Exploring the Role of Moral Disengagement and Counterproductive Work Behaviours in Information Security Awareness.

Key Words: Information Security Awareness; Moral Disengagement; Counterproductive Work Behaviours; Organizational Security

Abstract

As security breaches in organisations are on the rise, developing an understanding of factors enabling and preventing such breaches is crucial. Even though previous studies have examined organisational aspects of information security, not much focus has been placed on human factors. In the present work we examined the tendency to morally disengage (MD), information security awareness (ISA), and counterproductive work behaviours (CWB), in a sample of 718 employees who used computers on daily basis, in order to establish predictors of CWB and the behavioural outcomes of ISA. The results showed that the propensity to morally disengage plays an important role in ISA, particularly the aspect of diffusion of responsibility. Secondly, ISA knowledge and ISA attitude, as expected, were part of a mediating mechanism underlying the relationship between MD and ISA behaviours, as well as between MD and CWB. This demonstrates that ISA and CWB constructs overlap to a certain degree, and thus affecting one should have effects also on the other. The results are discussed in the context of intervention-based approaches and the need to consider ways of targeting both ISA knowledge and attitudes where there is a tendency to morally disengage.

Introduction

The potential consequences of a breach in information security can have wide ranging impacts, including loss of company reputation, competitive edge, funds, future revenue, productivity, and, in extreme cases, bankruptcy (Safa & Maple, 2016; Sen & Borle, 2015; Schatz & Bashroush, 2016). In the U.S., 71% of breaches in information security were attributed in part to human error or accidental loss (Shred-it, 2018). In the UK, 43% of businesses had reported a breach in cybersecurity in a preceding 12-month period (Department for Digital, Culture, Media, 2018); 75% of these breaches were related to staff responding to fraudulent emails. Even though breaches from negligent behaviours of employees continue to occur, individual differences that serve to influence employee uptake of information security awareness are often overlooked by security professionals in favour of technology-related interventions (Hadlington, 2018). Considering the size of the problem this needs to change.

Over the past decade, there has been an exponential growth in research exploring the role of human factors as predictors for information security awareness (ISA) in the work place (e.g. Egelman & Peer, 2015; Hadlington, Popovac, Janicke, Yevseyeva, & Jones, 2018; McCormac et al., 2018; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014a). ISA has been previously defined as 'the extent to which an individual understands the importance and implications of information security polices, rules, and guidelines, and, the extent to which they behave in accordance with these (McCormac, Parsons, Zwaans, Butavicius, & Pattinson, 2016, p. 3). Predominately, research has focused on individual differences related to sex, age and personality traits, such as agreeableness and conscientiousness as related to ISA (Butavicius et al., 2017; McCormac et al., 2017). More recent research, however, has explored how information security awareness is linked to individual differences which have a specific

work-based focus, including work locus of control, work identity and engagement in cyberloafing activities (Hadlington & Parsons, 2017; Hadlington et al., 2018).

To expand this point, research has suggested that factors influencing the 'fit' of the individual within the organisation may also have a detrimental impact on adherence to ISA rules (Hadlington et al., 2018). Work on more general counterproductive work behaviours (CWB) suggests that individual differences within moral disengagement may be reliably associated with adherence to ISA (Fida et al., 2015; Hystad, Mearns, & Eid, 2014; Moore, Detert, Treviño, Baker, & Mayer, 2012) . Indeed, this willingness to morally disengage has been a central factor highlighted in the context of dysfunctional or ineffective organisational membership (Barsky, 2011). For instance, previous research has noted that moral disengagement (MD) is often viewed as a potential coping mechanism deployed by employees to deal with the pressures of security-based requirements in the work place (D'Arcy, Herath, & Shoss, 2014), as well as a mechanism between perceived organisational injustice and deviant work behaviours (Hystad et al., 2014). In sum, the propensity for moral disengagement has been shown to influence a wide range of unethical and counterproductive work based behaviours (Moore et al., 2012). Similarly, counterproductive work behaviours (CWB) have also been linked to a general disregard for organisational safety and policies (Spector & Fox, 2010; Spector et al., 2006). It would therefore be logical to assume that individuals who have a higher tendency to morally disengage, will also be more likely to engage in aspects of CWB, and less likely to adhere to core principles of ISA.

Information Security Awareness and CWB

CWBs have been defined as 'voluntary employee behaviours that are viewed by the organisation as contrary to its legitimate interests, violate significant organisational norms, and

threaten the well-being of the organisation or its members (Berry, Carpenter, & Barratt, 2012, p. 613). Robinson and Bennett (1995) suggested that workplace deviance encapsulated any behaviour that voluntarily violates organisational norms, in turn threatening the well-being of members of the organisation and/or the organisation itself. Fox, Spector, Goh, Bruursema and Kessler (2012) further suggested that counterproductive work behaviours (CWB) are volitional in nature, and are set aside from those actions that may be deemed as being accidental or directly mandated. Robinson (2008) pointed out that much of the work in this area had been centred on predicting why an individual is more likely to engage in CWB and how they could be prevented from doing so. Additionally, Kelloway, Francis, Prosser and Cameron (2010) suggested that CWB could be viewed as a type of protest behaviour. In this instance, individuals or groups of employees may actively engage in CWB in order to redress a perceived injustice or organisational dysfunction.

According to some researchers, information and communications technology (ICT) related behaviours are often overlooked as a form of CWB (Weatherbee, 2010). The perspective taken here is that low levels of ISA are a direct indicator of potential ICT misuse, with ISA typically being conceptualised as having a behavioural component (Parsons et al., 2017). ICT misuse, in turn, could serve to compromise information security within the organisation (Hadlington & Parsons, 2017). This suggestion has some basis in previous research demonstrating that cyberloafing (the use of work-based ICT for non-work purposes) was a significant predictor of poor ISA, with more frequent engagement in cyberloafing linked to reduced engagement in ISA (Hadlington & Parsons, 2017). Information security is generally governed by a set of formal rules created by the organisation the individual works for, and these are defined in terms of accepted practices and protocols (e.g., keeping passwords safe, reporting security incidents; Parsons et al., 2014). Carvalho Wilks (2011) suggested that deviancy and unethical motives

(which can have a reflection in moral disengagement) often predispose employees to violate accepted procedures or to use ICT inappropriately. Such non-commitment to organisational norms can be seen as an aspect of organisational citizenship as well as an issue with a strong moral dimension (Carvalho Wilks, 2011).

Moral Disengagement

Moral disengagement was originally described by Bandura (1986), who argued that the capacity to govern one's own actions is self-regulatory in nature, but can be selectively activated (Hystad et al., 2014). Moral disengagement has been defined as "an individual's propensity to evoke cognitions which restructure one's actions to appear less harmful, minimize one's understanding of responsibility for one's actions, or attenuate the perception of the distress one causes others" (Moore, 2008, p. 129). Moral disengagement consists of eight inter-related cognitive mechanisms, each of which allows the individual to set aside internal moral standards in order to behave in a morally questionable way (Bandura, 1990; Albert Bandura, 1999). These cognitive processes allow the individual to mitigate feelings of distress (Moore et al., 2012).

The first set of cognitive mechanisms restructures the unethical or amoral act in order to make it morally justifiable (Bandura, 1999; Moore, 2015). Moral justification reframes unethical acts as being for the greater good, an example of such being the justification of military atrocities as serving a worthy goal (Bandura, 1990). Euphemistic Labelling is the use of sanitised language that relabels harmful actions making them appear more benign, such as taking something without permission as 'borrowing'. Advantageous comparisons use a contrast between the behaviour that is currently being engaged in with and even a more reprehensible behaviour. This means that the former appears to be minimised in terms of its seriousness when

compared to the latter. One of the examples presented by Moore et al. (2015) included the contrast between damaging property and physical assault against an individual.

The next set of cognitive processes allows the individual to obscure their moral involvement through the mechanisms of displacement and diffusion (Bandura, 1990; Bandura, 1999). By using displacement of responsibility, the individual is able to attribute the responsibility of their actions to an authority figure, whether this be condoned or directed behaviour. Diffusion of Responsibility disperses the actions of the individual across multiple members of a group, and means that the action is no longer that of the individual, but instead multiple individuals are to blame. In the final set of cognitive mechanisms, the aim is to minimise the perceived stress being caused by an amoral act (Bandura, 1990; Bandura, 1999). By using distortion of consequences, the individual is able to minimise the seriousness of the effects for the action, such as suggesting that stealing from large organisations is a 'victimless crime' (Detert, Treviño, & Sweitzer, 2008). Dehumanisation reframes the victims of amoral actions as being undeserving of basic human consideration. This process is often enabled by identifying individuals as members of an outgroup who are unworthy of moral regard (Bandura, 1999). Finally, attribution of blame assigns the responsibility for the action to the victim themselves, with their own actions typically being viewed as the root cause for any negative repercussions (Bandura, 1990; Bandura, Barbaranelli, Caprara, & Pastorelli, 1996) .

According to Moore et al. (2012) the workplace presents ample opportunities for the individual to morally disengage. Previous work by Alnuaimi, Robert and Maruping (2010) demonstrated that moral disengagement was linked to social loafing, particularly when individuals were part of a larger team. Moore et al. (2012) and others (Hinrichs et al., 2012; Lindkvist & Llewellyn, 2003) further state that most modern organisations are based around a hierarchical structure,

meaning that the potential for an individual to displace their responsibility is great, either onto other employees or the leadership of that organisation (Hinrichs, Wang, Hinrichs, & Romero, 2012; Moore et al., 2012). Furthermore, work is usually undertaken across different teams within an organisation, meaning that diffusion of responsibility could also be an issue. Finally, organisational membership automatically gives a boundary for where the ingroup ends and where the outgroup begins. This in turn allows for moral justification as a mechanism to protect the organisation, alongside cognitive minimisation of the impact amoral actions have on those outside.

Work by Detert and colleagues (2008) linked the propensity to morally disengage to behaviours such as cheating, lying, and stealing. In addition, D'Arcy and colleagues (2014) explored how moral disengagement could be used as a coping mechanism for stress created by complex and ambiguous information security requirements. The authors noted that moral disengagement was a good predictor for intentional violations of ISA. However, it needs highlighting that the research presented by D'Arcy et al. (2014) only focused on a narrow set of violations related to ISA, and did not explore other antecedents to disengaging in ISA, such as knowledge of ISA practices and attitudes towards the same. Further research by Chen, Chau, and Li (2019) explored the influence of MD on individual information security behaviours. The authors found that MD has a significant positive correlation with employee intention to violate organisational information security policies. Based on what limited research exists in this area, it is suggested that moral disengagement, particularly those related to diffusion of responsibility (see similar argument here: Hinrichs et al., 2012), could predict employees' engagement with ISA.

Aims and Objectives

The first aim of the current study is to explore the relationships between moral disengagement, CWB and ISA. Based on previous research, it is hypothesised that individuals who morally disengage less have higher levels of ISA and lower levels of CWB. The second aim is to examine whether cognitive-affective aspects of ISA (i.e., ISA knowledge and attitude) can provide the mechanisms explaining the relationship between MD and ISA behaviours, as well as MD and CWB. Even though previous research demonstrated that MD predicts higher levels of CWB (e.g., Moore et al., 2012), the mechanisms behind that relationship are not clear. Similarly, the research demonstrating the link between MD and ISA is highly limited, at least in the Western sphere (see Chen, Chau, & Li, 2019, for recent findings in a Chinese context), and lacks a systematic investigation of the potential mechanisms linking the two.

Here, we propose that the relationship between MD and CWB, as well as MD and ISA behaviours, is mediated by ISA attitude and knowledge. This hypothesis builds on previous research that demonstrated that the propensity for an individual to morally disengage was directly linked with engaging in counterproductive work behaviours, which can, theoretically, include withdrawal from engaging in ISA in the workplace (Cohen et al., 2013; Fida et al., 2015; Moore et al., 2012). To elaborate, people's attitudes and knowledge are well known to affect their behaviour (e.g. Ajzen, 1991; Siponen, 2000), but they themselves can be affected by individual characteristics such as MD. MD can function, as mentioned before, as a means of coping with security-related organisational pressures, but in a negative way, such that individuals do not internalise security-related requirements. We therefore propose that individuals with high levels of MD will therefore build up and command less ISA knowledge and will develop negative attitudes towards ISA-related matters. Lower levels of knowledge and more negative attitudes should in turn lead to higher levels of CWB, and engagement in behaviours that are not conducive to effective ISA within the organisation.

By gaining a more systematic understanding of the potentially causal relationships that exist between MD, ISA behaviours and CWB, it is hoped that more effective strategies for interventions can be designed and delivered.

Method

Participants

In total 718 participants aged between 18 and 64 years (M = 38.87; SD = 12.45) were recruited to take part in the current study through Qualtrics Participants Panels, and completed an online questionnaire. Participants were paid a small honorarium for taking part in the study (£4.50). The sample consisted of 49% male participants (51% were female), with 97% stating that they were working full-time, and 3% part-time. Participants were required to meet a series of inclusion criteria, as laid out by Parsons et al. (2017), to complete the measure of information security awareness. These included being currently in full or part-time employment, be at least 18 years of age, spend at least 20% (above one-and three-quarter hours) of one's working day using computer-based technology, and work for an organisation that had formal or informal rules governing IT use and information security. Response bias in participant responses was checked prior to analysis, and any individual who responded with the same answer (e.g., Strongly Agree) for over 90% of the items were removed prior to analysis. In this instance no data was removed at this stage.

Materials

The following self-report measures were used in the current study.

The Human Aspects of Information Security Awareness Scale (HAIS-Q)

The HAIS-Q (Parsons et al., 2014) was employed as a measure of ISA. This scale has undergone extensive testing in a number of studies (Hadlington & Parsons, 2017; Mccormac, Parsons, Zwaans, Butavicius, & Pattinson, 2016; Parsons et al., 2014b). The scale comprises of 63 items which probe seven core areas of security across knowledge, attitudes and behaviour (Parsons et al., 2014). These core focus areas include password management, email use, Internet use, social networking site use, incident reporting, mobile computing and information handling. Total scores for each of the key areas of knowledge, attitude, and behaviour can be calculated, as well as total scores for each of the focus areas detailed above. An overall score which represents a global measure of information security awareness can also be presented, with a higher score being indicative of a better engagement with ISA. All of the questions in this questionnaire were responded to on a five-point Likert-type scale (from 1 = Strongly Disagree to 5 = Strongly Agree). Cronbach's alphas of between .84 and .86 have been reported for the Knowledge subscale, .84 and .92 for Attitude, and .90 and .92 for the Behaviour subscale (McCormac et al., 2016; McCormac et al., 2017; Parsons et al., 2017, 2014). For the present study, scores fell within the ranges reported by previous research ($\alpha_{\text{Knowledge}} = 0.91$; $\alpha_{\text{Attitude}} = 0.94$; $\alpha_{\text{Behaviour}} = 0.93$), showing high reliability of the scale. Possible scores for the sub-scales range from 21-105, with possible total scores for the HAIS-Q ranging from 63-315.

Propensity to Morally Disengage Scale (MDS)

The 24-item propensity to morally disengage scale was developed by Moore et al. (2012). The scale asks participants to rate on a 7-point Likert scale (from 1 = Strongly Disagree to 7 = Strongly Agree) how likely they would engage in a number of morally questionable behaviours. The items are grouped around the eight cognitive mechanisms originally proposed by Bandura (1987), these being:

- Moral justification (e.g., “it is okay to spread rumours to defend those you care about”).
- Euphemistic labelling (e.g., “taking something without the owner’s permission is okay as long as you’re just borrowing it”).
- Advantageous comparison (e.g., “considering the ways people grossly misrepresent themselves, it is hardly a sin to inflate your own credentials a bit”).
- Displacement of responsibility (e.g., “people shouldn’t be held accountable for doing questionable things when they were just doing what an authority figure told them to do”).
- Diffusion of responsibility (e.g., “people can’t be blamed for doing things that are technically wrong when all their friends are doing it too”).
- Distortion of consequences (e.g., “taking personal credit for ideas that were not your own is no big deal”).
- Dehumanisation (e.g., “some people have to be treated roughly because they lack feelings that can be hurt”).
- Attribution of blame (e.g., “people who get mistreated have usually done something to bring it on themselves”).

The total 24-item scale had good internal reliability (α = .92. In contrast to the initial findings by Moore et al. (2012) it was noted in the current study that each of the subscales had alpha coefficients greater than .70 (Moral justification α = .85; Euphemistic Labelling α = .83; Advantageous Comparison α = .82; Displacement of Responsibility α = .87; Diffusion of Responsibility α = .88; Distortion of Consequences α = .85; Dehumanisation α = .80; Attribution of Blame α = .78), reflecting good reliability of the subscales. Possible scores for each of the sub-scales range from 3-21, with a higher score indicative of a greater propensity to morally disengage. Possible total scores for the Propensity to Morally Disengage scale range from 24-168.

Counterproductive work behaviour checklist (CWB-C)

Counterproductive work behaviours were assessed with the 32-item Counterproductive Work Behaviours Checklist (CWB-C, Spector et al., 2006). The scale asks participants to rate on a 5-point scale (1 = Never to 5 = Everyday) how often they have engaged in a number of counterproductive work behaviours (e.g., 'Purposely wasted your employer's materials/supplies', 'Purposely did you work incorrectly'). In the currently study the scale had high internal reliability (α = .99), and is in line with previous research (Cohen et al., 2013). Although the alpha level of .99 is particularly high, it is consistent with other research that has used the CWB-C (further details related to the psychometric information of the scale can be found on Paul Spector's website: http://shell.cas.usf.edu/~pspector/scales/cwbcover.html). Cohen et al (2013) also noted, as the measure acts as a behavioural checklist, measures of internal consistency do not act as a good indicator of reliability. Possible scores for the CWB-C range from 32-160.

Results

In this section, first descriptive statistics and bivariate correlations are presented. Subsequently, we report on the hierarchical regression and two multiple mediation models, testing the hypotheses of the current study. All of the analyses were performed in SPSS software (Version 25).

Descriptive statistics for the key variables of interest in the present study alongside Pearson's correlations are shown in Table 1, where n = 718. There were moderate significant negative correlations noted between total scores on the HAIS-Q and CWB (r = -.70, p < .01). Total HAIS-Q scores were also significantly negatively correlated with the each of the sub-scales

from the moral disengagement scale, with moderate negative correlations for Moral Justification (r = -.50, p < .01), Advantageous Comparison (r = -.61, p < .01), Displacement of responsibility (r = -.59, p < .01), Diffusion of Responsibility (r = -.65, p < .01), Distortion of Consequences (r = -.54, p < .01), and Attribution of Blame (r = -.54, p < .01). The propensity to morally disengage seems to have a significant relationship with ISA, where moral disengagement negatively impacts on ISA.

TABLE 1 ABOUT HERE

Moral Disengagement and ISA

To further explore the relationship between moral disengagement and ISA a hierarchical multiple regression was conducted focusing on ISA as the outcome variable. In the first stage, age and gender were included as per findings from previous research (Hadlington, 2017; Hadlington & Parsons, 2017; McCormac et al., 2017). Given the lack of direct research evidence to support the influence of moral disengagement on ISA, these sub-scales were entered simultaneously in the second stage. The Durbin-Watson statistic was 1.95, suggesting that independence of errors could be assumed. Values of tolerance and VIF also indicated that multicollinearity was not a concern (VIF average = 3.05; Tolerance Average = .46; Hair, Black, Babin, Anderson, & Tatham, 2006).

The results of the regression are presented in Table 2. In the first stage, with age and sex entered, the model explained a total of 19% of the variance observed in ISA scores, and is comparable to previous findings in other research (Hadlington et al., 2018). In the second stage, with Moral Disengagement added, a further 32% of the variance in total scores on the HAISQ were explained. In the final stage, age, sex, Euphemistic Labelling, Diffusion of Responsibility,

Advantageous Comparison, and Attribution of Blame remained significant predictors for ISA, with Diffusion of Responsibility largest amount of variance in ISA. In total the variables entered served to explain total of 50% variance observed in the total scores on the HAIS-Q.

TABLE 2 ABOUT HERE

Mediation Analysis: Moral Disengagement, ISA and CWB

To examine the potential mediating role of ISA knowledge and attitude, for the postulated causal relationships between (i) moral disengagement and CWB, and (ii) moral disengagement and ISA behaviour, two multiple mediation analyses were performed using PROCESS (Hayes, 2019) with 5000 Bootstrapping samples. As suggested in the introduction, because we expected similar effects of the attitude and knowledge dimensions of ISA, these were entered simultaneously as mediators. The results of these analyses are presented in Figures 1 and 2 below.

ISA attitude and ISA knowledge mediate the link between Moral disengagement and CWB

Unstandardized parameter estimates for the model are shown in Figure 1, with all associated SE estimates following in parentheses. Regressing ISA knowledge on moral disengagement showed that moral disengagement significantly decreased ISA knowledge [a_1 = -.28 (.014); p < .001; 95% CI: -.31, -.26]. Regressing ISA attitude on moral disengagement showed that moral disengagement also significantly decreased ISA attitude [a_2 = -.29 (.015); p < .001; 95% CI: -.32, -.26]. Finally, regressing CWB on ISA knowledge, IS attitude, and moral disengagement showed that both mediators significantly affected the outcome, and that a significant direct effect of MDS on CWB remained after the mediators were modelled [b_1 = -.44 (.13); p < .001;

95% CI: -.70, -.18; b_2 = -.55 (.12); p < .001; 95% CI: -.78, -.31]. Mediation analysis showed that both ISA knowledge (a_1b_1) and IS attitude (a_2b_2) significantly mediated the effects of the moral disengagement on CWB (see 1Figure 1) [a_1b_1 = .13 (.04); 95% CI: .05, .21; a_2b_2= .16 (.04); 95% CI: .08, .24]. Overall, R^2 = 46.09% of the variance in CWB was explained by variables in the model. Proportion-mediated effect size estimates for the individual mediation pathways indicated that ISA knowledge (PM = 19%) conveyed a slightly smaller portion of the impact of moral disengagement on CWB, compared with ISA attitude (PM = 23%). Given the significant direct effect of the moral disengagement on CWB, as well as the magnitude of the observed variance explained by the model, it is likely that there are additional mediators that could contribute to understanding the effect of the MDS on CWB.

FIGURE 1 ABOUT HERE

ISA attitude and ISA knowledge mediate the link between Moral disengagement and ISA behaviours

Unstandardized parameter estimates for the model are shown in Figure 2, with all associated SE estimates following in parentheses. Regressing ISA knowledge on moral disengagement showed that moral disengagement significantly decreased IS knowledge [a_1 = -.28 (.014); p < .001; 95% CI: -.31, -.26]. Regressing ISA attitude on moral disengagement showed that moral disengagement also significantly decreased IS attitude [a_2 = -.29 (.015); p < .001; 95% CI: -.32, -.26]. Finally, regressing ISA behaviours on ISA knowledge, ISA attitude, and moral disengagement showed that both mediators significantly affected the outcome, and that a significant direct effect of MDS on ISA behaviours remained after the mediators were modelled [b_1 = .19 (.04); p < .001; 95% CI: .12, .27; b_2 = .66 (.03); p < .001; 95% CI: .59, .72].

Mediation analysis showed that both IS knowledge (a_1b_1) and ISA attitude (a_2b_2) significantly mediated the effects of the moral disengagement on ISA behaviours (see Figure 2) [a_1b_1 = -.05 (.01); 95% CI: -.08, -.03; a_2b_2= -.19 (.02); 95% CI: -.22, -.16]. Overall, R^2 = 35.27% of the variance in CWB was explained by variables in the model. Proportion-mediated effect size estimates for the individual mediation pathways indicated that ISA knowledge (PM = 20%) conveyed much smaller portion of the impact of moral disengagement on ISA behaviours, compared with ISA attitude (PM = 76%). Given the significant direct effect of the moral disengagement on CWB, as well as the magnitude of the observed variance explained by the model, it is likely that there are additional mediators that could contribute to understanding the effect of the MDS on CWB.

FIGURE 2 ABOUT HERE

Discussion

The aim of the current research was to examine how individual differences in moral disengagement (MD) and counterproductive work behaviour (CWB) were linked to information security awareness (ISA). While previous studies have highlighted general associations among MD and CWB in the context of organisational IT security protocols (Chen et al., 2019; D'Arcy et al., 2014), more detailed and robust models that would allow for the development of effective training and further intervention have been missing. Based on the plethora of work tasks that are related to the use of information technologies, it was theorised that ISA would explain, at least in part, the link between MD and CWB. A model was proposed in which two dimensions of ISA, knowledge and attitudes, mediated effects of MD on CWB. In addition, similar processes were postulated to underlie the link between MD and the

behavioural component of ISA, i.e., the extent to which people make use of online security measures and comply with security protocols. A second mediation model was therefore put to test, in which ISA knowledge and attitudes mediated effects of MD on ISA behaviours. In the following section, key findings of the present study are discussed first. Further suggestions for additional research and potential practical applications for the current research are offered second.

Associations among MD, ISA and CWB

Overall the results identify several interesting trends between the propensity to morally disengage and information security awareness. All of the sub-scales from the moral disengagement scale were significantly negatively correlated with total scores on the HAIS-Q, six of which were moderate ($.5 < |r| < .7$). Among the strongest correlations between ISA and MD, when all subscales are inspected, were those involving diffusion of responsibility. In the context of information security, this may indicate a main barrier towards active compliance with protocols. In any larger organisation, the individual may find it very easy to sidestep their own personal role in ISA, perhaps relying on others to take up the burden. Previous research noted that many employees often fail to see their role in effective organisational cybersecurity, instead believing that this is something management should be responsible for (Hadlington, 2017).

Associations between ISA and CWB can be characterised as similar to those between ISA and MD. CWB was correlated negatively with all ISA variables, with coefficients in between -.7 and -.65. It is worth noting that ISA knowledge and attitudes were just as strongly related to CWB as the behavioural dimension. This may reflect, firstly, a certain conceptual overlap between CWB and ISA behaviours. The CWB measure used here captures a wide range of

general counterproductive behaviours, and it is likely that study participants interpreted this to encompass IT-related tasks. As we have argued before, IT-based activities take up a substantial portion of all workplace activities for many professions, and it is unsurprising that CWB and negative ISA behaviours should go hand in hand. A second, related point to make is that ISA knowledge and attitudes therefore have the potential, as postulated in our multiple mediation models, to affect both CWB and ISA behaviours. Further, CWB was positively related to all eight subscales of MD, providing the exact mirror image to the association between ISA and MD. This further corroborates earlier evidence linking MD to unethical behaviours, and general disregard of safety policy frameworks (Cohen et al., 2013; Spector & Fox, 2010).

Regression results confirm the picture provided by the inspection of bivariate associations. Taken together, the other study variables explained 50% of the variance in HAIS-Q scores. The most prominent psychometric predictor was diffusion of responsibility. Four out of the eight components of MD (moral justification, displacement of responsibility, distortion of consequences, and dehumanization) were not significant when age and gender were taken into account. These findings should be considered in future conceptual refinement and validation of the HAIS-Q. The role of age and gender supports previous findings (Hadlington, 2017). Older IT users and male IT users tended to show higher levels of ISA. Experience and exposure to IT technology is likely to play a part in both cases, although gender effects are notoriously difficult to interpret and are likely to extend to other factors such as self-confidence, differences in job roles, self-reporting accuracy and so forth.

Multiple mediation of MD effects on CWB

The results from multivariate causal modelling were in line with our theoretical model. As expected, knowledge and attitudes regarding information security, mediated the relationship

between moral disengagement and behavioural outcomes. Importantly, the behavioural outcomes assessed in the present work were two-fold. The first mediating process, leading to information security behaviours seems immediately plausible. Increases in moral disengagement, according to the model, lead to decreases in knowledge levels, presumably because individuals see less need to follow and comply with organizational communications, and by the same token it also leads to less positive attitudes towards information security protocols and policies. Both attitudes and knowledge are direct and necessary precursors to behaviours that affect information security for the individual user and the organization at large. The second mediating process in the model, however, extends the mediating role of attitudes and knowledge specific to ISA to the more general domain of CWB. This may indicate that CWB and the behavioural component of ISA show overlap at the level of theory or operationalisation, but both constructs have been defined within different theoretical frameworks and the measures used in the present study differ substantially regarding the specificity of behaviours. Another interpretation would be that knowledge and attitudes surrounding ISA tap into a more general pathway leading from MD to CWB and represent motivational drivers of wider importance for compliance behaviours.

Directions for Future Work

The present work is not without shortcomings, and some are noted here to inform future work. To strengthen causal conclusions, it would be desirable to run longitudinal designs and to model associations over time. Since our findings rest on cross-sectional data, they cannot provide immediate insights into the process from one time point to another, and correlational evidence needs to be used for approximation. We would expect mediation effects to hold over time, though, not least for the theoretical reasons that led to our model specification. It is also worth noting that mere context effects, i.e., responses provided earlier in the study for one

measure affecting responses provided later for subsequent measures, cannot explain the mediation effects found since all measures were counter-balanced in the design.

Our findings rely on a convenience sample of organizational members. While sample diversity may have helped in getting a wide range of variable responses, future work should consider sampling within specific organizations. This could help in building interventions suited for a particular organizational context, but it could also serve to find out more about how much of a role the organizational context plays for the multiple mediation model. Multi-level modelling would help in separating out organization-level and individual-level effects.

Lastly, and unsurprisingly, we concede that our model rests entirely on self-report measures. While self-reports are highly suited for capturing variables related to personality and attitudes, adding alternative indicators of organizational behaviours, in the form of other-reports or observational data, would be desirable. The potential for common method bias to be present in the current data is an accepted consequence of using self-report measures. However, in line with the suggestions made by Conway and Lance (2010), proactive steps were taken in the design of the study in an attempt to minimize this. For example, the order of the items presented to participants was randomised to ensure that order effects did not take place. In the context of the constructs under investigation, self-report measures are seen as the most appropriate mechanism to collect data (Spector, 1994). Questions related to moral disengagement, counterproductive work behaviours, and adherence to information security protocols are all potentially sensitive topics. Lastly, as some employees may be reticent to discuss these items, the anonymity provided by the self-report measures goes some way to ensure participants are revealing their true feelings and intentions.

Implications for Intervention

In terms of practical implications, recommendations for organisations and employers can be derived from our findings. Although the present work cannot provide definitive causal evidence, the suggestion that ISA knowledge and attitudes are part of a causal process opens up the possibility of effective interventions in the workplace. While organizational members may be unwilling to disclose actual levels of moral disengagement, let alone take part in related intervention programmes, knowledge and attitudes are comparatively easy to target. Our mediation perspective emphasises that moral disengagement does not automatically translate into problematic behaviour and that ISA knowledge and attitudes can cushion negative effects. The HAIS-Q is proposed here as an instrument that allows for an IT risk assessment posed by organizational members and, in addition, provides indirect insight into counterproductive behaviours more generally. The instrument can be used to determine training needs and to evaluate training effectiveness, expanding on and going beyond existing intervention programmes (McCormac et al., 2016; Parsons et al., 2014; Pattinson et al., 2018).

However, such interventions are only useful in the context where failings in ISA are the result of naïve and accidental behaviours (Calic, Pattinson, Parsons, Butavicius, & McCormac, 2016; Dupuis & Khadeer, 2016). The work here focuses on behaviours where individuals have a conscious intent to engage (or disengage) in activities that fundamentally undermine the security stance of the organisation. There is still the issue of how to effectively engage individuals in safe ISA practices, particularly when they may be fundamentally opposed to such. In previous work, both work identity and work locus of control have been shown to have an direct influence on ISA (Hadlington et al., 2018). Therefore, one potential pathway to an intervention could be to instil a greater sense of organisational culture or a greater perception of autonomy over decision being made within the workplace (Hadlington et al., 2018).

However, the practical framework for accomplishing this requires further research, potentially longitudinal in nature. Some recent pilot research fits well with this suggested approach, highlighting the use of game-based methods to increase cyber-literacy of employees and impact their perceptions of responsibility (Filipczuk, Mason, & Snow, 2019).

At the same time, the mediation models provide a more informed position for those cases where interventions are unsuccessful. As discussed previously, moral disengagement can be an indicator of perceived injustice and grievance within organisations (e.g., Hystad, Mearns, & Eid, 2014). To the extent that MD does affect ISA, a change in ISA is most likely to occur during training if the underlying factors that drive MD are not too deeply embedded in the organisational context. Challenges in increasing ISA can therefore be used fruitfully in a diagnostic process that goes further back to the determinants of MD.

In summary, the present study showed that the propensity to morally disengage plays an important role in ISA, in particular the aspect of diffusion of responsibility. A second key finding was that both ISA knowledge and ISA attitude were part of a mediating mechanism underlying the relationship between MD and ISA behaviours, as well as MD and CWB. This demonstrates that ISA and CWB constructs overlap to a certain degree, and thus affecting one should have effects also on the other.

References

Ajzen, I. (1991). The theory of planned behavior. *Orgnizational Behavior and Human Decision Processes*, *50*, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Alnuaimi, O. A., Robert, L. P., & Maruping, L. M. (2010). Team Size, Dispersion, and Social Loafing in Technology-Supported Teams: A Perspective on the Theory of Moral

Disengagement. *Journal of Management Information Systems*, *27*(1), 203–230. https://doi.org/10.2753/mis0742-1222270109

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory.* New Jersey, US: Prentice-Hall, Inc.

Bandura, A., Barbaranelli, C., Caprara, G., & Pastorelli, C. (1996). Mechanisms of Moral Disengagement in the Exercise of Moral Agency. *Journal of Personality and Social Psychology*, *71*(2), 364–374. https://doi.org/10.1037/0022-3514.71.2.364

Bandura, A. (1990). Selective Activation and Disengagement of Moral Control. *Journal of Social Issues*, *46*(1), 27–46. https://doi.org/10.1111/j.1540-4560.1990.tb00270.x

Bandura, Albert. (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review*, *3*(3), 193–209.

Barsky, A. (2011). Investigating the Effects of Moral Disengagement and Participation on Unethical Work Behavior. *Journal of Business Ethics*, *104*(1), 59–75. https://doi.org/10.1007/s10551-011-0889-7

Berry, C. M., Carpenter, N. C., & Barratt, C. L. (2012). Do other-reports of counterproductive work behavior provide an incremental contribution over self-reports? A meta-analytic comparison. *Journal of Applied Psychology*, *97*(3), 613–636. https://doi.org/10.1037/a0026739

Butavicius, M., Parsons, K., Pattinson, M., Mccormac, A., Calic, D., & Lillie, M. (2017). *Understanding Susceptibility to Phishing Emails : Assessing the Impact of Individual Differences and Culture*. *2016*(Haisa).

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

Carvalho Wilks, D. (2011). Attitudes towards unethical behaviours in organizational settings: an empirical study. *Ethics in Progress Quarterly*, *2*(2), 9–22. https://doi.org/10.1002/jmv.24507

Chen, H., Chau, P., & Li, W. (2019). The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior. *Information Technology and People*, *32*(4), 973–992. https://doi.org/10.1108/ITP-12-2017-0421

Cohen, T. R., Panter, A. T., & Turan, N. (2013). Predicting Counterproductive Work Behavior from Guilt Proneness. *Journal of Business Ethics114*, *114*(1), 45–53. https://doi.org/10.1007/s10551-012-1326-2.Published

Conway, J. M., & Lance, C. E. (2010). What reviewers should expect from authors regarding common method bias in organizational research. *Journal of Business and Psychology*, *25*(3), 325–334. https://doi.org/10.1007/s10869-010-9181-6

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

Daniel Schatz, & Rabih Bashroush. (2016). The impact of repeated data breach events on organisations' market value. *Information and Computer Security*, *24*(1), 73–92. https://doi.org/10.1108/ICS-03-2014-0020

Department for Digital, Culture, Media, and S. (2018). Cyber Security Breaches Survey 2018. In *Cyber Security Breaches Survey 2018*. https://doi.org/10.13140/RG.2.1.4332.6324

Detert, J. R., Treviño, L. K., & Sweitzer, V. L. (2008). Moral Disengagement in Ethical Decision Making: A Study of Antecedents and Outcomes. *Journal of Applied Psychology*, *93*(2), 374–391. https://doi.org/10.1037/0021-9010.93.2.374

Dupuis, M., & Khadeer, S. (2016). Curiosity Killed the Organization: A Psychological Comparison between Malicious and Non-Malicious Insiders and the Insider Threat. *RIIT 2016 - Proceedings of the 5th Annual Conference on Research in Information Technology*, 35–40. https://doi.org/10.1145/2978178.2978185

Egelman, S., & Peer, E. (2015). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*, *1*, 2873–2882. https://doi.org/10.1145/2702123.2702249

Fida, R., Paciello, M., Tramontano, C., Fontaine, R. G., Barbaranelli, C., & Farnese, M. L. (2015). An integrative approach to understanding counterproductive work behavior: The roles of stressors, negative emotions, and moral disengagement. *Journal of Business Ethics*, *130*(1), 131–144. https://doi.org/10.1007/s10551-014-2209-5

Filipczuk, D., Mason, C., & Snow, S. (2019). Using a game to explore notions of responsibility for cyber security in organisations. *Conference on Human Factors in Computing Systems - Proceedings*, 1–6. https://doi.org/10.1145/3290607.3312846

Fox, S., Spector, P. E., Goh, A., Bruursema, K., & Kessler, S. R. (2012). The deviant citizen: Measuring potential positive relations between counterproductive work behaviour and organizational citizenship behaviour. *Journal of Occupational and Organizational Psychology*, *85*(1), 199–220. https://doi.org/10.1111/j.2044-8325.2011.02032.x

Hadlington, L. (2018). The "Human Factor" in Cybersecurity. In J. Mcalaney & L. A. Frumkin (Eds.), *Psychological and Behavioral Examinations in Cyber Security* (pp. 46–63). https://doi.org/10.4018/978-1-5225-4053-3.ch003

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

Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I., & Jones, K. (2018). Exploring the

role of work identity and work locus of control in information security awareness. *Computers & Security*, *81*, 41–48. https://doi.org/10.1016/j.cose.2018.10.006

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis.* (6th ed.). Uppersaddle River: Pearson Prentice Hall.

Hinrichs, K. T., Wang, L., Hinrichs, A. T., & Romero, E. J. (2012). Moral disengagement through displacement of responsibility: The role of leadership beliefs. *Journal of Applied Social Psychology*, *42*(1), 62–80. https://doi.org/10.1111/j.1559-1816.2011.00869.x

Hystad, S. W., Mearns, K. J., & Eid, J. (2014). Moral disengagement as a mechanism between perceptions of organisational injustice and deviant work behaviours. *Safety Science*, *68*, 138–145. https://doi.org/10.1016/j.ssci.2014.03.012

Kelloway, E. K., Francis, L., Prosser, M., & Cameron, J. E. (2010). Counterproductive work behavior as protest. *Human Resource Management Review*, *20*(1), 18–25. https://doi.org/10.1016/j.hrmr.2009.03.014

Lindkvist, L., & Llewellyn, S. (2003). Accountability, responsibility and organization. *Scandinavian Journal of Management*, *19*(2), 251–273. https://doi.org/10.1016/S0956-5221(02)00027-1

McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lillie, M. (2018). The Effect of resilience and job stress on information security awareness. *Information and Computer Security*, *26*(3), 277–289.

Mccormac, A., 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). *Australasian Conference on Information Systems*, 1–10.

McCormac, A., 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). *Australian Conference on Information Systems*, 1–10. Wollongong.

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

Moore, C., Detert, J., Trevino, L., Baker, V., & Mayer, D. (2012). Why Employees Do Bad Things : Moral Disengagement and Unethical. *Personnel Psychology*, *65*, 1–48.

Moore, Celia. (2008). Moral disengagement in processes of organizational corruption. *Journal of Business Ethics*, *80*(1), 129–139. https://doi.org/10.1007/s10551-007-9447-8

Moore, Celia. (2015). Moral disengagement. *Current Opinion in Psychology*, Vol. 6, pp. 199–204. https://doi.org/10.1016/j.copsyc.2015.07.018

Moore, Celia, Detert, J. R., Treviño, L. K., Baker, V. L., & Mayer, D. M. (2012). Why Employees Do Bad Things : Moral Disengagement and Unethical. *Personnel Psychology*, *65*, 1–48.

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. https://doi.org/10.1016/j.cose.2017.01.004

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 and Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Pattinson, M., Butavicius, M., Ciccarello, B., Lillie, M., Parsons, K., Calic, D., & McCormac, A. (2018). Adapting Cyber Security Training to Your Employees. *In Proceedings of the Twelfth International Symposium on Human Aspects of Information Security &*

Assurance (HAISA 2018).

Robinson, S. L., & Bennett, R. J. (1995). A Typology of Deviant Workplace Behaviors: A Multidimensional Scaling Study. *Academy of Management Journal*, *38*(2), 555–572. https://doi.org/10.5465/256693

Safa, N. S., & Maple, C. (2016). Human errors in the information security realm – and how to fix them. *Computer Fraud and Security*, *2016*(9), 17–20. https://doi.org/10.1016/S1361-3723(16)30073-2

Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, *32*(2), 314–341. https://doi.org/10.1080/07421222.2015.1063315

Shred-it. (2018). *The State of the Industry*. https://doi.org/10.1080/10920277.2000.10595929

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

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., & Fox, S. (2010). Counterproductive work behavior and organisational citizenship behavior: Are they opposite forms of active behavior? *Applied Psychology*, *59*(1), 21–39. https://doi.org/10.1111/j.1464-0597.2009.00414.x

Spector, P. E., Fox, S., Penney, L. M., Bruursema, K., Goh, A., & Kessler, S. (2006). The dimensionality of counterproductivity: Are all counterproductive behaviors created equal? *Journal of Vocational Behavior*, *68*(3), 446–460. https://doi.org/10.1016/j.jvb.2005.10.005

Weatherbee, T. G. (2010). Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. *Human Resource Management*

Review, *20*(1), 35–44. https://doi.org/10.1016/j.hrmr.2009.03.012

Table 1: Correlations and Descriptive Statistics for Key Variables.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Age	_													
HAISQ Total	.38**	_												
HAISQ Knowledge	.35**	.96**	_											
HAISQ Attitude	.36**	.98**	.92**	_										
HAISQ Behaviour	.39**	.96**	.87**	.91**	_									
CWB	-.32**	-.70**	-.69**	-.69**	-.66**	_								
Moral Justification	-.23**	-.50**	-.50**	-.47**	-.49**	.57**	_							
Euphemistic Labelling	-.17**	-.46**	-.45**	-.43**	-.45**	.57**	.78**	_						
Advantageous Comparison	-.25**	-.61**	-.60**	-.58**	-.59**	.66**	.75**	.78**	_					
Displacement Responsibility	-.26**	-.59**	-.58**	-.56**	-.56**	.61**	.65**	.69**	.80**	_				
Diffusion Responsibility	-.26**	-.65**	-.64**	-.63**	-.62**	.67**	.75**	.73**	.83**	.82**	_			
Distortion Consequences	-.22**	-.54**	-.54**	-.52**	-.52**	.59**	.72**	.74**	.81**	.76**	.84**	_		
Dehumanization	-.19**	-.46**	-.46**	-.44**	-.44**	.51**	.65**	.65**	.72**	.64**	.71**	.75**	_	
Attribution of Blame	-.18**	-.54**	-.54**	-.52**	-.51**	.58**	.64**	.69**	.76**	.78**	.78**	.79**	.75**	_
Score Range (Min-Max)	18-64	169-315	48-105	48-105	50-105	32-160	3-21	3-21	3-21	3-21	3-21	3-21	3-21	3-21
Mean	38.86	241.99	79.67	82.06	80.25	59.18	10.04	10.07	9.17	9.37	9.2	9.84	10.41	9.85
SD	12.46	46.51	15.67	16.77	15.68	34.06	4.91	4.70	4.70	4.91	5.03	4.80	4.82	4.60

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 2: Hierarchical Regression Analysis

	Model 1				Model 2			
	B	**SE B**	**β**	**t**	**B**	**SE B**	**β**	**t**
(Constant)	164.73	6.20		26.55**	250.21	6.72		37.26**
Gender (Female=0)	21.11	3.33	.227	6.33**	10.38	2.70	.11	3.84**
Age	1.71	.13	.46	12.79**	.95	.11	.25	8.50**
Moral Justification					-.66	.44	-.07	-1.50
Euphemistic Labelling					1.50	.49	.15	3.08**
Advantageous Comparison					-2.15	.59	-.22	-3.65**
Displacement of Responsibility					-.89	.48	-.09	-1.86
Diffusion of Responsibility					-3.75	.56	-.41	-6.63**
Distortion of Consequences					.71	.56	.07	1.27
Dehumanization					.73	.43	.08	1.70
Attribution of Blame					-1.12	.50	-.11	-2.22*
R^2	.19				.51			
Adj R^2	.19				.50			
F	83.82**				72.30**			

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

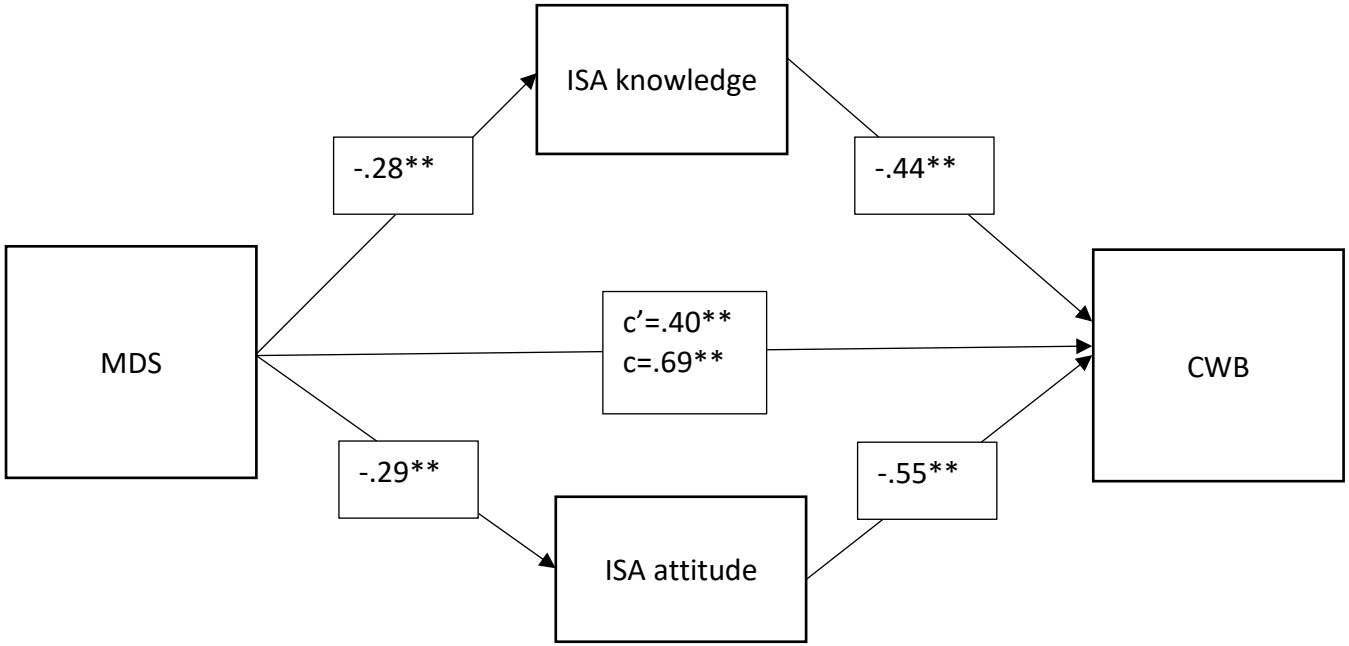

Figure 1 Parallel multiple mediator model, estimating mechanism between MDS and CWB.

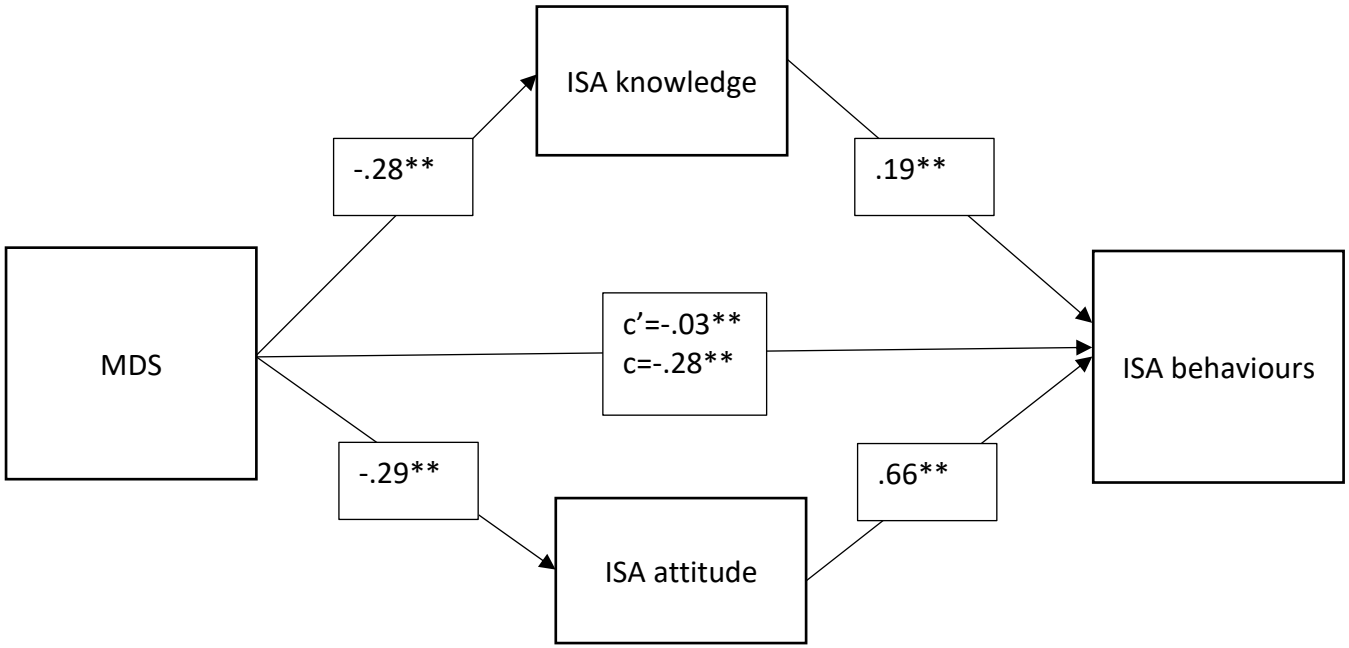

Figure 2 Parallel multiple mediator model, estimating mechanism between MDS and ISA behaviours.