individuals who are more conscientious and agreeable, individuals displaying greater resilience, individuals with a higher education level, and those with a propensity to take fewer risks (McCormac et al. 2017a; McCormac et al., 2018; Öğütçü, Testik, & Chouseinoglou, 2016; Pattinson et al., 2016).

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 (Da Veiga & Eloff, 2010; OECD, 2004, 2015; Schlienger & Teufel, 2003) research in the area is still preliminary. Current literature suggests that security culture should be part of organisational culture (Schlienger & Teufel, 2003; von Solms, 2000), as information is best protected when individuals understand, internalise and behave to information security standards (van Niekerk & von Solms, 2005; Sanders, 2016; Thomson, von Solms & Louw, 2006).

1.2 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 & 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, that has worked well enough to be considered valid and, therefore, 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, 1986, 1990). Schein's (1985, 1992, 2004) 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. Other prominent researchers also dominate the field of organisational culture, each offering a unique perspective on the complex phenomenon. These theories vary in their approach, complexity, applicability and empirical support (Cameron & Quinn, 2011; Deal & Kennedy, 1982; Harrison, 1972; O'Reilly, Chatman, & Caldwell 1991; Quinn & Rohrbaugh, 1983).

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 (Denison et al., 2006). Due to its confirmed reliability, validity and demonstrated link to behavioural outcomes (e.g., Gillespie et al., 2008; Kotrba et al., 2012; Yilmaz & Ergun, 2008), the Denison Organisational Culture Survey (DOCS) is the most widely used measure for assessing organisational culture (Kokina & Ostrovska, 2013; Sackmann, 2011; Schneider, Ehrhart, & Macey, 2011). Other measures also demonstrate similar reliability estimates, however, they have not been linked as strongly to behaviour (e.g., OCP - O'Reilly, Chatman & Caldwell, 1991), are of a longer duration (e.g., OCI - Cooke & Szumal, 1994) or are quite costly, with an inability to receive raw data (e.g., OCAI - Cameron & Quinn, 2011).

The study and measurement of culture is important due to its influence on individual and group behaviours and subsequent relationships with organisational behaviours such as job satisfaction (Fey & Denison, 2003; Sempane, Rieger & Roodt, 2002; Schneider & Snyder, 1975) and job performance (Boyce et al., 2015; Hartnell, Ou & Kinicki, 2011; Sackmann, 2011). 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 (Ryder & Southey, 1990; Schneider et al., 2017: Schwartz & Davis, 1981), however, now distinctions are primarily in interpretation (Denison, 1996; Moran & Volkwein, 1992).

1.3 Security Culture

An understanding of organisational culture is fundamental when trying to understand security culture (Ruighaver, Maynard & Chang, 2007; Mowday & Sutton, 1993). This is because effective security is strongly entrenched within organisational culture (Da Veiga & Martins, 2015) and is often explained as a sub-culture of organisational culture (Borck, 2000; Connolly et al., 2017; Ruighaver, Maynard & Chang, 2007). Therefore, it cannot be assessed in isolation. The focus on security culture is relatively new. Its growth in the literature is primarily attributed to our significant reliance on information systems and digital devices, coupled with the social and political environment surrounding the safeguarding of information. Therefore, 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 (D'Arcy, Hovav & Galletta, 2009; Hassan & Ismail, 2012; Knapp et al., 2006). 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 (1985) 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, procedures, daily tasks and activities. It is shaped through a combination of both the internal and external environments (Da Veiga & Martins, 2015;

Thompson, von Solms & Louw, 2006). 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 & Eloff, 2010; Mahfuth et al., 2017; Schlienger & Teufel, 2003). A strong security culture exists when individuals are aware of security risks and preventative measures, and when individuals assume responsibility and take the required steps to improve the security of their information systems and networks (Business and Advisory Committee to the OECD, 2004). The primary objective of a strong security culture is to protect information assets by influencing employees. This can be achieved through increasing information security awareness in order to improve the security behaviour of employees (Furnell, 2007).

Despite ample theoretical support, the measurement of security culture is limited. While security culture tools have been developed (Al-Mayahi & Mansoor, 2013; Alhogail & Mirza, 2014; Ashenden, 2008; Da Veiga & Martins, 2015; Flores and Ekstedt, 2016; Karlsson, Åström & Karlsson, 2015; Martins & Eloff, 2002; Schlienger & Teufel, 2003), a publicly available, comprehensive, validated and reliable security culture instrument is not currently available. 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 address the empirical literature that has explored the relationship between culture and ISA.

1.4 Previous Research: ISA, Organisational Culture, Security Culture

As previously explained, theoretical support exists for the relationship between organisational culture and security culture (Nosworthy, 2000) and between security culture and ISA (Da Veiga & Eloff, 2010; Schlienger & Teufel, 2003). Despite this, limited empirical support exists.

An exploratory quantitative study by Parsons et al. (2015) found a positive relationship between ISA and security culture. Employees from organisations with better information security culture were more likely to have knowledge, attitudes, and behaviours in accordance with information security policy and procedures. D'Arcy and Greene (2014) had similar findings in their 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 influence of leadership support on information security management (Fourie, 2003; Knapp et al., 2004) and the creation of a security culture (Stewart, 2005; Zakaria et al., 2007). These studies emphasised the importance of leaders in encouraging good security behaviours through strategic management and planning, communication, and decision making. In addition, it was also found that an organisations security mission was strongly linked to their security culture (Höne & Eloff, 2002; Ruighaver, Maynard, & Chang, 2007; Schlienger & Teufel, 2003).

Limited support has been found for other culture constructs. Benefits of collaboration in decision making was found to improve both security behaviours and culture (Koh et al., 2005; Ruighaver, Maynard & Chang, 2007), as involvement gave employees a sense of ownership around security management. It was also found people-oriented organisations were more likely to see a positive-orientation to ISA (Albrechtsen, 2007; Connolly et al., 2017), as a focus on task-orientation can create a conflict of interest between functionality and information security behaviours. Lastly, while findings vary for the influence of punishment on ISA (Chen, Ramamurthy & Wen, 2012; Parsons et al. 2015; Sasse, Brostoff & Weirich, 2001), the importance of punishment expectancy and the perceived justice of punishment on ISA has been noted (Xue, Liang, & Wu, 2011).

These findings provide preliminary empirical evidence to support the strong theoretical literature linking ISA, organisational culture and security culture.

1.5 Study aims

While theoretical support exists for the relationship between ISA, organisational culture, and security culture; a study is yet to empirically examine the contribution of all three. This study aims to empirically investigate the relationship between ISA, organisational culture and security culture. Given the previous findings relating to demographic variables (e.g. age and gender) and their relationship to ISA (McCormac et al., 2017a, 2018; Pattinson et al., 2016), the influence of these variables will also be analysed. Therefore it is hypothesised that organisational culture, security culture and ISA will be positively related.

2. 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. Ethics approval was granted by the Human Research Ethics Subcommittee of the University of Adelaide School of Psychology. Participants took on average 20 minutes to complete the survey.

2.1 Participants

A total of 508 (300 females, 207 males, 1 gender unspecified) working Australians completed the online questionnaire. Participants were primarily casual/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, roles and levels (see Table 1 for detailed participant demographics). Comparative to the Australian population (ABS, 2016) our sample demographics were relatively representative, however, included a larger proportion of females and younger adults.

Table 1
Participant Demographics

	Participants (*N* = 508)
	N (%)
Age Categories	
18-29	144 (28)
30-39	144 (28)
40-49	85 (17)
50-59	75 (15)
> 60	62 (12)
Employment Sector	
Government	172 (34)
Non-Government	335 (66)
Industry	
Health and Community Services	75 (15)
Retail and Wholesale	110 (25)
Education & Research	54 (11)
Finance, Banking, Insurance & Business Services	55 (11)
Mining, Manufacturing and Construction	66 (13)
Government and Defence	30 (6)
IT	28 (6)
Other	90 (18)

2.1.1. Inclusion and Exclusion Criteria

Participants were required to be over the age of 18, currently employed, working within Australia, and spent some of their time at work on a computer. Quality control measures were also implemented. Participants who declined the question ‘do you commit to thoughtfully provide your best answers to each question in this survey?’ or who appeared to not be providing considered responses were removed during survey participation. For example, this included participants who responded using only one response category, irrespective of reverse scoring. Additionally, a further eight responses were excluded from the sample, as their answers indicated a lack of content responsiveness. Exclusion was based on the content non-responsivity criteria, outlined in Parsons et al. (2014).

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, position level, industry sector, organisation size, frequency of using electronic devices at work, and information security education.

2.2.2. 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 .96 for ISA. These are consistent with alpha levels reported in previous studies (e.g., McCormac et al. 2016, 2017a). For detailed validity and reliability assessments of the HAIS-Q, refer to Parsons et al. (2017) and McCormac et al. (2016). A sample knowledge item is "*I can't be fired for something I have posted on social media.*"

2.2.3. Organisational Culture: DOCS Denison Organisational Culture Survey

The DOCS (Denison et al., 2006) measures organisational culture through four traits; 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 .97, which is considered reliable and is consistent with previous studies (Kotrba et al., 2012). The DOCS has demonstrated adequate Factor Analysis and validity (Denison & Mishra, 1995; Kotrba et al. 2012). A sample item from the involvement: empowerment index is “*Most employees are highly involved in their work.*”

Consistent with the approach of Boyce et al. (2015), we derived an index for overall culture by taking the mean across all four culture traits. While this approach is not sensitive to potential differences at the trait level, given the high trait correlations, resulting in consistent mediation patterns, and the exploratory purpose of the study, this method was most suitable.

2.2.4. Security Culture: Organisational Security Culture Measure

The Organisational Security Culture Measure assesses an organisation’s information 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 .71 has been previously reported (Parsons et al., 2015), and the results of this study found the measure to have an alpha value of .69. A sample item is “*Most of my colleagues generally behave in a secure manner when they are using a computer.*”

3. Results

Table 2 presents a correlation matrix, including mean and standard deviation scores, to examine the relationship between ISA, organisational culture, security culture, gender, and age. Organisational demographic variables relating to position level, employment sector, industry, and organisation size were also examined. There were no significant relationships found between organisational demographic variables and ISA, organisational culture and security culture. Therefore, they are not reported further.

Inspection of the distribution of scores indicated that ISA scores were slightly negatively skewed, whereas, organisational culture and security culture were normally distributed. However, it is generally accepted that most parametric and non-parametric tests, are largely robust to such minor violations of normality (Edgell, Noon & Zeaman, 1984; McHugh, 2013). Parametric testing has demonstrated robust effects even when the assumption of normality is violated (Edgell, Noon & Zeaman, 1984; Schmider et al., 2010), particularly when sample size is greater than 200 (Tabachnick & Fidell, 2013). Four outliers were identified from the organisational culture measure. However, Cook's Distance score ascertained that the four outliers, as determined by Mahalanobis Distance, didn't change the significance of reported results. Therefore, they were included in the analysis to better represent the diversity of the population. Collinearity diagnostics analysis revealed that tolerance values were all greater than .10 and the variance inflation factor values were all well below 10, suggesting that multi-collinearity had not been violated.

Table 2

Correlations and Descriptive Statistics; ISA, Organisational Culture, Security Culture, Age, Gender (N=508)

Variables	Gender	Age	ISA	Security Culture	Organisational Culture
Age	- .13**				
ISA	.16**	.25**			
Security Culture	.10*	.11*	.55**		
Organisational Culture	.03	.01	.25**	.50**	
Mean	***	***	259.33	3.57	3.59
SD	***	***	35.71	.64	.59

Note. **p* < .05; ***p* < .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.

3.1 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 ή^{2}= .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 to the 40-49 group (*M* = 265.13, *SD* = 33.99), the 50-59 group (*M* = 268.05, *SD* = 33.30), and the 60+ 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 to 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); 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., 2017a).

3.2 ISA, Organisational Culture, Information Security Culture

A three-stage hierarchical regression was used to investigate the extent to which organisational culture and security culture predicted ISA. Preliminary analyses were conducted to ensure no violation of the assumptions of normality, linearity, multicollinearity and homoscedasticity. The results of the regression are summarised in Table 3.To control for the effects of age and gender, which have been previously found to predict ISA (McCormac et al. 2017a), these variables were entered at Stage 1. Strong theoretical literature highlights the importance of organisational culture on individual and group behaviours (Boyce et al., 2015; Cronk & Salmon, 2017); therefore, this variable was entered at Stage 2. The addition of organisational culture to the model, explained an additional 5% of variance. As security culture is often explained as a sub-component of organisational culture (Borck, 2000; Connolly et al., 2017; Ruighaver, Maynard & Chang, 2007; Schlienger & Teufel 2003), it was entered at Stage 3. Entering security culture into the model explained an additional 20% of variance, with the final model explaining a total of 35% variance in ISA. However, despite the initial contribution and significant correlation with ISA, the contribution of organisational culture was no longer significant. To further investigate this we conducted a mediation analysis, examining the relationship between ISA, organisational culture and security culture.

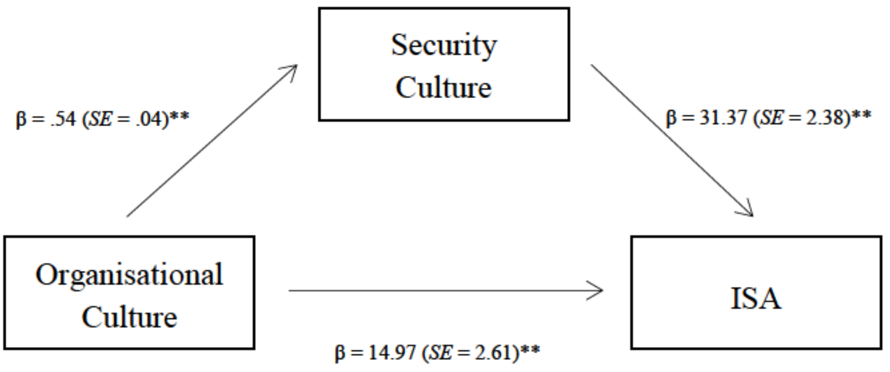
Table 3

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	<.001
Gender	13.88	4.52	<.001
Stage 2	$F_{(3, 507)}$ = 30.97, adjusted R^2 = 0.15**		
Age	6.80	6.55	<.001
Gender	13.39	4.50	<.001
Organisational culture	14.53	5.87	<.001
Stage 3	$F_{(4, 507)}$ = 68.78, adjusted R^2 = 0.35**		
Age	5.21	5.67	<.001
Gender	9.60	3.66	<.001
Organisational culture	-1.02	- .41	.68
Security culture	28.88	12.41	<.001

Note. *p < .05; **p < .001

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



Note. ** $p < .001$

Figure 1: Model testing hypothesis; Security Culture mediates the relationship between Organisational Culture and ISA.

4. Discussion

A large body of literature explores aspects relating to organisational culture and ISA separately, however, there is limited literature exploring the relationship between ISA, organisational culture and security culture. Therefore, the aim of this study was to empirically examine the relationship between ISA, organisational culture, and security culture. The following sections will discuss the study’s findings, applications, limitations and future directions.

4.1 Findings and Implications

In line with the overarching hypothesis, we found a significant positive relationship between ISA, organisational culture and security culture. Furthermore, after controlling for age and gender, organisational culture and security culture predicted approximately 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 the theoretical literature (Da Veiga & Martins, 2015) and can be partially explained by suggesting security culture is a sub-component of organisational culture (Schlienger & Teufel 2003; van Niekerk & von Solms 2005), with both constructs sharing the same theoretical underpinning derived from Schein’s (1985) theory.

A significant positive liner relationship was also found between security culture and ISA, consistent with the theoretical (Da Veiga & Eloff, 2010) and preliminary empirical literature (Parsons et al., 2014). As security culture increased, so did ISA; individuals from organisations with higher security culture scores were more likely to have higher ISA. Conversely, individuals from organisations with lower security culture scores were more likely to have lower ISA scores.

Despite these linear relationships, the study found a more complex relationship which explained the interplay between organisational culture, security culture and ISA. Our findings suggest 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. However, as organisational culture is still a predictor of performance (Boyce et al., 2015; Hartnell, Ou & Kinicki, 2011; Sackmann, 2011), job satisfaction (Fey & Denison, 2003; Sempane, Rieger & Roodt, 2002), and ISA, its importance within the information security literature still remains.

Relationships between ISA and demographic variables were also found. A positive linear relationship between age and ISA was found, with ISA improving as age increased. However, the distinction between age brackets began to plateau as age increased (>40 years). Similar findings were also reported by Pattinson et al. (2015), McCormac et al., (2017a), and McCormac et al. (2018). Further support for age-related ISA differences have also been found in phishing studies (Jagatic et al., 2007; Pattinson et al., 2012; Sheng et al., 2010). Inconsistent with previous research (McCormac et al., 2017a, 2018), a significant main effect was not found between male and female ISA scores.

4.1.1 Applied Implications

These findings have both theoretical and practical implications. The results contribute to the theoretical literature by providing support for the relationship between ISA, organisational culture and security culture. More specifically, the study provides empirical support to confirm the relationship between security culture and ISA, which to date has been primarily theoretical (Da Veiga & Eloff, 2010; van Niekerk & von Solms, 2010). It also provides further support for the relationship between organisational culture and ISA, by suggesting that the relationship is largely mediated by security culture.

Organisational culture is deeply ingrained within an organisation and can be difficult to change (Schein, 1999). However, as security culture is a sub-component of organisational culture (Schlienger & Teufel, 2003; van Niekerk & von Solms, 2005), and is less encompassing, it may be easier to change. Therefore, from a practical perspective, organisations would more effectively utilise their resources by focusing on security culture to improve 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 as well. It is therefore recommended that organisations hoping to improve ISA may target security culture through infrastructure (e.g., technical and procedural) and group norms (e.g., mechanisms such as management support) rather than overall organisational cultural change.

4.2 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 assessment of organisational culture (Ashkanasy et al., 2000; Ott, 1989; Sackmann, 2011; Tucker, McCoy & Evans, 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 (Austin et al., 1998; Podsakoff & Organ, 1986; Spector, 1994), yet it allows for systemisation, repeatability, comparability and convenience (Tucker, McCoy & Evans, 1990).

Given this was an exploratory study, using a survey-based quantitative method alone was justified. In addition, to reduce the previously mentioned effects, this study also implemented quality control measures, and guaranteed confidentiality and anonymity (Donaldson & Grant-Vallone, 2002). However, to offset some of these weaknesses and to provide a greater breadth of understanding, it is recommended that future studies use a mixed methods design.

The measurement tools used in this study may also present a limitation. A short security culture measurement tool was used. Currently a comprehensive, valid and reliable measure of security culture is yet to be published. However, the 6-item tool demonstrated sound reliability, and due to the exploratory nature of this study was sufficient. Given these findings, further development and validation of a security culture measure is warranted. In addition, the DOCS culture tool has shown considerable reliability and validity, and is the most widely used organisation culture assessment tool (Kokina & 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 traits 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 individual differences. While the DOCS model is applicable for assessing organisational culture globally (Denison et al., 2012), the influence of national culture on organisational culture, security culture and ISA is likely. Hofstede and Minkov (2010), Schein (2004) and House et al. (2004), have 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 (McCormac et al. 2017a, 2018; Pattinson et al., 2016; Shropshire et al. 2006), incorporating these into a more comprehensive model with culture could be beneficial. This would give organisations and industry practitioners a greater understanding of the factors contributing to ISA of their employees. In turn, this could influence and inform intervention initiatives such as training programs, strategy development, risk analysis modelling and culture change.

4.3. Conclusion

This study empirically examined the relationship between ISA, organisational culture and security culture. It was found that security culture played a mediating role in the relationship between organisational culture and ISA. These findings have important theoretical and applied implications. Theoretically, the results of this study can be further developed by future research to more comprehensively investigate these relationships. From an applied perspective, rather than focussing on the broader organisational culture which may be more time consuming and resource intensive, organisations may achieve greater employee ISA by focussing on developing and strengthening their organisation's security culture.

5. References

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289.

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.

Al-Mayahi, I., & Mansoor, S. (2013). Information security culture assessment: Case study. In Proceedings of the *Information Science and Technology (ICIST), 2013 International Conference* (pp. 789-792). Yangzhou: China.

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report, 13*(4), 195-201.

Ashkanasy, N., Wilderom, C., & Peterson, M. (2000). *Handbook of organizational culture & climate.* Thousand Oaks, Calif, London: Sage Publications.

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.

Austin, E., Deary, I., Gibson, G., Mcgregor, M., & Dent, J. (1998). Individual response spread in self-report scales: Personality correlations and consequences. *Personality and Individual Differences, 24*(3), 421-438.

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. *Journal of Personality and Social Psychology, 51*(6), 1173.

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

Borck, J. (2000). Keys to the privacy-enabled enterprise - Building trust across computing environments requires a combination of firewalls, VPNs, SSL, PKI, digital certificates.(Industry Trend or Event). *InfoWorld, 22*(37), 58-60.

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. *Journal of Organizational Behavior, 36*(3), 339-359.

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.

Cameron, K., & Quinn, Robert E. (2011). *Diagnosing and changing organizational culture: Based on the competing values framework (Third ed.).* San Francisco, CA: Jossey-Bass.

Chen, Y., Ramamurthy, K., & Wen, K. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems,29*(3), 157-188.

Connolly, L., Lang, M., Gathegi, J., & Tygar, D. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information and Computer Security, 25*(2), 118-136.

Cooke, R., & Szumal, J. (1994). The Impact of Group Interaction Styles on Problem-Solving Effectiveness. *The Journal of Applied Behavioral Science, 30*(4), 415-437.

Cronk, L., & Salmon, C. (2017). Culture’s Influence on Behavior: Steps Toward a Theory. *Evolutionary Behavioral Sciences, 11*(1), 36-52.

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101.

Da Veiga, A., & Eloff, J. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207.

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.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees’ security compliance. *Information Management & Computer Security,22*(5), 474-489.

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*(1), 79-98.

Deal, T., & Kennedy, A. (1982). *Corporate cultures: The rites and rituals of corporate life.* Reading, Mass: Addison/Wesley.

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. *The Academy of Management Review,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.

Denison, D., & Mishra, A., (1995). Toward a theory of organizational culture and effectiveness. *Organization Science, 6*(2), 204–223.

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

Edgell, S., Noon, S., & Zeaman, D. (1984). Effect of violation of normality on the t test of the correlation coefficient. *Psychological Bulletin, 95*(3), 576-583.

Egelman, S., Harbach, M., & Peer, E. (2016) Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS). In Proceedings of the *SIGCHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA.

Fey, C., & Denison, D. (2003). Organizational culture and effectiveness: Can American theory be applied in Russia? *Organization Science, 14*(6), 686-706.

Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*(C), 26-44.

Fourie, L. (2003). The management of Information Security- A South Africa case study. *South Africa Journal of Business Management, 34*(2), 19-29.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(8), 983-988.

Furnell, S. (2007). IFIP workshop – Information security culture. *Computers & Security, 26*(1), 35.

Geertz, C. (1973). *The interpretation of cultures : Selected essays / by Clifford Geertz*. New York: Basic Books.

Gillespie, M., Denison, D., Haaland, S., Smerek, R., & Neale, W. (2008). Linking organizational culture and customer satisfaction: Results from two companies in different industries. *European Journal of Work and Organizational Psychology,17*(1), 112-132.

Grant, G. (2005). Information sharing key to U.S. security. *Computerworld, 39*(27), 6.

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

Harrison, R. (1972). Understanding your organisation's character. *Harvard Business Review, 50*(3), 119-128.

Hartnell, C., Ou, A., & Kinicki, A. (2011). Organizational culture and organizational effectiveness: A meta-analyticinvestigation of the competing values framework's theoretical suppositions. *Journal of Applied Psychology, 96*, 677–694.

Hassan, N., & Ismail, Z. (2012). A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment. *Procedia - Social and Behavioral Sciences, 65,* 1007-1012.

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

Höne, K., & Eloff, J. (2002). Information security policy — what do international information security standards say? *Computers & Security, 21*(5), 402-409.

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

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

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture – state-of-the-art review between 2000 and 2013. *Information & Computer Security*, *23*(3), 246-285.

Knapp, K., Marshall, T., Rainer, R., & Morrow, D. (2006). The Top Information Security Issues Facing Organisations: What Can Government do to Help? *EDPACS, 34*(4), 1-10.

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, AB., Maynard, S., & Ahmad, A. (2005). Security Governance: Its Impact on Security Culture. *Proceedings of the 3rd Australian Information Security Management Conference: AISM*. Perth, Western Australia.

Kokina, I., & Ostrovska, I. (2013). The analysis of organizational culture with the Denison model: (the case study of Latvian municipality. *European Scientific Journal: Special Edition, 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. *Human Relations*, *65*(2), 241–262.

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

Lundy, O., & Cowling, A. (1995). *Strategic human resource management / Olive Lundy and Alan Cowling.* New York: Routledge.

Mahfuth, A., Yussof, S., Baker, A., & Ali, N. (2017). A systematic literature review: Information security culture. In Proceedings of the *5th International Conference on Research and Innovation in Information Systems: Social Transformation through Data Science*, ICRIIS 2017, IEEE Computer Society. Langkawi Island: Malaysia.

Martins, A., & Eloff, J. (2002). Information Security Culture. *Paper presented at the 17th International Conference on Information Security.* Cairo, Egypt.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2017a). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156.

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

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 & Computer Security, 26*(3), 277-289.

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

McHugh, M. (2013). The chi-square test of independence. *Biochemia Medica, 23*(2), 143-9.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences, 147*, 424-428.

Moran, E., & Volkwein, J. (1992). The Cultural Approach to the Formation of Organizational Climate. *Human Relations, 45*(1), 19-47.

Mowday, R., & Sutton, R. (1993). Organizational Behavior: Linking Individuals and Groups to Organizational Contexts. *Annual Review of Psychology, 44*(1), 195-229.

Nosworthy, J. (2000). Implementing Information Security In The 21st Century — Do You Have the Balancing Factors? *Computers & Security, 19*(4), 337-347.

O'Driscoll, M., & Evans, R. (1988). Organizational Factors and Perceptions of Climate in Three Psychiatric Units. *Human Relations, 41*(5), 371-388.

Öğütçü, M., Testik, Ö., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56,* 83-93.

O'Reilly, C., Chatman, J., & Caldwell, D. (1991). People and Organisational Culture: A profile comparison approach to assessing person-organization fit. *Academy of 233 Management Journal, 34*(3), 487-516.

Organisation for Economic Co-operation and Development [OECD]. (2004). *Principles of Corporate Governance.* Retrieved from oecd.org/corporate/ca/corporategovernanceprinciples/31557724.pdf

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

Ott, J. (1989). *The organizational culture perspective*. Chicago, Ill: Dorsey Press.

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

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165-176.

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M., & Jerram, C. (2015). The Influence of Organisational Information Security Culture on Cybersecurity Decision Making. *Journal of Cognitive Engineering and Decision Making: Special Issue on Cybersecurity Decision Making*, *9*(2), 117-129.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., Calic, D., & Jerram, C. (2015). Factors that Influence Information Security Behaviour: An Australian Web-based Study. In T.Tryfonas, & I. Askoxylakis. *Proceedings of Third International Conference on Human Aspects of Information Security, Privacy and Trust (HAISA 2015), HCI International 2015*, LNCS 9190 (pp. 231-241). Los Angeles, CA: USA.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security, 20*(1), 18-28.

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: A comparison of two studies. *Information and Computer Security,24*(2), 228-240.

Pfleeger, S., & Caputo, D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611.

Podsakoff, P., & Organ, D. (1986). Self-Reports in Organizational Research: Problems and Prospects. *Journal of Management, 12*(4), 531-544.

Pricewaterhouse Coopers. (2016). *Key findings from the global state of information security survey 2016. Turnaround and transformation in cyber security.* Retrieved from pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf

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

Quinn, R., & Rohrbaugh, J. (1983). A Spatial Model of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Analysis. *Management Science, 29*(3), 363-377.

Reid, R., & van Niekerk, J. (2014). Brain-compatible, web-based information security education: A statistical study. *Information Management & Computer Security, 22*(4), 371-381.

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

Rousseau, D. (1990). Normative Beliefs in Fund-Raising Organizations: Linking Culture to Organizational Performance and Individual Responses. *Group & Organization Management, 15*(4), 448-460.

Ruighaver, A., Maynard, S., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.

Ryder, P., & Southey, G. (1990). An exploratory study of the Jones and James organisational climate scales. *Asia Pacific Journal of Human Resources Management, 28*(3). 45-52.

Sackmann, S. (2011). *Culture and performance*. In N. Ashkanasy, C. Wilderom, & M. Peterson (Eds.), The handbook oforganizational culture and climate (2nd edn., pp. 188–224). Thousand Oaks, CA: Sage Publications.

Sanders, J. (2016). Defining terms: Data, information and knowledge. *SAI Computing Conference (SAI), 2016,* 223-228.

Sasse, A., Brostoff, AMR., & Weirich, D. (2001). Transforming the 'weakest link' - a human-computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122 - 131.

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

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

Schein, E. (1999). Empowerment, coercive persuasion and organizational learning: Do they connect? *The Learning Organization, 6*(4), 163-172.

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

Schein, E. (1986). What you need to know about organizational culture. *Training and Development Journal, 40*(1), 30-34.

Schein, E. (1990). Organizational culture. *American Psychologist, 45,* 109-19.

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

Schneider, B., Ehrhart, M., & Macey, W. (2011). Perspectives on organizational climate and culture. *APA handbook of industrial and organizational psychology, 1,* 373-414.

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. *Journal of Applied Psychology, 102*(3), 468-482.

Schneider, B., & Snyder, R. (1975). Some relationships between job satisfaction and organization climate. *Journal of Applied Psychology, 60*(3), 318-328.

Schulz, D. (2005). *Bureau of Industry and Security*. Encyclopedia of Law Enforcement, 566-568.

Schwartz, H., & Davis, S. (1981). Matching Corporate Culture and Business Strategy. *Organizational Dynamics, 10*, 30-48.

Sempane, M., Rieger, H., & Roodt, G. (2002). Job Satisfaction In Relation To Organisational Culture. *SA Journal of Industrial Psychology, 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* (pp. 373-382). ACM. Atlanta, Georgia: USA.

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. *AMCIS 2006 Proceedings*. 415. aisel.aisnet.org/amcis2006/415. Acapulco: México.

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

Siponen, M., & Vance, A. (2012). IS Security Policy Violations: A Rational Choice Perspective. *Journal of Organizational and End User Computing (JOEUC), 24*(1), 21-41.

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.

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.

Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Stewart, A. (2005). Information security technologies as a commodity input. *Information Management & Computer Security, 13*(1), 5-15.

Tabachnick, B., & Fidell, L. (2013) *Using Multivariate Statistics.* Boston: Pearson.

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.

Thomson, K., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security, 2006*(10), 7-11.

Tucker, R., Mccoy, W., & Evans, L. (1990). Can Questionnaires Objectively Assess Organisational Culture? *Journal of Managerial Psychology, 5*(4), 4-11.

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

Van Niekerk, J., & von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486.

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

Velki, T., Solic, K., & Ocevcic, H. (2014). Development of Users' Information Security Awareness Questionnaire (UISAQ); Ongoing work. *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on,*1417-1421. Opatija: Croatia.

Von Solms, B. (2000). Information security - the third wave. *Computers & Security, 19*(7), 615-620.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

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

Workman, M., Bommer, W., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

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. *Information Systems Research, 22*(2), 400-414,416-417.

Yilmaz, C., & Ergun, E. (2008). Organizational culture and firm effectiveness: An examination of relative effects of culture traits and the balanced culture hypothesis in an emerging economy. *Journal of World Business, 43*(3), 290-306.

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.

Appendices

Appendix A: Journal Guidelines for Submission

Computers & Security

ELSEVIER

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

EDITORIAL BOARD

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.

Appendix B: Questionnaire

Computers at Work

The purpose of this research is to investigate the knowledge, attitude and behaviour of individuals, whilst using a computer for work, and how factors, such as their organisation may affect their use.

Your participation is completely voluntary. This survey will take you approximately 20 to 30 minutes to complete and will time-out in 60 minutes.

This project is being conducted by researchers from the University of Adelaide and the Defence Science and Technology Group. The principal researcher is Agata McCormac.

To take part in this survey, you must be an adult living in Australia. You must be employed (full time, part time or casually) and must spend some work time using a computer or portable device. You must also confirm that you have read and understood the Information Sheet.

Please click on the following link to view the Participant Information Form.

I have read the Information Sheet titled “Computers at Work?” and I consent to take part in the current study.

○ Yes (1)
○ No (2)

If No Is Selected, Then Skip To End of Survey

Are you an adult (at least 18 years old) living in Australia?

○ Yes (1)
○ No (2)

If No Is Selected, Then Skip To End of Block

What is your age?

○ 19 and under (1)
○ 20 - 29 (2)
○ 30 - 39 (3)
○ 40 - 49 (4)
○ 50 - 59 (5)
○ 60 or over (6)

What is your gender?

○ Male (1)
○ Female (2)
○ Other (3)

What is your country of origin?
[open text answer]

What country did you undertake most of your studies?
[open text answer]

What language do you speak most at home?
[open text answer]

Do you have more than one job?
If you have multiple jobs, please answer the questions in this survey based on your primary place of work.

○ Yes (1)
○ No (2)

What is your employment status?

○ Not employed (1)
○ Part-time (2)
○ Contract / Casual (3)
○ Full-time (4)

If Not employed Is Selected, Then Skip To End of Block

What percentage of your time at work is spent using a computer or portable device (e.g. laptop, tablet, smartphone)?

○ No time at all (1)
○ 20% or less (2)
○ 21% - 40% (3)
○ 41% - 60% (4)
○ 61% - 80% (5)
○ 81% - 100% (6)

If No time at all Is Selected, Then Skip To End of Block

ISA & CULTURE

What is your job / occupation (i.e. your job title / job role)?
[open text answer]

What kind of business or industry do you work for?
○ Health and Community Services (1)
○ Retail and Wholesale (2)
○ Education (3)
○ Finance, Banking and Insurance (4)
○ Mining, Manufacturing and Construction (5)
○ Government and Defence (6)
○ Other, please specify (7) ____________________

Approximately how many people are employed by your place of work?
○ 1-4 (micro enterprises) (1)
○ 5-19 (small) (2)
○ 20-199 (medium) (3)
○ 200+ (large) (4)

What type of employer do you work for?
○ Public (1)
- a) Local
- b) State
- c) Federal

○ Private (2)
- a) International organisation
- b) Australian organisation
- c) Local company ?
  - i) Not-For-Profit
  - ii) For-Profit

What category would best describe your job level?
○ Management / Leadership Position (1)
○ Supervisor / Team Leader (2)
○ Team Member / Regular Staff Member (3)

Does your place of work have rules about computer use and information security?
○ Yes, there is a formal policy (1)
○ Yes, there is an informal policy or basic rules (2)
○ No (3)
○ Unsure (4)

Have you completed any subjects in the area of information security? (e.g , University / TAFE / Private college)?
○ Yes (1)
○ No (2)

How frequently does your place of work provide information security education, training or awareness programs?
○ Never (1)
○ Every two years (2)
○ Every year (3)
○ Every six months (4)
○ Every three months (5)
○ At least once a month (3)
○ Other (please specify) _____________

What types of information security education, training or awareness programs have you received at your place of work?
○ Instructor led lecture (1)
○ Instructor led workshop (2)
○ Emails (3)
○ Training videos (4)
○ Pop-up messages (5)
○ Newsletters or online bulletins (6)
○ E-learning (7)
○ Review a policy document (8)
○ Posters (9)
○ Discussions with colleagues (10)
○ Other (please specify) __________ (11)
○ None (12)

We care about the quality of our data. In order for us to get the most accurate measures of your opinions, it is important that you thoughtfully provide your best answers to each question in this survey.
Do you commit to thoughtfully provide your best answers to each question in this survey?
○ I will provide my best answers (1)
○ I will not provide my best answers (2)
○ I can't promise either way (3)

If I will not provide my best answers or I can't promise either way Is Selected, Then Skip To End of Block

ISA & CULTURE

Please confirm you are not a robot via Captcha.

[PAGE BREAK]

You will now be asked to complete three sets of questions about using a computer for work.

These sets of questions are about:

1. Your *knowledge* of computer use guidelines.
2. Your *attitude* towards these computer use guidelines.
3. Your *behaviour* when using a computer for work.

[PAGE BREAK]

Knowledge
The following statements are about your *knowledge* of how you should use a computer for work.

[PAGE BREAK]

Knowledge
The following statements are about your *knowledge* of how you should use a computer for work.

	SD (1)	D (2)	NAnD (3)	A (4)	SA (5)
I can't be fired for something I post on social media. (9)	○	○	○	○	○
I am allowed to enter information on any website if it helps me do my job. (10)	○	○	○	○	○
Sensitive print-outs can be disposed of in the same way as non-sensitive ones. (8)	○	○	○	○	○
I am permitted to open every email in my inbox. (6)	○	○	○	○	○
If I see someone acting suspiciously in my workplace, I should report it. (22)	○	○	○	○	○
A mixture of letters, numbers and symbols is necessary for work passwords. (2)	○	○	○	○	○
When working in a public place, I have to keep my laptop with me at all times. (25)	○	○	○	○	○
I am allowed to download any files onto my work computer if they help me to do my job. (23)	○	○	○	○	○
I must not ignore poor security behaviour by my colleagues. (26)	○	○	○	○	○
I can post what I want about work on social media. (30)	○	○	○	○	○
When working on a sensitive document, I must ensure that strangers can't see my laptop screen. (31)	○	○	○	○	○
If I find a USB stick in a public place, I shouldn't plug it into my work computer. (33)	○	○	○	○	○
It's acceptable to use my social media passwords on my work accounts. (34)	○	○	○	○	○
I am allowed to send sensitive work files via a public Wi-Fi network. (35)	○	○	○	○	○
It's optional to report security incidents. (37)	○	○	○	○	○
I am allowed to open email attachments from unknown senders. (41)	○	○	○	○	○
I must periodically review the privacy settings on my social media accounts. (45)	○	○	○	○	○
I am allowed to leave print-outs containing sensitive information on my desk overnight. (47)	○	○	○	○	○
I am allowed to share my work passwords with a colleague. (50)	○	○	○	○	○
I am not permitted to click on a link in an email from an unknown sender. (51)	○	○	○	○	○
While I'm at work, I shouldn't access certain websites. (53)	○	○	○	○	○

[PAGE BREAK]

Attitude
The following statements are about your *attitude*.
You've told us about your *knowledge* of computer use guidelines. Now please tell us what you *think* about these guidelines.

[PAGE BREAK]

Attitude

The following statements are about your *attitude*.

You've told us about your *knowledge* of computer use guidelines. Now please tell us what you *think* about these guidelines.

	SD (1)	D (2)	NAnD (3)	A (4)	SA (5)
It’s safe to use the same password for social media and work accounts. (11)	○	○	○	○	○
It’s a bad idea to share my work passwords, even if a colleague asks for it. (22)	○	○	○	○	○
It’s safe to have a work password with just letters. (19)	○	○	○	○	○
It’s always safe to click on links in emails from people I know. (7)	○	○	○	○	○
Nothing bad could happen if I click on a link in an email from an unknown sender. (16)	○	○	○	○	○
It’s risky to open an email attachment from an unknown sender. (23)	○	○	○	○	○
It can be risky to download files on my work computer. (21)	○	○	○	○	○
Just because I can access a website at work, doesn't mean that it’s safe. (5)	○	○	○	○	○
If it helps me to do my job, it doesn’t matter what information I put on a website. (18)	○	○	○	○	○
It’s necessary to regularly review my social media privacy settings. (6)	○	○	○	○	○
It doesn’t matter if I post things on social media that I wouldn't normally say in public. (20)	○	○	○	○	○
It's risky to post certain information about my work on social media. (29)	○	○	○	○	○
When working in a café, it’s safe to leave my laptop unattended for a minute. (30)	○	○	○	○	○
It’s risky to send sensitive work files using a public Wi-Fi network. (31)	○	○	○	○	○
It's risky to access sensitive work files on a laptop if strangers can see my screen. (32)	○	○	○	○	○
Disposing of sensitive print-outs by putting them in the rubbish bin is safe. (33)	○	○	○	○	○
If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer. (34)	○	○	○	○	○
It’s risky to leave print-outs that contain sensitive information on my desk overnight. (35)	○	○	○	○	○
If I ignore someone acting suspiciously in my workplace, nothing bad can happen. (36)	○	○	○	○	○
Nothing bad can happen if I ignore poor security behaviour by a colleague. (37)	○	○	○	○	○
It’s risky to ignore security incidents, even if I think they’re not significant. (38)	○	○	○	○	○

[PAGE BREAK]

Behaviour

The following statements are about your *behaviour*.

You've told us what you *know*, and what you *think* about computer use guidelines. Now please tell us what you *do* when using a computer for work.

[PAGE BREAK]

Behaviour

The following statements are about your *behaviour*.
You've told us what you *know*, and what you *think* about computer use guidelines. Now please tell us what you *do* when using a computer for work.

	SD (1)	D (2)	NAnD (3)	A (4)	SA (5)
I use a different password for my social media and work accounts. (13)	○	○	○	○	○
I share my work passwords with colleagues. (14)	○	○	○	○	○
I use a combination of letters, numbers and symbols in my work passwords. (4)	○	○	○	○	○
I do not always click on links in emails just because they come from someone I know. (15)	○	○	○	○	○
If an email from an unknown sender looks interesting, I click on a link within it. (16)	○	○	○	○	○
I do not open email attachments if the sender is unknown to me. (1)	○	○	○	○	○
I download any files onto my work computer that will help me get the job done. (17)	○	○	○	○	○
When accessing the Internet at work, I visit any website that I want to. (18)	○	○	○	○	○
I assess the safety of websites before entering information. (11)	○	○	○	○	○
I do not regularly review my social media privacy settings. (7)	○	○	○	○	○
I do not post anything on social media before considering any negative consequences. (9)	○	○	○	○	○
I post whatever I want about my work on social media. (22)	○	○	○	○	○
When working in a public place, I leave my laptop unattended. (23)	○	○	○	○	○
I send sensitive work files using a public Wi-Fi network. (24)	○	○	○	○	○
I check that strangers can't see my laptop screen if I'm working in a café. (25)	○	○	○	○	○
When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed. (26)	○	○	○	○	○
I wouldn't plug a USB stick found in a public place into my work computer. (27)	○	○	○	○	○
I leave print-outs that contain sensitive information on my desk when I'm not there. (28)	○	○	○	○	○
If I saw someone acting suspiciously in my workplace, I would do something about it. (29)	○	○	○	○	○
If I noticed my colleague ignoring security rules, I wouldn't take any action. (30)	○	○	○	○	○
If I noticed a security incident, I would report it. (31)	○	○	○	○	○

[PAGE BREAK]

Please read each statement carefully and decide if you ever feel this way about your job. If you have never had this feeling, cross the '0' (zero) in the space after the statement. If you have had this feeling, indicate how often you feel it by crossing the number (from 1 to 6) that best describes how frequently you feel that way.

	Never (0)	Almost Never (1)	Rarely (2)	Someti mes (3)	Often (4)	Very Often (5)	Always (6)
At my work, I feel bursting with energy	○	○	○	○	○	○	○
At my job, I feel strong and vigorous	○	○	○	○	○	○	○
I am enthusiastic about my job	○	○	○	○	○	○	○
My job inspires me	○	○	○	○	○	○	○
When I get up in the morning, I feel like going to work	○	○	○	○	○	○	○
I feel happy when I am working intensely	○	○	○	○	○	○	○
I am proud on the work that I do	○	○	○	○	○	○	○
I am immersed in my work	○	○	○	○	○	○	○
I get carried away when I'm working	○	○	○	○	○	○	○

ISA & CULTURE

How strongly do you agree or disagree with the following statements?

	SD (5)	D (4)	NAnD (3)	A (2)	SA (1)
Some of my colleagues will ignore information security policies to get the job done.	○	○	○	○	○
I would feel comfortable reporting a mistake I made at work that could have information security implications.	○	○	○	○	○
I believe that meeting deadlines is more important than complying with information security policies.	○	○	○	○	○
My colleagues generally behave in a secure manner when they are using a computer.	○	○	○	○	○
I would feel comfortable reporting a mistake someone else made at work that could have information security implications.	○	○	○	○	○
In my organisation, it is expected that I meet deadlines even if it means ignoring information security policies.	○	○	○	○	○

[PAGE BREAK]

How strongly do you agree or disagree with the following statements?

	SD (1)	D (2)	NAnD (3)	A (4)	SA (5)
Most employees are highly involved in their work	○	○	○	○	○
Decisions are usually made at the level where the best information is available	○	○	○	○	○
Information is widely shared so that everyone can get the information he or she needs when it's needed	○	○	○	○	○
Everyone believes that he or she can have a positive impact	○	○	○	○	○
Business planning is ongoing and involves everyone in the process to some degree	○	○	○	○	○
Cooperation across different parts of the organisation is actively encouraged	○	○	○	○	○
People work like they are part of a team	○	○	○	○	○
Teamwork is used to get work done, rather than hierarchy	○	○	○	○	○
Teams are our primary building blocks	○	○	○	○	○
Work is organised so that each person can see the relationship between his or her job and the goals of the organisation	○	○	○	○	○
Authority is delegated so that people can act on their own	○	○	○	○	○
The "bench strength" (capability of people) is constantly improving	○	○	○	○	○
There is continuous investment in the skills of employees	○	○	○	○	○
The capabilities of people are viewed as an important source of competitive advantage	○	○	○	○	○
Problems often arrive because we do not have the skills necessary to do the job (RS)	○	○	○	○	○

[PAGE BREAK]

ISA & CULTURE

How strongly do you agree or disagree with the following statements?

	SD (1)	D (2)	NAnD (3)	A (4)	SA (5)
The leaders and managers “practice what they preach”	○	○	○	○	○
There is a characteristic management style and a distinct set of management practices	○	○	○	○	○
There is a clear and consistent set of values that governs the way we do business	○	○	○	○	○
Ignoring core values will get you in trouble	○	○	○	○	○
There is an ethical code that guides our behaviour and tells us right from wrong	○	○	○	○	○
When disagreements occur, we work hard to achieve “win-win” solutions	○	○	○	○	○
There is a “strong” culture	○	○	○	○	○
It is easy to reach consensus, even on difficult issues	○	○	○	○	○
We often have trouble reaching agreement on key issues (RS)	○	○	○	○	○
There is a clear agreement about the right way and the wrong way to do things	○	○	○	○	○
Our approach to doing business is very consistent and predictable	○	○	○	○	○
People from different parts of the organisation share common perspective	○	○	○	○	○
It is easy to coordinate projects across different parts of the organisation	○	○	○	○	○
Working with someone from another part of this organisation is like working with someone from a different organisation (RS)	○	○	○	○	○
There is a good alignment of goals across levels	○	○	○	○	○

[PAGE BREAK]

How strongly do you agree or disagree with the following statements?

	SD (1)	D (2)	NAnD (3)	A (4)	SA (5)
The way things are done is very flexible and easy to change	○	○	○	○	○
We respond well to competitors and other changes in the business environment	○	○	○	○	○
New and improved ways to do work are continually adopted	○	○	○	○	○
Attempts to create change usually meet with resistance (RS)	○	○	○	○	○
Different parts of the organisation often cooperate to create change	○	○	○	○	○
Customer comments and recommendations often lead to changes	○	○	○	○	○
Customer input directly influences our decision	○	○	○	○	○
All members have a deep understanding of customers wants and needs	○	○	○	○	○
The interests of the customer often get ignored by our decisions (RS)	○	○	○	○	○
We encourage direct contact with customers by our people	○	○	○	○	○
We view failure as an opportunity for learning and improvement	○	○	○	○	○
Innovation and risk taking and encouraged and rewarded	○	○	○	○	○
Lots of things “fall between the cracks” (RS)	○	○	○	○	○
Learning is an important objective in our day-to-day work	○	○	○	○	○
We make certain that the “right hand knows what the left hand is doing”	○	○	○	○	○

[PAGE BREAK]

How strongly do you agree or disagree with the following statements?

	SD (1)	D (2)	NAnD (3)	A (4)	SA (5)
There is a long-term purpose and direction	○	○	○	○	○
Our strategy leads other organisations to change the way they compete in the industry	○	○	○	○	○
There is a clear mission that gives meaning and direction to our work	○	○	○	○	○
There is a clear strategy for the future	○	○	○	○	○
Our strategic direction is unclear to me (RS)	○	○	○	○	○
There is widespread agreement about goals	○	○	○	○	○
Leaders set goals that are ambitious, but realistic	○	○	○	○	○
The leadership has "gone on record" about the objectives we are trying to meet	○	○	○	○	○
We continuously track our progress against our stated goals	○	○	○	○	○
People understand when needs to be done for us to succeed in the long run	○	○	○	○	○
We have shared vision of what the organisation will be like in the future	○	○	○	○	○
Leaders have a long-term viewpoint	○	○	○	○	○
Short-term thinking often compromises our long-term vision (RS)	○	○	○	○	○
Our vision creates excitement and motivation for our employees	○	○	○	○	○
We are able to meet short-term demands without compromising our long-term vision	○	○	○	○	○

[PAGE BREAK]

We invite you to comment on this questionnaire
[open text answer]

While completing this survey were you only focussing on this task?

○ Yes (1)

a) Yes - Only focussing on this task

○ No (2)

a) No - Switching between tasks on this device (e.g. completing other surveys or checking social media)
b) No - Participating in tasks outside of this device (e.g. childminding or watching television)
c) No - Other

Did you respond randomly at any point during the study?

○ Yes (1)
○ No (2)

○ **Did you search the internet (via Google or otherwise) to assist with answering any questions?**

○ Yes (1)
○ No (2)

Thank you for taking the time to complete this survey.

It is greatly appreciated.

If you have any questions or feedback related to the study, please contact us via the details below:

Ms Agata McCormac
Phone: (08) 7389 5787
Email: Agata.McCormac@adelaide.edu.au

If you wish to speak with an independent person, please contact Paul Delfabbro, Chair of the Subcommittee for Human Research Ethics in the School of Psychology on (08) 8313 4936 or Paul.Delfabbro@adelaide.edu.au

Thank you again for taking the time to take part in this study!

Appendix C: Participant Information Sheet

PARTICIPANT INFORMATION SHEET

PROJECT TITLE: Computers at Work - Investigation of the Human Aspects of Cyber Security.
HUMAN RESEARCH ETHICS COMMITTEE APPROVAL NUMBER: H-18-38
PRINCIPAL INVESTIGATOR: Ms Agata McCormac

Dear Participant,

You are invited to participate in the research project described below.

What is the project about?
This research project is investigating people's knowledge, attitude and behaviour towards computer use at work. Through this research, we hope to better understand how individuals use computers, laptops, smartphones and tablets for work purposes and how this relates to their organisation.

Who is undertaking the project?
This project is being conducted by researchers from the University of Adelaide and the Defence Science and Technology Group. The principal researcher is Agata McCormac.

Why am I being invited to participate and what will I be asked to do?
This project is seeking participants who are adults living in Australia. Individuals must also be employed (full-time, part-time or casually) and must use a computer or portable device for some of their time spent at work. You will be asked to complete an online survey.

How much time will the project take?
The survey will take you approximately 30 minutes to complete.

Are there any risks associated with participating in this project?
There are no foreseeable risks. In the case of any unforeseen event or incident, which may have an effect on you as the participant, you can contact the researchers. Furthermore, you can discuss any issues with Paul Delfabbro, Chair of the Subcommittee for Human Research Ethics in the School of Psychology.

What are the benefits of the research project?
While there are no direct benefits to participants, this study will enable us to better understand employees' knowledge, attitude and behaviour towards using computers at work. This should help to inform organisations on appropriate policies and procedures.

Can I withdraw from the project?
Participation in this project is completely voluntary. If you agree to participate, you can withdraw from the study at any point before the submission of the survey. After this point, because your data is anonymous, we are unable to remove it.

What will happen to my information?
The information gathered in this survey will be stored electronically, retained for a minimum of five years. Identifiable data will only be accessible to the research team and non-identifiable data may be

shared with collaborative research partners. All data is non-identifiable, which means it is not possible for the researchers to identify a specific individual. The results will be published in conference proceedings and journals.

Who do I contact if I have questions about the project?
If you have questions or problems associated with the practical aspects of your participation in the project, or wish to raise a concern or complaint about the project, then please contact Ms Agata McCormac [redacted]

What if I have a complaint or any concerns?
The study has been approved by the Human Research Ethics Subcommittee of the University of Adelaide School of Psychology (approval number H18/38). If you wish to speak with an independent person regarding concerns or a complaint, the University's policy on research involving human participants, or your rights as a participant, please contact Professor Paul Delfabbro, Chair of the School of Psychology, Human Ethics Subcommittee on (08) 8313 4936 or paul.delfabbro@adelaide.edu.au

Any complaint or concern will be treated in confidence and fully investigated. You will be informed of the outcome.

If I want to participate, what do I do?
Please return to the online survey, and complete the question, *'I have read the Information Sheet titled "Computers at Work" and I consent to take part in the current study'*.

Yours sincerely,

Ms Agata McCormac