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

Exploring the role of work identity and work locus of control in information security awareness.

Dr Lee Hadlington*
Division of Psychology, De Montfort University, The Gateway, Leicester, LE1 9BH
Lhadlington@dmu.ac.uk
Telephone: 0116 207 8626

Dr Maša Popovac (University of Buckingham)
masa.popovac2@buckingham.ac.uk
Department of Psychology, University of Buckingham, Hunter Street, Buckingham, MK16 1EG

Prof. Helge Janicke (De Montfort University)
heljanic@dmu.ac.uk
School of Computer Science and Informatics, De Montfort University, The Gateway, Leicester, LE1 9BH

Dr Iryna Yevseyeva (De Montfort University)
iryna@dmu.ac.uk
School of Computer Science and Informatics, De Montfort University, The Gateway, Leicester, LE1 9BH

Dr Kevin Jones (Airbus UK)
kevin.jones@airbus.com
Head of Cyber Security Architecture, Innovation and Scouting, Airbus UK, Quadrant House, Celtic Springs Business Park, Duffryn, Newport NP10 8FZ

* Corresponding Author

Abstract

A growing body of research evidence has been focused on exploring aspects of individual differences in the context of human factors and adherence to organisational information security. The present study aimed to extend this research by exploring three individual variables related directly to the individual's perceived control within the workplace, their commitment to current work identity, and the extent to which they are reconsidering commitment to work. A total 1003 participants aged between 18-65 (Mean = 40.29; SD = 12.28), who were in full or part-time employment took part in the study. The results demonstrated that work locus of control acted as a significant predictor for total scores on a measure of information security awareness. Those individuals who demonstrated more externality had weaker engagement in accepted information security within the workplace. The findings from the current study are discussed in the context of potential links to counterproductive work behaviours, as well as presenting possible practical routes for intervention strategies to help mitigate poor engagement in information security awareness.

Keywords: Information Security Awareness, Work Locus of Control, Work Identity, Counterproductive Work Behaviours; Organisational Security

Acknowledgement: This work was funded by Airbus UK as part of the Human Factors in Cybersecurity Project

1. Introduction

Measures designed to mitigate the potential threat posed by accidental and malicious attempts to gain access to company data and systems have met with some limited success. For the most part, technology-related interventions have failed to prevent organisations from becoming victims of cyberattacks and loss of sensitive data (Colwill, 2009; Hadlington, 2018; Sasse & Flechais, 2005). Such failures are presented in the context of one key confound for the successful operation and implementation of such technologies, that being the human end user. Over the past decade there has been a growing focus on work that explores the role of the end user and the associated individual differences that may influence information security within the workplace (Calic, Pattinson, Parsons, Butavicius, & McCormac, 2016; Hadlington & Parsons, 2017; McCormac et al., 2017; Parsons et al., 2017). Whilst this work has demonstrated that Big-5 personality factors such as conscientiousness can serve to influence an employee's adherence to accepted information security protocol (McCormac et al., 2017), limited work has focused directly on personality factors linked into commitment to the workplace. Aspects such as how much perceived control the individual has over their work environment, or how strongly they identify within their workplace could also provide additional findings that could be used in education and training, designed to bolster and enhance workplace information security awareness.

1.1 Human Factors and Information Security

Latterly there has been an increasing focus in the role aspects of human factors play in the context of information security (Hadlington, 2017; 2018; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Parsons et al., 2017; McCormac et al., 2017). Indeed, the UK National Cybersecurity Strategy 2016-2021 (HM Government, 2016) stated that ‘Cyber security is not just about technology. Almost all successful cyber attacks have a contributing human factor’ (p. 38). The growing realisation that, for the most part, technology cannot be the only solution to issues related to organisational cybersecurity is matched by a further realisation that employee (the human factor), can present a paradoxical element in the fight to bolster such. On the one hand, employees can be a critical asset in the fight against cybersecurity breaches, and can act to deny malicious attempts to access sensitive company data. On the other hand, employees can be the ‘weakest link’ (Sasse, M., Brostoff, S., Weirich, 2001; Sasse & Flechais, 2005) in the cybersecurity system; they are not logical, prone to misunderstanding and confusion, act on impulse and want to get their jobs done (Hadlington, 2018). The research that explores how and why employees fail to adhere to the most basic principles related to information security in the context of their everyday work lives is of critical importance. Detailed information about the potential risk factors employees present in the context of information security can help researchers and security practitioners develop a comprehensive framework for such. In turn, such a framework could be used to provide a set of practical intervention techniques designed to enhance information security awareness in a targeted, rather than a ‘one-size fits all’ approach (Hadlington, 2017; Hadlington, 2018).

1.2 Defining and Measuring Information Security Awareness

According to Parsons et al. (2017), definitions associated with the concept of Information Security Awareness (ISA) have two essential components. The first of these elements relates to the level of understanding the individual has about the organisational information security policy. In this context, knowledge of information security policies and protocols may not be equitable to actually understanding them, as many employees often fail to fully comprehend what they need to do in order to be effective in the context of information security (Sasse & Flechais, 2005). The second component in defining ISA is the extent to which the individual commits to the core principles of information security within their organisation, and how much of their behaviour meets the requirements for 'best practice' in such a context (Parsons et al., 2017). This second aspect presents an interesting avenue to further explore individual differences in the context of ISA, particular in relation to the level of commitment an individual has to their current work place. This will be explored later in this section.

As a result of their continued exploration of how ISA is constructed, Parsons et al. (2015, 2017) developed a holistic measure that aimed to tap into the core elements proposed to be at the heart of ISA; these core components are knowledge (how much an individual knows about accepted rules and procedures), attitude (towards information security polices), and behaviour (what individuals do in the context of ISA). Previous attempts to measure aspects of ISA through the use of self-report questionnaires have either focused narrowly on limited aspects of ISA, or have explored responses to broad statements rather than speciic ISA behaviours (McCormac, Parsons, Zwaans, Butavicius, & Pattinson, 2016). Previous measures have also been criticised for lacking consistency in terms of their internal reliabiliity, as well as limited deployment in empricial research (McCormac et al., 2016). To counter this, Parsons et al. (2014) presented the development of the Human Aspects of Information Security Questionnaire (HAIS-Q). In brief, the HAIS-Q assesses ISA across 7 key focus areas, including password management, email use, Internet use, social media use, mobile device securement, information handling, and incident reporting. There are further sub-divisions within these focus areas; in turn this creates 21 key areas of interest for ISA, with each aspect being probed for knowledge, attitude and behaviour (Parsons et al., 2014, 2017).

The HAIS-Q has undergone an impressive amount of testing in a wide variety of organisational populations in Australia, and has proven validity and re-test reliability (Parsons et al, 2017). The scale has also been paired with a variety of psychological and demographic variables, including age, sex, and personality factors. For example McCormac et al. (2017) explored the role of risk taking, the Big-5, age, and gender on scores for the HAIS-Q. The results showed that older adults had higher scores on the measure of ISA, and this finding was linear in nature even once age-related differences in risk-taking had been controlled for. McCormac et al. (2017) also noted significant differences between sex and total scores on the HAIS-Q, with females scoring higher, therefore having better ISA in comparison to males. In the context of the Big-5 Personality traits, the research also noted that those individuals who scored more highly on the constructs conscientiousness, agreeableness, and openness to experience also had better overall ISA. Such findings map well onto previous research exploring the behavioural intention to use security software, which also demonstrated that conscientiousness and agreeableness to be key in determining the willingness to use such technology (Shropshire, Warkentin, Johnston, & Schmidt, 2006).

1.3 Work Locus of Control, Counterproductive Work Behaviours and ISA.

More recent research using the HAIS-Q has explored individual differences in factors that are outside Big-5 personality constructs. For example, research by Hadlington and Parsons (2017) presented an exploration of how two previously unexplored factors, that of Internet addiction and cyberloafing, served to influence ISA. Cyberloafing is defined as an individuals' propensity to engage in the use of work-based information technology for non-work purposes (Blanchard & Henle, 2008). In the research by Hadlington and Parsons (2017) major cyberloafing (e.g. visiting adult websites, updating personaly webpages) acted as significant negative predictor for scores on the HAIS-Q. Those individuals who engaged in more frequent major cyberloafing activities had poorer ISA. The authors concluded that there might be a link between these aspects of an individual's personality and the notion of risk compensation, where individuals who believe that they are more protected by organisational security take increasing risks to get online to access certain types of material or activity (Hadlington & Parsons, 2017). Another suggestion is that for these individuals, they fail to engage fully in ISA as they have little regard for the organisation they are working for and their job role within it.

One of the key aspects related to the definition of ISA noted earlier is that of the level at which an individual commits to the organisational policies related to such (Parsons et al., 2017). It would seem plausible to suggest that if the individual has poor engagement with their workplace and their organisation, or if they feel they have limited control over their work, they will be less likely to engage in effective information security. One construct that offers the potential to explore an aspect of work place engagement is that of work locus of control (WLCS; Spector, 1988). The

WLCS was designed to explore the extent to which an individual views the control they have over workplace roles and activities (Spector, 1988). Locus of control has been defined in terms of an individuals expectancy related to how rewards or aspects of life outcomes are controlled on the basis of the actions of the individual (internality) or as a result of forces outside the control of the individual (externality) (Spector, 1988). Spector (1982, 1988) noted that, in the context of the original LOC scale produced by Rotter (1966), internals tend to have greater job satisfaction, are less likely to report job stress, and perceive themselves as having more control in their workplace.

In the original research by Spector (1988) it was noted that WLCS was significantly negatively correlated with job satisfaction, job commitment, and organisational commitment. So those individuals who scored more 'externally', having the perception that they had little control over their work and associated outcomes, also scored lower on these key variables. Additional work has made a link between WLCS and the potential to engage in counterproductive work behaviours Counterproductive work behaviours refer to intentional behaviours conducted by employees that could harm both the organisation and members within that organisation (Carpenter & Berry, 2014; Sprung & Jex, 2012). Sprung and Jex (2012) suggested that individuals demonstrating more externality may feel that they are unable to change work based outcomes, and therefore engage in counterproductive work behaviours to regain a sense of self-control. Indeed, findings from their research indicated that those individuals who scored higher on externality were more likely to engage in counterproductive work behaviours. As information security is seen as a critical aspect of the workplace environment, it could be suggested that there is a connection here between engagement in ISA and WLCS. Based on the previous findings related to counterproductive work behaviours (Sprung & Jex, 2012), it could be that those individuals who have a more external WLCS also have a poorer engagement in ISA, again in an attempt to gain control over aspects of their workplace or as part an active attempt to harm their host organisation.

1.4 Exploring the Role of Work Identity in ISA.

The current study also includes the use of another measure that explores the role of an individual's work identity and its impact on ISA. Work identity is a different construct to that of organisational commitment, a concept that has been previously explored in relation to ISA (Reeves, Parsons, & Calic, 2017). Organisational commitment refers to the level of attachment an employee has with their workplace, with more committed employees exhibiting better ISA (Reeves et al., 2017). In contrast, work identity measures the strength of an individual's identification with their work, and not directly their workplace or organisation. This allows an exploration of commitment to work outside of the organisation, and presents a more holisitic measure of someones engagement with their job and workplace. (Adams et al., 2016).

Work is a critical aspect of adult identity, as well as providing an aspect of focus and self-expression (Adams et al., 2016; Gini, 1998). According to Adams et al. (2016) work is not only an important source of well-being, health and self-esteem, it can also provide a 'sense of existence'. In their model of work identity, Adams et al (2016) presented two individual factors that contributed to this concept, both of which appear to have important ramifications for exploring ISA. Work Identity Commitment

(WIC) is seen as the firmness with which the individual identifies with their work, as well as the level at which they are both committed to their work, plus experience a sense of belonging in the workplace (Adams et al., 2016). In contrast, Work Identity Reconsideration of Commitment (WIRC) is the extent to which the individual is re-evaluating their current work identity, and how open they currently are to other opportunities in the realm of work (Adams et al., 2016). Individuals who feel less committed or engaged in their current workplace could be less likely to play an active role in aspects of information security. It is proposed that there could be a potential link between both WIC and WIRC, where those individuals who are more secure and committed to their work identity are more likely to engage in efficient ISA, whereas those who are less committed and who are also reconsidering their current workplace identity may not see the value in engaging in ISA. This suggestion does have some precedence in previous literature that explored organisational commitment and ISA (Reeves et al., 2017). This research noted that individuals who had stronger organisational commitment have better ISA, but the study was limited to exploring information security in the context of mobile device securement. The present research aims to extend these findings to explore a wider range of information security areas featured in the HAIS-Q.

1.5 Aims and Objectives

In the context of the continued examination of human factors related to ISA, a great deal of emphasis has been placed on the role of individual differences in personality factors. However, limited research has explored personality factors in the context of work, such as the individual's perceived level of control they believe they have over their work place environment, or the closeness of fit between the current work and their own self-concept. Leading on from the previous research in this area, the current study had a number of aims. The first aim was to explore if an individual’s work locus of control could predict the level at which employees engage in effective ISA. The second aim was to explore if the construct of work identity could also serve to predict an individual’s adherence to ISA within the workplace. If a clearer picture of these additional individual differences in human factors can be achieved, it would again move our understanding of the contributing factors in ISA, as well as presenting a clearer route for establishing theoretically-based interventions that could be targeted towards those who perceive limited control over their work environment.

2. Method

2.1 Participants

In total 1003 participants aged between 18-65 (Mean = 40.29; SD = 12.28) took part in an online study between the 3rd March 2018 to the 8th March 2018 and were recruited via Qualtrics Participants Panels. The sample consisted 49% Male and 51% Female,76% of the sample was in full-time employment and 24% part-time.. Participants were required to meet the following inclusion criteria in order to take part in the study, as outlined in Parsons et al., (2017). Participants had to be currently employed within the UK, be at least 18 years of age, spend at least 20% of their standard working day using computer technology, and work for an organisation that had formal or informal rules governing information security.

2.2 Materials

2.2.1 Human Aspects of Information Security Questionnaire (HAIS-Q)

The HAIS-Q was employed as a measure of ISA. The scale comprises of 63 individual items which probe the seven core areas of security across knowledge, attitudes and behaviour (Parsons et al., 2014). All of the questions in this section were responded to on a five-point Likert-type scale, where 1 = Strongly Disagree and 5 = Strongly Agree. Parsons et al. (2014) reported Cronbach's alphas of 0.84, 0.84 and 0.92 for Knowledge, Attitude and Behaviour, respectively, with similar scores obtained in the present study ($\alpha_{\text{Knowledge}}$ = 0.88; α_{Attitude} = 0.93; $\alpha_{\text{Behaviour}}$ = 0.91).

2.2.2 Work Locus of Control (WLCS).

Devised by Spector (1988) the work locus of control scale (WLCS) was used to measure locus of control in the context of a work-based environment. This is a 16-item scale that asks participants to respond to a series of statements on a Likert Scale (1 = disagree very much – 6 agree very much). In line with the original scoring system presented by Spector (1988), 8 of the internally worded items were reversed scored. An individual with an internal WLCS will have a low score, and a high score indicates an external WLCS. In the original study by Spector (1988), internal reliability was found to range from 0.75 – 0.85. In the context of the present study, a Cronbach's Alpha of .835 was found.

2.2.3 Tilburg Work Identity Scale of Commitment and Reconsideration of Commitment (TWIS-CRC).

This scale was originally developed by Adams et al. (2016) to act as an assessment of work identity across three key components, these being personal, relational, and social. These aspects are seen as being critical in the construction of identity (Adams & Van de Vijver, 2015). The scale also includes a consideration for fluidity of an individual's identity in the context of work, such as the capacity to reconsider work identity (e.g. ‘I am looking for a different line of work’). The 12-item scale is therefore split into two sub-scales, these being the Work Identity Commitment (WIC; 9 items), and Work Identity Reconsideration of Commitment (WIRC; 3 items) (see Adams et al., 2016 for a full list of items and scale construction). Higher scores on the WIC indicate a higher degree of individual commitment to work, as well as their sense of belonging to the work place. In the context of WIRC, a higher score is indicative of a greater level of revaluation regarding their commitment to current work identity and the exploration of other work related opportunities. The original study by Adams et al. (2016) presented Cronbach’s Alpha of .89 for WIC and .93 for WIRC. In the context of the present study, the WIC obtained a α = .90 and the WIRC had a α = .85.

3. Results

Descriptive statistics for the key variables in the present study and Pearson’s correlations are shown in table 1, where n = 1003. There were significant negative correlations between ISA (total HAIS-Q scores), WLCS and WIRC. Both age and WIC presented significant positive correlations to ISA. These findings suggest that those individuals who are more external in terms of their work locus of control have poorer ISA. Similarly those individuals who are going through a period of reconsideration of their current work identity and how committed they are to their current job roles also demonstrated poorer ISA.

3.1 Work Locus of Control, work identity commitment, and Reconsideration of work commitment.

To further determine how work locus of control, work identity commitment and reconsideration of work commitment served to predict scores on the measure of ISA, a 2-stage hierarchical multiple regression was conducted. In the first stage age, gender, and knowledge of formal/informal rules governing the use of IT in the work place were entered in line with findings from previous research (Hadlington, 2017; Hadlington & Parsons, 2017; McCormac et al., 2017). In the second stage of the model, WLCS, WIC, and WIRC were entered simultaneously given the lack of existing research to indicate which of these factors are most likely to act as significant predictors for ISA scores. The Durbin-Watson statistic was 2.065, suggesting that independence of errors could be assumed. Values of tolerance and VIF also indicated that multicolinearity was not a concern.

The results of the regression are presented in table 2. In the first stage, with the key demographic and organisational variables as the key predictors, the model explained a total of 19% of the variance in total HAIS-Q scores. Age, sex and knowledge of rules related to formal or informal policies governing IT use in the workplace all acted as significant predictors for total scores on the HAIS-Q ($p < .0001$) In the second stage, where WLCS, WIC, and WIRC were added as predictors, an additional 17% of variance was accounted for. However, it is noted that both WIC and WIRC failed to act as significant predictors for total scores on the HAIS-Q ($p > 0.05$), with only WLCS presenting as a significant predictor in this stage ($p < .001$). Overall, the key demographic and organisational variables, alongside that of WLCS accounted for 35% of total variance in total HAIS-Q scores.

3.2 Gender, Knowledge of ISA rules and ISA

In line with previous research (Hadlington & Parsons, 2017; McCormac et al., 2017) further analysis was conducted to examine the differences between sex and knowledge of formal or informal rules governing ISA. A one-way between subjects ANOVA revealed a significant difference between males and females in regards to scores on the HAIS-Q (*F*(1, 1003) = 7.600, *p* = .006, η_p^2 = .008). Females were observed to score consistently higher than males in terms of ISA, although it is noted that the effect size is very small. A second one-way between subjects ANOVA demonstrated a significant difference between knowledge of rules governing ISA and total scores on the HAIS-Q (*F*(1, 1003) = 82.757, *p* =.000, η_p^2 = .077). Here, those individuals who had knowledge of formal rules governing ISA within their workplace scored significantly higher in terms of ISA versus those that had knowledge of informal rules. This finding is supportive of earlier work by Hadlington and Parsons (2017) who also found a similar difference.

4. Discussion

The present study aimed to further explore individual differences in human factors in the context of information security awareness. Three key personality constructs exploring work locus of control, work identity consideration and work identity reconsideration were examined, alongside a measure of information security awareness. The results from the present study highlight some interesting aspects of the relationship between these constructs, and shall be discussed in turn in relation to previous research.

4.1 Work Locus of Control and ISA

In the context of the three key variables that were the focus of the present study, only WLCS emerged as significant predictor for scores on the measure of ISA. The results demonstrated that those individuals who scored higher on the WLCS, therefore exhibiting a greater degree of externality, had lower scores on the HAIS-Q. To the authors' knowledge, this is the first time such a link between WLCS and adherence to ISA has been noted in the literature exploring aspects of human factors in the area. It is possible that those individuals who have an internal WLCS are more likely to believe that their actions in the context of information security are more likely to protect themselves and in turn the company. In contrast those who score higher on externality may assume that, irrespective of their own actions, the company could still be vulnerable to an attack. The potential reasons for the association between WLCS and HAIS-Q could also be linked directly to aspects of counterproductive work behaviours mentioned earlier on in the introduction to this study. Sprung and Jex (2012) previously noted that WLCS acted as moderator between work stressors and counterproductive work behaviours, with those individuals demonstrating greater externality having a higher propensity to engage in counterproductive work behaviours. Following on from this work, it could be that poorer employee engagement or blatant disregard for organisational ISA could be one aspect of counterproductive work behaviours. Penney and Spector (2002) suggested that counterproductive work behaviours are typified by intent to harm the organisation, and includes theft, sabotage, interpersonal aggression, work slowdowns, wasting time, and spreading rumours. A lack of clear engagement in ISA could potentially fit into this category of activities, and not adhering to accepted ISA protocols could be a clear attempt to harm the organisation. As those individuals who score more highly on aspects of externality perceive a minimal amount of control over their work place and work (Spector, 1988; Penney & Spector, 2002). Disengagement with ISA could also be seen as another attempt for these individuals to regain some semblance of control over their work environment.

One further link between WLCS and ISA could be related to a sense of devolved responsibility. As external individuals view themselves as having little perceived control over outcomes related to their work, they may also see little worth in following relevant rules related to information security. The line of thought here is that for externals, forces outside of their control govern aspects of their work life, therefore even if they do adhere to ISA, there is still a potential for the organisation to be a victim of an attack. However such a link needs further empirical research to establish how aspects such as WLCS, counterproductive work behaviours and ISA act in such a way that allows further theoretical models to be built. Exploring the role that WLCS has on ISA would appear to be a productive endeavour, as the process of offering individuals who perceive limited control over their work environment could be built into active interventions for increasing ISA engagement. How this could be achieved in a practical sense is something that warrants further exploration, and it may be that interventions stressing the importance of ISA could be targeted to groups based on their WLCS. The alternative processes, actively attempting to alter the locus of control of an individual would appear to be less productive, with research generally accepting that locus of control is a stable trait that changes very little over time (Legerski, Cornwall, & O'Neil, 2006).

4.2 Work Identity Commitment and Reconsideration of Commitment.

Although both of these aspects of commitment were significantly correlated with the total scores on the HAIS-Q, neither presented as significant predictors once entered into the regression. WIC, conceptualised as the level with which the individual identifies with their work, where a higher scores indicates a stronger work identity (Adams et al., 2016), was positively correlated with total scores on the HAIS-Q. This would suggest that those individuals who have a stronger and more developed sense of work identity also have a better adherence to ISA. This is a novel and interesting result showing that the extent to which an individual is committed to their work environment and experience a sense of belonging with the same can impact on ISA. Indeed, WIC was also strongly negatively correlated with WLCS, suggesting a potential connection between the two factors, with externality related to a poorer sense of belonging in the work place as well as a weaker work identity. The extent to which an individual is reconsidering their current work identity and exploring potential new opportunities (Adams et al., 2016) was significantly negatively correlated with total scores on the HAIS-Q. It appears that individuals who have a less secure work place identity and are exploring options outside of their current role have a negative engagement in ISA.

4.3 Organisational factors and demographics

Although the main focus of the present study was to examine how WLCS and WIC/WIRC contributed to ISA, some of the findings related to other variables included in the current study are also worthy of mention. For example, the current work provided further support for studies demonstrating that age is a key determiner for ISA, with older individuals scoring better on this measure (McCormac et al., 2017;

Parsons et al., 2017). Previous work exploring the role of sex have produced mixed results however, with McCormac et al. (2017) noting a small but significant difference between males and females according to ISA scores. Parsons et al. (2017) noted that sex differences according to ISA have provided inconsistent results, whilst Sheng, Holbrook, Kumaraguru, Cranor, and Downs (2010) showed that women were more susceptible to phishing attacks versus males. It would appear that sex differences in ISA and susceptibility to actual attacks are more complex than perhaps initially assumed, with the present study also demonstrating sex as being a significant predictor for score on the HAIS-Q. Females were again found to score significantly higher on the measure of ISA, again supporting the findings from McCormac et al. (2017).

As in previous research by Hadlington and Parsons (2017), employee knowledge of the rules governing IT use within their organisation also served to act as a significant predictor for scores on the HAIS-Q. Those individuals with clear knowledge of formal rules that governed their use of IT and information security within the workplace scored significantly higher on the HAIS-Q. It is unclear how such a variable shapes ISA adherence, but one prospective mechanism could be clarity of guidance about what is acceptable in the context of ISA (Hadlington & Parsons, 2017). It is also noted that this information relies heavily on the participant's detailed knowledge of the rules governing ISA in their organisation, and the potential for them to be misinterpreted as 'guidance' rather than formal rules to be followed. A follow up study should focus directly on establishing the connection between organisations that have formal rules governing ISA and the interpretations and knowledge of such in employees. This may provide an additional route to engage individuals in more effective ISA through additional training and awareness (Hadlington & Parsons, 2017).

4.4 Limitations

As in previous research exploring aspects of ISA, the study relies heavily on self-report data from employees (Hadlington & Parsons. 2017). There may be a potential for respondents to portray an ideal set of responses in the context of their ISA posture, these potentially being significantly different to their actual knowledge, attitudes, and behaviour. In the absence of more objective data, the use of self-report material in the context of ISA has been demonstrated to be an effective approach, with the above limitations accepted (Hadlington & Parsons, 2017). Spector (1994) also detailed the usefulness of self-reported questionnaires in the context of organisation behaviour research, particularly when exploring how people think and feel about their work.

Establishing a degree of causality between Work Locus of Control and scores on the measure of ISA also needs some further work. It may be that those individuals who exhibit higher levels of externality are prone to reject their responsibility for their actions within the workplace, perceiving a lack of any worth in doing such (e.g. the company will still get attacked irrespective of what I do). It could also be that those scoring higher on aspects of externality may also be engaging in counterproductive work behaviours, with disengagement in ISA being an attempt to take control of their workplace. Both of these potential reasons for the link between work locus of control and ISA warrant further exploration outside of the scope for the current study.

5. Conclusion

The present research examined how work locus of control, work identity commitment, and reconsideration of work commitment served to influence knowledge, attitudes, and behaviours for information security. The results highlight that work locus of control acted as a key predictor for information security practice that could hinder the cybersecurity posture of the host organisation. Those individuals who were categorised as being more external, having limited perceived control over their workplace environments, were more likely to have weaker information security awareness. The present research demonstrates that other factors outside of Big-5 personality traits can be effective in predicting employee adherence to ISA, and could provide another pathway for effective intervention strategies. These programmes could serve to enhance employees perception of control within the workplace, which in turn may serve to bolster their understanding of ISA as well as engaging them to take more control over such.

6. References

Adams, B. G., Bueza, C., Cazan, A. M., Sekaja, L., Stefenel, D., Gotea, M., and Meyers, M. C. (2016). Measurement invariance of the Tilburg Work Identity Scale for Commitment and Reconsideration of Commitment (TWIS-CRC) in Romania, England, the Netherlands and South Africa, *14*, 122–135.

Blanchard, A. L., and Henle, C. A. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior*, *24*(3), 1067–1084. https://doi.org/10.1016/j.chb.2007.03.008

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

Carpenter, N. C., and Berry, C. M. (2014). Are Counterproductive Work Behavior and Withdrawal Empirically Distinct? A Meta-Analytic Investigation. *Journal of Management*, *43*(3), 834–863. https://doi.org/10.1177/0149206314544743

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196. https://doi.org/10.1016/j.istr.2010.04.004

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hadlington, L. (2018). The “Human Factor” in Cybersecurity. In J. Mcalaney and L. A.

Frumkin (Eds.), *Psychological and Behavioral Examinations in Cyber Security* (pp. 46–63). Hershey. PA: IGI Global. https://doi.org/10.4018/978-1-5225-4053-3.ch003

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

HM Government. (2016). *National Cyber Security Strategy*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Legerski, E., Cornwall, M., and O'Neil, B. (2006). Changning Locus of Control: Steelworkers Adjusting to Forced Unemployment. *Social Forces*, *84*(3), 1521–1537. https://doi.org/10.3868/s050-004-015-0003-8

McCormac, A., Parsons, K., Zwaans, T., Butavicius, M., and Pattinson, M. (2016). Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire (HAIS-Q). In *Australian Conference on Information Systems* (pp. 1–10). Wollongong.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. https://doi.org/http://dx.doi.org/10.1016/j.chb.2016.11.065

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

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Penney, L. M., and Spector, P. E. (2002). Narcissism and Counterproductive Work Behavior: Do Bigger Egos Mean Bigger Problems? *International Journal of Selection and Assessment*, *10*(1&2), 126–134. https://doi.org/10.1111/1468-2389.00199

Reeves, A., Parsons, K., and Calic, D. (2017). Securing Mobile Devices : Evaluating the Relationship between Risk Perception , Organisational Commitment and Information Security Awareness, (Haisa), 145–155.

Sasse, M., Brostoff, S., Weirich, D. (2001). Transforming the weakest link a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122–131.

Sasse, M., and Flechais, I. (2005). Usable Security: Why Do We Need It? How Do We Get It? In L. F. Cranor and S. Garfinkel (Eds.), *Security and Usability* (pp. 13–30). Sebastopol, CA: O'Reilly Publishing. Retrieved from http://discovery.ucl.ac.uk/20345/

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. (2010). Who falls for phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10*, 373–382. https://doi.org/10.1145/1753326.1753383

Shropshire, J., Warkentin, M., Johnston, A. C., and Schmidt, M. B. (2006). Personality and IT security: An application of the five-factor model. *Americas Conference on Information Systems (AMCIS)*, 3443–3449.

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.

Spector, P. E. (1988). Development of the Work Locus of Control Scale. *Journal of Occupational Psychology*, *61*(4), 335–340. https://doi.org/10.1111/j.2044-8325.1988.tb00470.x

Sprung, J. M., and Jex, S. M. (2012). Work locus of control as a moderator of the relationship between work stressors and counterproductive work behavior. *International Journal of Stress Management*, *19*(4), 272–291. https://doi.org/10.1037/a0030320

Lee Hadlington is an Associate Professor in Cyberpsychology at De Montfort University, United Kingdom. His current research focus centres on exploring how human factors can serve to influence individual cybersecurity posture both in and outside the organisation context. He has worked alongside a variety of organisations, including law enforcement, military and business examining topics such as insider threat, automated cyber defence and the gamification of cybersecurity. He completed his PhD at the University of Wolverhampton in 2006 in an area related to applied cognitive psychology and human factors.

Maša Popovac is a lecturer in Psychology and Research Officer at the University of Buckingham. Her research focuses primarily on online risks behaviours, experiences and perceptions of young people, particularly in the context of cyberaggression and cyberbullying. Her work also examines parental and school mediation strategies relating to technology use, and she works with a number of schools and organisations to implement effective online safety interventions both in the UK and abroad.

Helge Janicke is the Technical Director of De Montfort University's Cyber Technology Institute. He is the Head of School of Computer Science and Informatics. Prof. Janicke was awarded his PhD in Computer Science in 2007 and worked on Cyber Security with organisations such as Airbus Group, QinetiQ, Ministry of Defence and General Dynamics UK amongst others. His interests are covering formal verification techniques and their application to Cyber Security, SCADA and Industrial Control System Security as well as aspects of Cyber Warfare. He established DMU's Airbus Group Centre of Excellence in SCADA Cyber Security and Forensics Research in 2013.

Iryna Yevseyeva is a Senior Lecturer in Computing Science and Cyber Security at the Faculty of Technology at De Montfort University, Leicester, UK (since Feb/2016) and is a member of DMU’s Cyber Technology Institute. Her research interests are in multicriteria decision analysis and optimisation and their application in various domains including security, manufacturing, health care and chemo-informatics. Previously to joining DMU, she was a leading Research Associate in Choice Architecture for Information Security (ChAISe) project at Newcastle University, UK, a part of first Research Institute on Science of Cyber Security (RISCS), where she was working on models of influencing security behaviours.

Dr Kevin Jones is Head of Cyber Security Architecture, Innovation and Scouting at Airbus, leading a global network of; teams, projects and collaborations including; research & innovation, state of the art solutions development, and technology scouting for cyber security across; IT, ICS and Product security domains. He holds a BSc in Computer Science and MSc in Distributed Systems Integration from De Montfort University, Leicester where he also obtained his PhD: A Trust Based Approach to Mobile Multi-Agent System Security in 2010. He is active in the cyber security research community, has published numerous papers and holds a number of patents within the domain. Kevin is a recognised expert in Critical National Infrastructure security, SCADA security, and the protection of critical systems. He currently acts as an executive consultant to Airbus on matters of cyber security

Table 1: Descriptive Statistics and Correlations

Measure	1	2	3	4	5	6	7	8
1. Age	-							
2. HAIS-Q Total	.344**	-						
3. HAIS-Q Knowledge	.294**	.933**	-					
4. HAIS-Q Attitude	.336**	..966**	.849***	-				
5. HAIS-Q Behaviour	.351**	.956**	.826**	.904**	-			
6. Extraversion	-123**	-.480**	-.418**	-.465**	-.486**	-		
7. Agreeableness								
8. Conscientiousness								
9. Neuroticism								
10. Openness								
11. $\text{RT}_{\text{Ethical}}$								
12. $\text{RT}_{\text{Financial}}$								
7. $\text{RT}_{\text{Health \& Safety}}$	.111**	.248**	.206**	.231**	.272**	-.452**	-	
8.$\text{RT}_{\text{Recreational}}$	-.263**	-.268**	-.244**	-.255**	-.267**	.379*	-.301**	-
9. $\text{RT}_{\text{Social}}$								
Mean	**40.29**	**248.31**	**79.70**	**84.87**	**83.73**	**47.87**	**34.94**	**9.64**

Table 2: Summary of Hierarchical Regression for Variables Predicting Total HAIS-Q scores (n = 1003)

Variable	β	*t*
Step 1	F ($_{3,\ 1002}$) = 75.946 R^2 = .186**	
Age	.328	11.09**
Sex (Female = 1)	.141	4.84**
ISA Rule Awareness (Formal = 1)	.209	7.13**
Step 2	ΔF($_{6,\ 1003}$)= 90.429, R^2 = 353**	
Age	.275	10.11**
Sex	.107	4.11**
ISA Rule Awareness	.162	6.14**
Work Locus of Control	-.396	-13.165**
WIC	.029	1.009
WIRC	-.016	-.556

**p < 0.001.