Behaviour & Information Technology

ISSN: 0144-929X (Print) 1362-3001 (Online) Journal homepage: http://tandfonline.com/loi/tbit20

How senior management and workplace norms influence information security attitudes and self-efficacy

Suresh Cuganesan, Cara Steele & Alison Hart

BEHAVIOUR & INFORMATION TECHNOLOGY, 2017
https://doi.org/10.1080/0144929X.2017.1397193

How senior management and workplace norms influence information security attitudes and self-efficacy

Suresh Cuganesan[a], Cara Steele[b] and Alison Hart[c]

[a]The University of Sydney Business School, University of Sydney, Sydney, Australia; [b]Australian Catholic University, Melbourne, Australia; [c]The University of Sydney, Sydney, Australia

ABSTRACT

Prior information security research establishes the need to investigate the informal factors that influence employee attitudes and self-efficacy beliefs about information security. Two informal workplace dynamics that are particularly important for how employees think about information security comprise senior management support and workplace norms. However, there are limitations to empirical research to date on these constructs, including conflicting evidence on the relationship between senior management support and information security attitudes and a lack of research on how norms impact self-efficacy beliefs. Also, although some studies suggest that norms might play a mediating role between information security attitudes, self-efficacy beliefs and their (informal and formal) antecedents, empirical research is yet to investigate these possibilities. Consequently, this study considers the relationships between senior management support, norms, formal controls and information security attitudes and self-efficacy beliefs. It comprises a cross-sectional survey of employees at a law enforcement organisation. Results indicate the central role that norms have on employee information security attitudes and self-efficacy beliefs including their direct and mediating role. In addition, the study highlights the important role that senior management support has on employees' thinking about information security.

ARTICLE HISTORY
Received 7 February 2016
Accepted 20 October 2017

KEYWORDS
Information security; workplace norms; senior management; employee attitudes; control mechanisms

1. Introduction

The amount and flow of data and information across commercial and government entities continue to increase rapidly. This flow is often necessary to facilitate digital interactions and greater collaboration across entities. Correspondingly, however, there is a growing information security risk. Continued evidence of employee-linked information security breaches (PWC 2014) makes it critical to understand the behavioural aspects of information security within organisations (Chen, Ramamurthy, and Wen 2013; Dhillon, Syed, and Pedron 2016; Soomro, Shah, and Ahmed 2016). Consequently, information systems (IS) research has shifted its attention from purely technological solutions (such as firewalls and encryption solutions) to consider how the behaviour of the people within the firm might be changed in ways productive for information security (Workman, Bommer, and Straub 2009; Abawajy 2014; Metalidou et al. 2014; Alhogail, Mirza, and Bakry 2015; Alavi et al. 2016). *Inter alia*, this research highlights the importance of shifting employee information security attitudes and beliefs in their self-efficacy.

IS research to date has emphasised formal programmes of awareness raising, behaviour monitoring and sanctions for security breaches, as ways of shifting information security attitudes, self-efficacy beliefs and ultimately behaviours (Hedström et al. 2011; Chen, Ramamurthy, and Wen 2013). In contrast, 'very few studies have focused on the informal aspects of a workplace and how elements within this workspace impact employee beliefs, attitudes, and perceptions related to compliance activities' (Warkentin, Johnston, and Shropshire 2011, p.276; see also Guo et al. 2011). IS researchers are thus urged to delve further into the informal factors that influence employee attitudes and self-efficacy beliefs about information security (Hedström et al. 2011; Chen, Ramamurthy, and Wen 2013; Alhogail, Mirza, and Bakry 2015).

Two informal workplace dynamics that are particularly important for how employees think about information security comprise senior management support and workplace norms.[1] Senior management support signals the importance of information security to the rest of the organisation and can empower employees to change how they approach information security (Kayworth and Whitten 2010; Flores and Ekstedt 2016). Similarly, users' information security attitudes and self-efficacy beliefs are likely to be influenced by the norms that characterise

CONTACT Suresh Cuganesan suresh.cuganesan@sydney.edu.au

their environment, such as the expectations and behaviours of their colleagues (Guo et al. 2011; Warkentin, Johnston, and Shropshire 2011; Da Veiga and Martins 2015). Indeed, the role of leadership and senior management support, as well as workplace norms, is enshrined in popular information security models, such as, for example, the ISACA (2009) Business Model for Information Security.

Despite their importance, empirical research on the actual effects of these factors on information security attitudes and self-efficacy beliefs is insufficient in three main ways. First, only a few studies examine the effect of senior management support on information security attitudes, and these report conflicting findings (e.g. Puhakainen and Siponen 2010; Hu et al. 2012; Flores and Ekstedt 2016). There is also only limited empirical evidence of the effect of senior management support on norms and self-efficacy beliefs. Second, reflecting a growing awareness of the importance of workplace norms, a small group of studies finds that norms influence information security attitudes (e.g. Guo et al. 2011; Ifinedo 2014). However, we know little about the effect of norms on self-efficacy. Indeed, to our knowledge, the effects of norms on information security self-efficacy beliefs are yet to be empirically tested. Finally, studies have suggested that characteristics of work environments such as shared norms and values could mediate the effect of senior management support on information security attitudes and beliefs (e.g. Hu et al. 2012; Flores and Ekstedt 2016). It is also plausible that norms play a mediating role in the relationships between formal information security controls, and attitudes and self-efficacy. However, empirical research is yet to investigate these possibilities and, as such, our knowledge of the role that norms play in information security contexts may be underdeveloped.

Hence, we investigate the relationships between senior management support, norms, formal controls and information security attitudes and self-efficacy beliefs. Developing a more comprehensive understanding of the antecedents to information security attitudes, norms and self-efficacy, as well as the direct and mediating effects of norms, is important given that research establishes the importance of these three constructs on actual information security behaviours (e.g. Bulgurcu, Cavusoglu, and Benbasat 2010; Safa et al. 2015; McGill and Thompson 2017).

Data on information security attitudes, norms and self-efficacy and their antecedents are collected through a cross-sectional survey of employees at a law enforcement organisation – a context where information security concerns are paramount and which is usually difficult to access and study. The next section reviews relevant prior literature and develops the hypotheses to be tested.

2. Background literature and hypothesis

In developing the hypotheses to be tested, we draw on prior literature that includes studies employing the theory of planned behaviour (TPB), which posits that intention to carry out a particular behaviour, and in turn the actual behaviour, can be predicted by attitudes, subjective norms and self-efficacy beliefs (Ajzen 1991). Non-TPB studies are also drawn upon to the extent that they shed light on the factors that influence the information security attitudes, norms and self-efficacy. In each of the sub-sections below, we develop the hypothesis that we test in the empirical part of the study.

2.1 The influence of senior management

It is well established in organisational research that leadership plays an important role in shaping perceptions and beliefs about work and required tasks (Wang, Tsui, and Xin 2011). Senior management support has also been posited as an important influence on information security perceptions, beliefs and attitudes (Hu, Hart, and Cooke 2007), but its effects are rarely examined empirically.

Only a few studies empirically examine the relationship between senior management support and information security attitudes. These provide conflicting findings. In an action research study, Puhakainen and Siponen (2010) observed that visible top management support (e.g. actively promoting security issues and leading by example through their own compliance behaviour) impacted employee information security attitudes and was important for achieving employee information security policy compliance. In contrast, Hu et al. (2012) did not find a significant relationship between senior management participation in information security initiatives and employee attitudes. A more recent study by Flores and Ekstedt (2016) also fails to find a significant relationship between these constructs.

In addition, to our knowledge, only one study examines the direct effects of senior management on information security norms and self-efficacy, finding evidence for a positive relationship (see Hu et al. 2012). Overall, there is either conflicting or limited evidence for the effects of senior management support on information security attitudes, norms and self-efficacy beliefs. To investigate this further, we formulate and test the following hypothesis:

> H1: Senior management support positively influences information security (a) attitudes, (b) self-efficacy and (c) norms.

2.2 The influence of workplace norms

The perceived expectations of relevant others, or subjective norms, have an established influence on intended information security behaviours (Herath and Rao 2009a; AlHogail 2015; McGill and Thompson 2017). Theoretical frameworks, the theory of reasoned action (TRA) (Ajzen and Fishbein 1980) and the TPB (Ajzen 1991), which is an extension of the TRA, conceptualise this relationship, and a number of information security studies find empirical support in terms of subjective norms (or normative beliefs) significantly influencing intentions to comply with information security policies (Herath and Rao 2009b; Bulgurcu, Cavusoglu, and Benbasat 2010; Siponen, Pahnila, and Mahmood 2010).

However, the role or influence of workplace norms on employees' attitudes and beliefs about their own skills and ability to undertake specific tasks and actions (i.e. self-efficacy) has either been largely ignored or assumed to independently affect intentions to comply (Guo et al. 2011; Warkentin, Johnston, and Shropshire 2011). Two studies provide empirical evidence of a relationship between norms and attitudes in the context of information security. A study by Guo et al. (2011) finds that workplace norms had a strong effect on employees' intentions to engage in non-malicious security violations, while, in a study of information security policy compliance, Ifinedo (2014) finds that subjective norms had a positive effect on compliance attitudes.

While there is nascent evidence of a relationship between workplace norms and information security attitudes, the influence of norms on employees' information security self-efficacy is yet to be examined empirically. A study by Warkentin, Johnston, and Shropshire (2011) found that persuasive messages from peers were associated with self-efficacy to comply with information security policies. Although this study does not focus specifically on the workplace norms construct, these findings are suggestive of the potential for it to have a positive impact on self-efficacy beliefs. Consequently, we propose:

> H2: Norms about information security positively influences information security (a) attitudes and (b) self-efficacy.

2.3 The influence of formal controls

In addition to the previous hypotheses, we are also interested in investigating whether and how workplace norms mediate the relationship between formal controls and information security attitudes and self-efficacy beliefs. To do this, we develop hypotheses between these variables that we test in our empirical study in the sub-sections that follow.

Organisational control systems research classifies formal controls into mechanisms that seek to regulate behaviours and those that measure outputs and outcomes of behaviours (Ouchi 1979; Merchant and Van Der Stede 2007). Policies and procedures exemplify the former in prescribing or proscribing required actions on the part of employees, while monitoring mechanisms and performance measures that evaluate the positive and negative achievements of employees illustrate the latter. Additionally, rewards may be offered or sanctions imposed. Hence, we investigate the following formal controls: (1) the specification of information security procedures, (2) performance monitoring and evaluation, and (3) the use of rewards and sanctions.[2] The paragraphs below detail the hypothesised effects of these formal controls on our dependent variables of interest.

2.3.1 Specification of procedures

Specification (i.e. formalised statements) of expected information security behaviours and objectives in the form of information security policies and procedures makes explicit the rules and guidelines for acceptable use of information resources (Kirsch and Boss 2007; Tsohou, Karyda, and Kokolakis 2015). Specification outlines the behaviours required from employees if they are to comply with the information security objectives of the organisation. In so doing, the importance of compliance to the organisation is communicated to employees, as are the organisation's expectations and this affects employee attitudes (Boss et al. 2009). Past research also identifies a relationship between the specification of organisational procedures for workplace norms (Jarrahi and Sawyer 2015; Safa et al. 2015; Dang-Pham, Pittayachawan, and Bruno 2016).

In addition, Herath and Rao (2009b) found that the availability of resources that facilitate information security compliance, including information security policies, significantly enhanced employee self-efficacy. Information security policies and procedures are a resource for employees to refer to for guidance in relation to information security compliance; thus, the presence of formal information security policies can serve as a mechanism that supports employees' ability to comply with information security requirements, thereby having positive self-efficacy effects (Lowry and Moody 2015). Accordingly, we expect specification to positively influence attitudes, norms and self-efficacy:

> H3: Specification of information security policies and procedures positively influences information security (a) attitudes, (b) self-efficacy and (c) norms.

2.3.2 Monitoring and evaluation

Monitoring and evaluation of employee performance in relation to information security are likely to affect attitudes and norms. The use of this control mechanism signals positive outcomes to be achieved and negative ones to be avoided by employees. It directs attention towards what is measured (Merchant and Van Der Stede 2007) and puts the onus on the employee to achieve expected performance on these measured dimensions. Hence monitoring and evaluation are often coupled (Vance, Siponen, and Pahnila 2012). In the context of information security, monitoring and evaluation of employees in terms of breaches, compliance and proper information management practices, again signals the importance of security and what is expected of employees (Boss et al. 2009; Chen, Ramamurthy, and Wen 2015), as well as promoting a sense of obligation and accountability (Vance, Siponen, and Pahnila 2012), thereby likely to positively influence both attitudes and workplace norms (see also Da Veiga and Martins 2015; Dang-Pham, Pittayachawan, and Bruno 2016).

Monitoring and evaluation also provide feedback and potential learning opportunities for employees in terms of information security requirements and their practices (Da Veiga and Martins 2015). It allows individuals 'to assess current status and make adjustments as necessary' (Boss et al. 2009, 154), not only to address undesirable behaviours but also to enhance desirable ones (Vance, Siponen, and Pahnila 2012). We posit that ability to obtain feedback and address awareness and knowledge gaps, facilitated by monitoring and evaluation, is likely to be beneficial for self-efficacy. Hence, we hypothesise the following:

H4: Monitoring and evaluation positively influence information security (a) attitudes, (b) self-efficacy and (c) norms.

2.3.3 Rewards and sanctions

Rewards and/or sanctions are an important mechanism for achieving congruence between employee goals and activities and organisational objectives. In the context of information security, studies posit the influence of rewards on policy compliance via perceived benefits of compliance (Bulgurcu, Cavusoglu, and Benbasat 2010). In relation to sanctions for information security non-compliance, prior studies establish the deterrence effects of this control mechanism (Straub 1990; Straub and Welke 1998; Hannah and Robertson 2015) and its influence on the perceived cost of non-compliance (Bulgurcu, Cavusoglu, and Benbasat 2010).

There has been much focus in previous information security behavioural studies on the role of sanctions. General Deterrence Theory (GDT) has featured prominently in this stream of research, with a focus in particular on the perceived certainty of detection and perceived severity of sanctions, which the theory posits act as disincentives or deterrents to prohibited behaviour (D'arcy and Herath 2011). In recent years, the role of non-punitive measures, such as rewards, to motivate employees to comply has also become a focus (e.g. Pahnila, Siponen, and Mahmood 2007; Bulgurcu, Cavusoglu, and Benbasat 2010; Siponen, Mahmood, and Pahnila 2014).

Findings from previous research in relation to the influence of sanctions on compliance intentions and/or behaviour have been mixed (Workman, Bommer, and Straub 2009; D'arcy and Herath 2011), as have findings in relation to the influence of rewards. Despite the lack of a clear picture from the information security literature regarding the role and impact of sanctions and rewards on intentions and/or behaviour, there is evidence to indicate that both are relevant factors that employees consider when thinking about and dealing with information security matters (Lowry and Moody 2015). As demonstrated by Bulgurcu, Cavusoglu, and Benbasat (2010), the use of sanctions and rewards feeds into assessments employees make about the overall consequences of compliance and non-compliance. Bulgurcu, Cavusoglu, and Benbasat (2010) found that rewards contributed to shaping employees' beliefs about the benefits of compliance, while sanctions contributed to shaping employees' beliefs about the costs of non-compliance (Hannah and Robertson 2015; Tsohou, Karyda, and Kokolakis 2015; Johnston et al. 2016). These beliefs about the consequences of compliance and non-compliance were found to significantly influence attitudes toward compliance and, in turn, intentions to comply with information security policies. Given the role the use of rewards and sanctions can have in shaping employees' beliefs about favourable and unfavourable consequences, it is expected that:

H5: The provision of rewards positively influences information security (a) attitudes, (b) self-efficacy and (c) norms.

H6: The imposition of sanctions positively influences information security (a) attitudes, (b) self-efficacy and (c) norms.

2.4 Summary

Figure 1 presents the research model and the hypothesised relationships to be tested. In our model, we propose attitude and self-efficacy as dependent constructs and norms as a mediating construct that contributes to

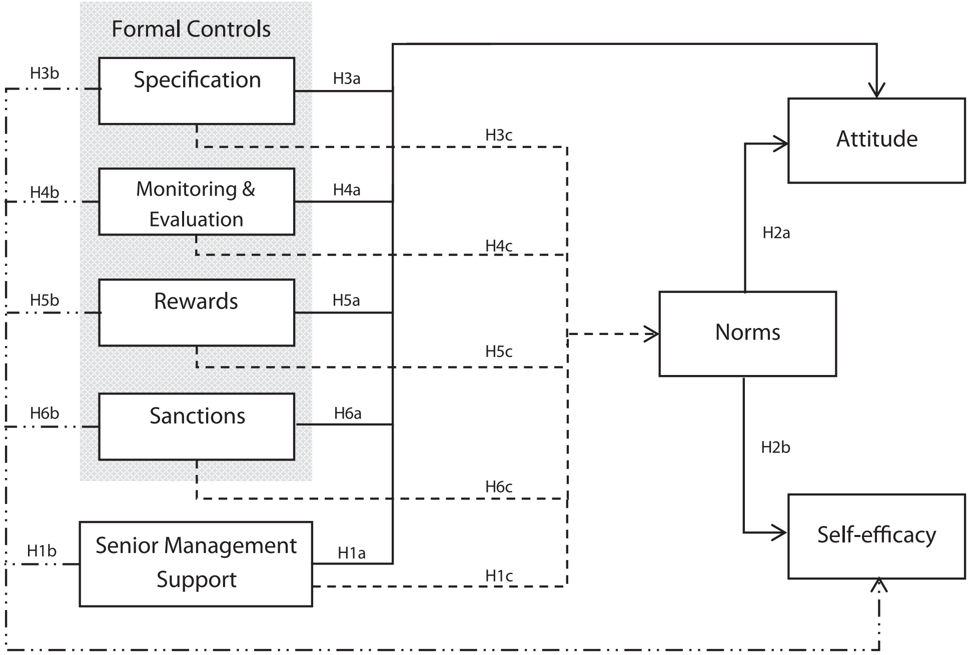


Figure 1. Hypothesised research model.

explaining information security attitudes and self-efficacy beliefs. Our independent variables comprise senior management support and formal controls (specification, monitoring and evaluation, rewards and sanctions). Overall, we propose a partial mediation model whereby senior management support and formal controls influence attitude and self-efficacy directly, as well as indirectly through the mediating role of norms.

3. Method

3.1 Context

To test the research model, data were collected via a web-based survey from employees at a law enforcement agency (LEA). Law enforcement is a context in which employees regularly deal with highly sensitive information; thus, information security is of paramount importance and the consequences of mishandling information can be wide-ranging and far-reaching. Information security breaches (whether intentional or unintentional) have the potential to jeopardise operational activities and may lead to highly damaging consequences not only for the individual/s directly involved but also for the organisation, the community and potentially other organisations, institutions and governments.

Information security was important for the LEA that was the empirical setting for the study. Law enforcement in general is a context where senior management can be expected to have a strong operational influence in terms of how investigations are prioritised and conducted. Social norms are also strong drivers of behaviours (Porter and Prenzler 2016). They are also rule-based organisations where one can expect formal controls to be in place. Despite the presence of information security protocols, LEA had experienced breaches in information security, suggestive that factors other than the formal controls – such as informal workplace dynamics, attitudes and/or beliefs – may be at play. In the year prior to the study, it had commenced an ‘information management’ programme to signal the need to secure information when employees obtained, handled, stored, exchanged and used information. As such, LEA represented a fruitful opportunity to investigate the interrelationships between senior management support, norms, formal controls and information security attitudes and beliefs.

3.2 Survey instrument

The survey instrument contained measures for attitude, self-efficacy, norms and five types of management control mechanisms: specification monitoring and evaluation; rewards; sanctions; and senior management support. The survey instrument was developed using items from existing scales used in related studies which were carried out in areas such as a large medical centre, defence technology and among experienced and well-trained IT users, and though none of these was specifically conducted in LEAs, modifications were made to better suit the context of this study. Multiple-item scales were used and all constructs were measured reflectively as the indicator items used to measure each construct represented the same concept and were expected to be highly correlated with each other (Hair et al. 2006). All items were measured on 7-point rating scales. Items for attitude were measured using a semantic differential response format, while self-efficacy, norms and management controls were all measured using 7-point Likert scales, where ‘1’ indicated ‘strongly disagree’ and ‘7’ indicated ‘strongly agree’.

The items measuring attitude to information security (four adjective pairs) and norms about information security (three items) were adapted from Bulgurcu, Cavusoglu, and Benbasat (2010), while the four items measuring information security self-efficacy were adapted from Bulgurcu, Cavusoglu, and Benbasat (2010) and Workman, Bommer, and Straub (2008). Turning to the formal controls, use of specification was measured using four items sourced from Boss et al. (2009), D’arcy, Hovav, and Galletta (2009) and Lee and Choi (2003). The use of monitoring and evaluation controls was measured using seven items, comprising five items sourced from Boss et al. (2009) and D’arcy, Hovav, and Galletta (2009) and two additional reverse coded items developed by the researchers. Use of rewards was measured using three items derived from Boss et al. (2009), and the use of sanctions was measured using three items derived from Bulgurcu, Cavusoglu, and Benbasat (2010). Finally, senior management support was measured using four items sourced from Knapp et al. (2006).

The survey instrument was pilot tested with LEA employees. Based on the responses and feedback received, minor modifications were made to introductory statements, terminology and question wording. As noted earlier, the terminology of ‘information management’ had been widely used at LEA as a means of emphasising and focusing employees on information security. Indeed, ‘information management’ was equated with ‘information security’ in LEA with the former term actually more widely understood and used. Feedback from the pilot was consistent with this, indicating that using the term information security rather than information management would create ambiguity and confusion. Hence, items that measured formal controls and senior management support were reworded to contain information management terminology rather than information security and a definition of information management was provided in the survey instrument immediately prior to these questions to further enhance clarity.

The Appendix contains the constructs used in the study, the studies that items were drawn from, the information management definition that was used to aid interpretation and the final wording of measurement items. Overall, the changes made were considered to improve face validity, aid interpretation of questions and improve the overall ease of survey completion.

3.3 Data collection

A purposive sampling approach was taken. Work areas with a high need to secure information were identified jointly by the researchers and senior-level LEA employees with relevant expertise and experience. Two work areas were selected with the number of employees in these areas totalling 1191. The type of work undertaken by these employees focused on ‘high-end’ serious and organised criminal investigations and intelligence and covert operations, respectively. Employees from these areas dealt with highly sensitive information concerning serious and organised criminals, their illegal activity and the actions that LEA was taking in response. Employees had to classify information, consider how to store this securely in IS and apply protocols in deciding what information could be shared with whom without jeopardising the law enforcement operations they were conducting.

All employees from the targeted work areas were invited to participate in the survey via an email with information about the study and the survey site link. At the end of the survey period, 411 employees had accessed the survey, from which 63 incomplete and 10 unreliable responses were excluded. Unreliable responses were identified through data screening, including checks for outliers and influential points and checks for patterns indicative of careless or inattentive responding (see Meade and Craig 2012). This included patterns such as consecutive ratings of a single response (e.g. all ‘4s’), ratings concentrated at one end (e.g. ‘6s’ and ‘7s’) or between either ends of the scale (e.g. ‘1s’ and ‘7s’), and/or apparent failure to notice negatively worded items. The final sample included 338 responses, reflecting an acceptable response rate of 28%.

The demographic profile of respondents is provided in Table 1 and visually represented in Figure 2. Over two-thirds (70%) of respondents were ‘sworn’ law enforcement officers, and over two-thirds (70%) were male. Over one-third (38%) were aged 41–50 years, half (49%) had worked at the organisation for more than 15 years and over half (59%) were in junior-ranked roles.

4. Data analysis and results

The research model was analysed using the partial least squares (PLS) structural equation modelling (SEM) technique, with SmartPLS 3 software (see Ringle, Wende,

Table 1. Profile of survey respondents ($n = 338$).

Demographic variables	Frequency	Percentage (%)
Gender[a]		
Male	235	69.8
Female	102	30.2
Age group		
25 or under	9	2.7
26–30	29	8.6
31–35	58	17.2
36–40	38	11.2
41–45	73	21.6
46–50	55	16.3
51–55	52	15.4
56 or over	24	7.1
Officer status		
Sworn officer	235	69.5
Public servant	103	30.5
Management level		
Junior	198	58.6
Middle	118	34.9
Senior	22	6.5
Years of service[a]		
Less than 5 years	60	17.8
5 to less than 10 years	49	14.5
10 to less than 15 years	63	18.7
15 to less than 20 years	37	11.0
20 or more years	128	38.0

[a]One respondent did not respond to the question item.

and Becker 2015). SEM techniques allow analysis of multiple relationships among latent variables that have been measured by multiple indicators (Vinzi, Trinchera, and Amato 2010). Moreover, paths pertaining to the measurement of the latent variables (i.e. the measurement model) and paths pertaining to the hypothesised relationships between the latent variables (i.e. the structural model) can be estimated simultaneously within the one technique (Gefen, Straub, and Rigdon 2011). PLS was selected over covariance-based SEM because the research objective was exploratory and oriented more towards prediction and theory-building, rather than theory-confirmation (Gefen, Straub, and Rigdon 2011).

4.1 Preliminary analyses

Graphical and statistical techniques were used to assess the distributions of measured variables, and a number showed non-normal distributions. However, the presence of non-normal data was not regarded as problematic as PLS does not assume data follow a particular distributional pattern (Chin 2010) and the sample size was sufficiently large. The commonly cited guideline regarding sample size requirements for PLS is the 'ten-times-rule'. This states the minimum requirement as ten times the number of indicators (at measurement level) or number of paths (at structural level) of the

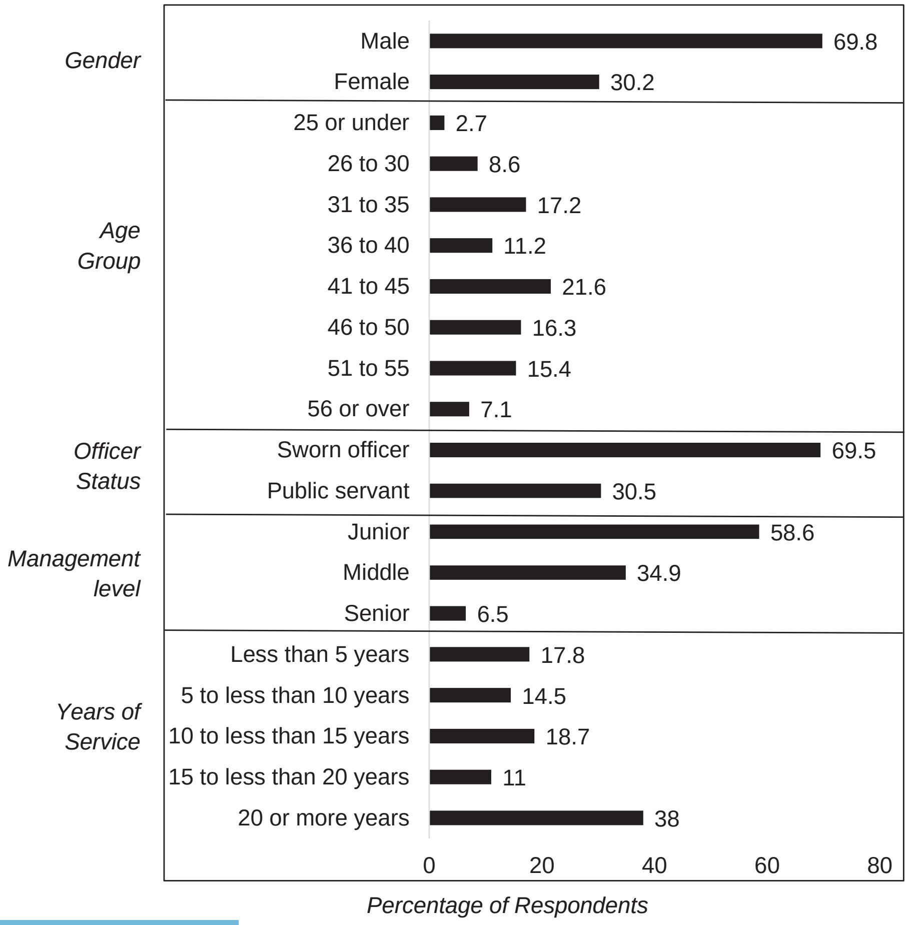


Figure 2. Visual profile of survey respondents ($n = 338$).

Table 2. Descriptive statistics.

Construct	Number of items	Mean	Standard deviation
Attitude to information security	4	6.62	0.73
information security self-efficacy	4	5.40	1.11
Norms about information security	3	6.14	0.87
Specification	4	5.65	0.90
Monitoring & evaluation	7	4.30	1.06
Rewards	3	2.46	1.09
Sanctions	3	5.10	1.32
Senior management support	4	5.61	1.20

most complex construct, whichever is larger (Barclay et al. 1995 cited in Henseler, Ringle, and Sinkovics 2009). However, other factors still need to be considered in relation to sample size, including distributional patterns (Hair et al. 2012; Marcoulides and Saunders 2006). As our data showed some deviations from normality, it was important that our sample size exceeds the ‘ten times’ minimum requirement, which it does, being over five times larger than the minimum we would require as per the ‘ten times’ rule. Importantly, a larger sample size provides more stable parameter estimates (Marcoulides and Saunders 2006). Descriptive statistics for each construct are presented in Table 2.

Common method bias is frequently cited as a potential problem with self-report surveys, as the predictor and criterion variables are measured with the same method and the data obtained come from the same source, that is, the individual respondent (Podsakoff et al. 2003). While there is a lack of consensus among scholars as to whether common method bias is indeed a real problem in survey research (Spector 2006), we nonetheless conducted the widely used Harman’s single factor test. Exploratory factor analysis (unrotated) was used to test whether one factor could account for all, or the majority (i.e. more than half), of the variance in the data. Multiple factors rather than a single factor emerged from the analysis, with the first factor accounting for less than half (32%) of the variance. These results were taken to indicate that common method bias was unlikely to be a serious concern in this study.

4.2 Measurement model

Evaluation of the measurement model involved assessing the reliability and validity of the model’s constructs with results presented in Table 3. Internal consistency reliability was evaluated using composite reliability and Cronbach’s α measures. Both measures are interpreted in the same way, with 0.70 generally considered to be the benchmark (Nunnally 1978) and values below 0.60 suggesting lack of reliability (Henseler, Ringle, and Sinkovics 2009). In this study, composite reliability and Cronbach’s α values were above 0.70 for all scales except specification. Composite reliability for specification was adequate; however, Cronbach’s α was below 0.60.

The reliability of individual items was assessed by examining the loadings of each indicator item with the construct it was designed to measure. Ideally, item loadings should be 0.70 or higher and loadings below 0.50 are unacceptable (Chin 1998; Hair et al. 2006; Hulland 1999). Of the 32 indicator items in this study, five had loadings below 0.70. Three were clearly above the minimum threshold (0.50) at close to or above 0.60; thus, the decision was made to retain these items. The other two items, however, were dropped due to loadings below 0.50. Both were items measuring specification and following their deletion Cronbach’s α for specification increased from 0.53 to 0.61, therefore showing an acceptable level of reliability (>0.60).

Assessment of convergent validity considers whether a set of indicator items represent the same underlying construct they were designed to measure (Henseler, Ringle, and Sinkovics 2009). Convergent validity was assessed based on the average variance extracted (AVE), as described by Fornell and Larcker (1981). The suggested guideline is that AVE values of at least 0.50 (i.e. 50%) are indicative of adequate convergent validity, as this demonstrates that the variance accounted for by the construct is greater than the variance due to measurement error (Fornell and Larcker 1981). In this study, AVE values for all constructs were greater than 0.50.

Discriminant validity, which can be assessed at construct and at indicator level, is concerned with whether

Table 3. Composite reliability, Cronbach’s α, AVE and squared inter-construct correlations.

	Composite Reliability	Cronbach’s α	1	2	3	4	5	6	7	8
1. Attitude	0.96	0.95	**0.87**							
2. Self-efficacy	0.89	0.83	0.08	**0.67**						
3. Norms	0.94	0.91	0.17	0.19	**0.84**					
4. Specification	0.84	0.61	0.08	0.23	0.19	**0.72**				
5. Monitoring & evaluation	0.89	0.85	0.05	0.23	0.17	0.23	**0.54**			
6. Rewards	0.86	0.79	0.00	0.03	0.02	0.02	0.14	**0.68**		
7. Sanctions	0.93	0.88	0.02	0.05	0.06	0.07	0.10	0.01	**0.81**	
8. Senior management support	0.93	0.91	0.11	0.21	0.21	0.24	0.42	0.11	0.11	**0.78**

Note: Diagonal elements display AVE and off diagonals display squared inter-construct correlations.

constructs that are considered to be conceptually different are indeed sufficiently different from each other (Henseler, Ringle, and Sinkovics 2009). At the construct level, using the Fornell–Larcker criterion, adequate discriminant validity is evident if the AVE of a construct is greater than the highest squared correlation between that construct and each of the other constructs in the model (Fornell and Larcker 1981; Chin 1998; Henseler, Ringle, and Sinkovics 2009). In this study, this condition was met for all constructs.

At the indicator item level, discriminant validity can be assessed based on cross-loadings (Henseler, Ringle, and Sinkovics 2009). To demonstrate adequate discriminant validity, an item should have a higher loading with the construct it was designed to measure than it has with other constructs, that is, its cross-loadings (Chin 1998). However, in the absence of clear-cut thresholds for loadings when assessing discriminant validity, the size of the difference between an indicator item's loading on its assigned construct and its cross-loadings should be taken into consideration (Gefen and Straub 2005). In this study, adequate discriminant validity was demonstrated as all items had much higher loadings for their respective constructs than for other constructs.

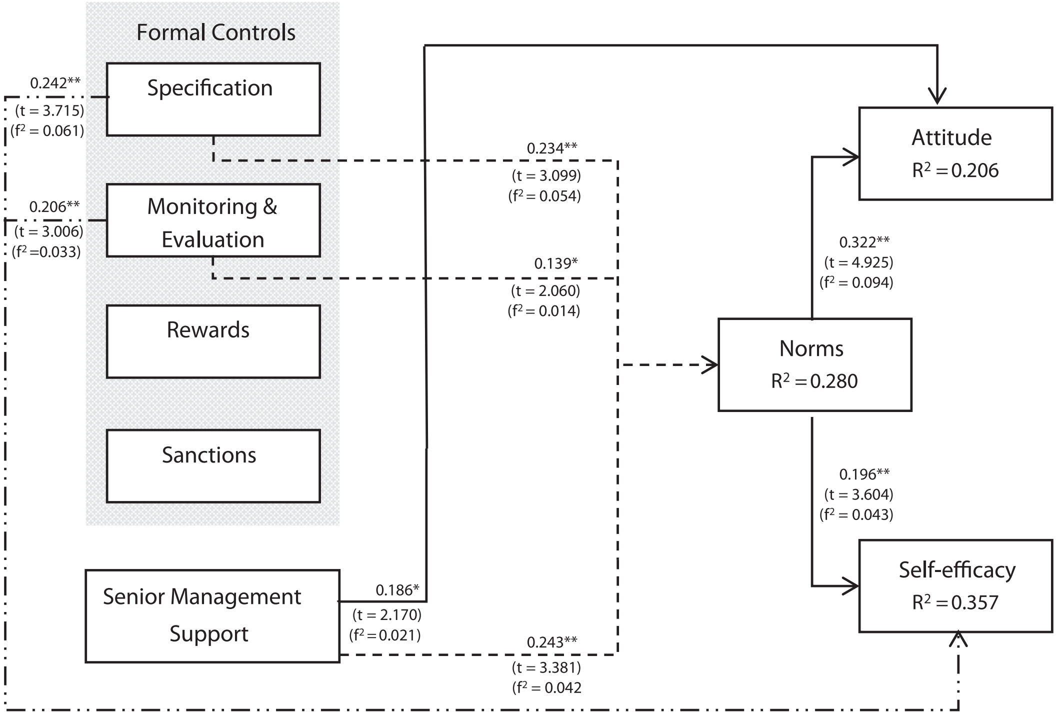
A standardised root mean square residual (SRMR) was also calculated to obtain insight into the model's goodness of fit. The calculated SRMR was 0.06. This meets the suggested threshold where a value of 0.08 or less is generally seen as indicative of an acceptable model (Hu and Bentler 1999).

4.3 Structural model

Evaluation of the structural component of the model involved examining the amount of variance explained for each dependent variable, as well as the signs and significance of the path coefficients. Calculations were performed with SmartPLS 3 using the PLS algorithm and bootstrapping resampling procedure (with 338 cases and 5000 resamples). The results obtained for the structural model are presented in Figure 3. Figure 3 only illustrates those paths that were found to be statistically significant, and reports path coefficients, *t*-statistics, direct effect sizes and R^2 statistics.

The explanatory power of the structural model was assessed based on the R^2 values, which represent the amount of variance in the dependent variables explained by the model (Chin 2010). The model explained 21% of the variance in attitude, 36% of the variance in self-efficacy and 28% of the variance in norms. Individual hypotheses testing results and effect sizes associated with significant associations are provided in Table 4.

Senior management support was found to have a significant influence on attitude and norms but not self-efficacy. Thus H1a and H1c were supported. Norms were found to significantly influence attitude and self-efficacy



**p<0.01 *p<0.05

Figure 3. Structural model.

Table 4. Tests of hypotheses.

Hypothesis	Relationship			Support	Significance	Direct effect size (f^2)
H1a	Senior mgmt support	(+) →	Attitude	Yes	$p < .01$	0.021
H1b	Senior mgmt support	(+) →	Self-efficacy	No	$p > .05$	
H1c	Senior mgmt support	(+) →	Norms	Yes	$p < .01$	0.042
H2a	Norms	(+) →	Attitude	Yes	$p < .01$	0.094
H2b	Norms	(+) →	Self-efficacy	Yes	$p < .05$	0.043
H3a	Specification	(+) →	Attitude	No	$p > .05$	
H3b	Specification	(+) →	Self-efficacy	Yes	$p < .01$	0.061
H3c	Specification	(+) →	Norms	Yes	$p < .01$	0.054
H4a	Monitoring & evaluation	(+) →	Attitude	No	$p > .05$	
H4b	Monitoring & evaluation	(+) →	Self-efficacy	Yes	$p < .01$	0.033
H4c	Monitoring & evaluation	(+) →	Norms	Yes	$p < .05$	0.014
H5a	Rewards	(+) →	Attitude	No	$p > .05$	
H5b	Rewards	(+) →	Self-efficacy	No	$p > .05$	
H5c	Rewards	(+) →	Norms	No	$p > .05$	
H6a	Sanctions	(+) →	Attitude	No	$p > .05$	
H6b	Sanctions	(+) →	Self-efficacy	No	$p < .01$	
H6c	Sanctions	(+) →	Norms	No	$p < .05$	

with evidence supporting H2a and H2b obtained. Support was also found for H3b and H3c with specification found to significantly influence self-efficacy and norms. A similar pattern was observed for monitoring and evaluation, with findings of significant effects for self-efficacy and norms supporting H4b and H4c. Our hypotheses regarding rewards (H5a, H5b and H5c) and sanctions (H6a, H6b and H6c) were not supported, as neither rewards nor sanctions were shown to have a significant influence on attitude, self-efficacy or norms.

In relation to direct effect sizes, Cohen (1988) proposes that a f^2 statistic of 0.02, 0.15 and 0.35 be interpreted as small, medium and large respectively. All significant relationships had direct effect sizes that exceeded the small effect threshold, except for senior management support to attitude which just met the threshold ($f^2 = 0.021$), and monitoring and evaluation to attitude which was less than the 0.02 threshold ($f^2 = 0.014$). Norms to attitude had the highest direct effect size observed ($f^2 = 0.094$), being approximately the mid-point between the small and medium effect size thresholds.

While senior management support, specification and monitoring and evaluation had significant but approximately small direct effects on attitudes and self-efficacy, these variables also had indirect effects via norms. Hence, a further evaluation of the PLS results was undertaken by examining the magnitude and significance of the total effects (the combined direct and indirect effects) of these independent variables on attitudes and self-efficacy. The total effects, ordered by magnitude, are shown in Table 5. The two most important influences on attitude were norms, followed by senior management support, while the two most important influences on self-efficacy were specification, followed by monitoring and evaluation.

It can be seen in Table 5 that, based on total effects, senior management support was a significant source of influence on self-efficacy, and specification was a significant source of influence on attitude. These results are of interest given the finding that, in our partial mediation model, both of these hypothesised relationships were not supported. In light of this pattern of results, recalling also that both senior management support and specification were found to significantly influence norms, the possibility of full mediation was explored by running the PLS analysis without norms (the mediator). In the absence of the mediator, the direct relationship between senior management support and self-efficacy was significant ($\beta = 0.169$, $p < .05$), and so too was the direct relationship between specification and attitude (= 0.166, $p < .05$). The results suggested that the influence of senior management support on self-efficacy was fully mediated by norms, and the influence of specification on attitude was fully mediated by norms.

5. Discussion

Continued evidence of employee-related information security breaches, despite significant organisation attention to the matter, suggests a need for more research on the human dimension of information security

Table 5. Total effects on attitude and self-efficacy.

	Coefficient	t-value	P
Attitude			
Norms → Attitude	0.322	4.925	$p < .01$
Senior management support → Attitude	0.264	3.218	$p < .01$
Specification → Attitude	0.166	2.109	$p < .05$
Sanctions → Attitude	0.022	0.446	$p > .05$
Monitoring & evaluation → Attitude	−0.013	0.213	$p > .05$
Rewards → Attitude	−0.052	0.967	$p > .05$
Self-efficacy			
Specification → Self-efficacy	0.287	4.296	$p < .01$
Monitoring & evaluation → Self-efficacy	0.233	3.299	$p < .01$
Norms → Self-efficacy	0.196	3.604	$p < .01$
Senior management support → Self-efficacy	0.171	2.511	$p < .05$
Sanctions → Self-efficacy	0.007	0.146	$p > .05$
Rewards → Self-efficacy	−0.010	0.229	$p > .05$

(Workman, Bommer, and Straub 2009; Abawajy 2014). Responding to calls for further research on how the informal elements of workplaces affect employees' thinking about information security (Guo et al. 2011; Warkentin, Johnston, and Shropshire 2011), this study examines how two informal workplace dynamics, namely norms and senior management support, influence information security attitudes and self-efficacy beliefs alongside formal controls. The study offers a number of important findings with implications for theory and practice.

5.1 Implications for theory

One important set of findings relates to the central role that workplace norms play in influencing employee attitudes and self-efficacy beliefs about information security. The information security literature finds that both workplace norms and employee attitudes directly influence information security behaviours (e.g. Herath and Rao 2009b; Siponen, Pahnila, and Mahmood 2010; Bulgurcu, Cavusoglu, and Benbasat 2010). Only a few studies, however, investigate the link between norms and attitudes specifically. We add to these few studies (for example, Guo et al. 2011; Ifinedo 2014) by finding that norms have a significant and sizeable influence on employee attitudes about information security (H2a).

In addition, we find a statistically significant relationship between norms and self-efficacy (H2b), albeit with a small effect size. Prior research indicates the importance of social persuasion and vicarious experiences for self-efficacy (Rhee, Kim, and Ryu 2009; Warkentin, Johnston, and Shropshire 2011), but has not explicitly examined the norms–self-efficacy relationship. Our findings indicate that the expectations of others have a positive influence on the beliefs of individuals in their abilities to mobilise the necessary resources and carry out the courses of action necessary for information security compliance. These results suggest that individuals derive confidence in their ability to comply with information security requirements in part when they observe others in the workplace doing the same, possibly because they see these others as sources of guidance and expertise that can be relied upon (Guo et al. 2011).

In addition, our analysis reveals that norms fully mediate the effect of other antecedents, namely senior management support on self-efficacy and procedure specification on attitudes. This finding adds further weight to the important effects that practices and expectations of influential workplace participants have on the information security intentions and behaviours of individuals within the organisation. However, the context of the study needs to be considered when interpreting these findings.

Law enforcement is a workplace where social norms are strong drivers of behaviours (Porter and Prenzler 2016). Close and influential bonds form within workgroups and teams and employees tend to place high value on 'fitting in' with the expectations of others (Chan, Devery, and Doran 2003), and it is plausible that the characteristics of this setting may help to explain the results we observed in relation to norms. In relation to this, however, we argue that our findings are not restricted to law enforcement settings alone. Indeed, there are other organisational contexts where norms have been shown to exert strong effects on employee behaviour, although not in relation to information security specifically. These include faith-based and social organisations (Kreiner, Hollensbe, and Sheep 2006) as well as parts of the financial service sector (Nicholson, Kiel, and Kiel-Chisholm 2011) and consulting (Alvesson and Kärreman 2004).

Equally, there are workplaces where employees are likely to place more value on individualism rather than conformity with collective expectations. Here, it is reasonable to expect that the importance of norms in shaping individual information security attitudes and beliefs may be diminished. Further work is thus required to investigate how particular types of workplace contexts (in terms of individual–collective tendencies) influence the role and effects that norms have on information security attitudes and behaviours of employees.

Another important finding of this study is to highlight how perceptions of senior management support can both directly influence employees' information security attitudes (H1a), as well as have indirect effects via workplace norms (H1c and H2a). Prior research has tended to consider senior management as removed from the day-to-day activities of employees and hence unlikely to have an impact on information security attitudes of employees (Alnatheer, Chan, and Nelson 2012; Hu et al. 2012). Indeed, even the main exception – Puhakainen and Siponen (2010) who find a link between senior management support and employee attitudes – caveats their finding by noting that it was obtained in a small organisation. In contrast, our study provides empirical support for the view that senior management can directly influence information security attitudes of employees, even in large organisations.

Hu et al. (2012) posit that that contingent factors such as organisational structure and leadership style might influence the senior management–attitude relationship. LEA, being a law enforcement organisation, is typified by strong leadership structures for operational matters with senior managers typically having experience and history in the 'front line'. In this context, it is likely that the actions of organisational leaders will have more immediate impacts on employees' information security attitudes and behaviours, rather than the trickle-down effects observed by other studies (e.g. Hu et al. 2012). However, achieving this requires the senior management to go beyond simply 'commanding' or requiring information security compliance, to providing visible support for information security, as well as role modelling the required behaviours (Knapp et al. 2006). Given the importance of understanding the role that senior managers can play in information security (Puhakainen and Siponen 2010; Hu et al. 2012), it is important for future research to empirically examine how the quality and nature of the relationship between senior management and employees influence the effects of senior management support on individual employee information security attitudes and behaviours.

Finally, turning to formal controls, we find positive relationships between procedure specification and both self-efficacy (H3b) and norms (H3c). We also find a positive association between monitoring and evaluation and self-efficacy (H4b) and norms (H4c). These results indicate that these control types offer important resources and assistance for individual employees in terms of their information security initiatives. Procedure specification stipulates what needs to be done, while monitoring and evaluation provide feedback and learning opportunities for employees as they engage in information security compliance. Indeed, the awareness that monitoring and evaluation procedures are in place may provide employees with reassurance in terms of an additional safety net in case they make unintentional mistakes or breaches. Both of these control types also influence the expectations of others in the workplace, suggesting that the provision of these resources is also associated with heightened expectations about information security behaviours.

The results obtained also did not indicate support for hypothesised relationships between rewards or sanctions and information security attitudes, self-efficacy or norms. One explanation for our lack of observed effects for these control mechanism pertains to our research setting. Extensive rewards were not provided for information security behaviours due to the organisation being a part of the government (see mean for the Rewards construct in Table 2). Also, sanctions are likely to have less effect when influences on information security are likely to be internalised (employees are law enforcement officers), or driven in the main by the informal aspects of their workplace and specifically the expectations of others and senior management's support for information security. Future research thus needs to examine rewards/sanctions as part of a broader organisational approach (Guo et al. 2011).

5.2 Practical implications

Our results pose a number of implications for practitioners interested in the human aspects of information security. First, careful attention must be paid to informal workplace dynamics (see also Warkentin, Johnston, and Shropshire 2011). Our findings indicate the importance of taking a 'bottom-up' perspective. The influence of norms on both attitudes and self-efficacy, and in mediating the effects of both senior management support and formal controls, suggests that changing information security intentions and behaviours requires locally embedded or organic initiatives within the immediate workgroup of the employee. Furthermore, those tasked with improving information security need to consider the role of senior management from an 'employee-centric' perspective and examine how people within the organisation perceive its leaders' support for information security through their communication and role modelling behaviours.

5.3 Limitations, future research and conclusion

Some limitations apply to our study. First, we focused on antecedents to information security intentions to comply and behaviours, and did not study these variables directly. Investigating the effects of senior management support, norms and formal controls directly on intentions and via attitudes, self-efficacy and norms represents an opportunity for future research in developing a more complete model of information security behaviours. One specific line of inquiry that future research might take involves the collection and analysis of qualitative data that unpacks the different ways that informal workplace dynamics shift information security attitudes and behaviours and the various contingent influences on this relationship. Another relates to quantitative examinations incorporating cross-over effects between attitudes, norms and self-efficacy, to explore in more detail which of these antecedents has more potent effects for information security behaviours.

Also, as we noted earlier, our findings in relation to the important role of informal dynamics on information security attitudes and beliefs are not necessarily generalisable beyond contexts similar to our research setting (in terms of the organisations where individuals are predisposed to compliance with collective expectations and strong leadership structures). In addition, a note of caution must be taken when interpreting the results we obtained in relation to rewards and sanctions. Further work examining the separate and joint effects of these mechanisms is required. More broadly, research is required to examine whether the findings we obtained in relation to formal controls apply in other settings and the nature of these relationships. Cross-sectional surveys conducted in other organisational contexts will be useful here, as will be longitudinal research that explores how formal controls are perceived by employees and how these reactions then translate into changes in information security behaviours within the workplace.

In closing, we highlight in this study the importance of senior management support and workplace norms for information security attitudes and self-efficacy beliefs, which in turn are key antecedents to information security behaviours. Further research on the human aspects of information security can usefully extend on the study's findings.

Notes

1. We use the term 'workplace norms' and 'norms' interchangeably to refer to subjective norms in an organisational setting.
2. We consider the effects these mechanisms on employees in terms of broad goal and behavioural alignment (e.g. Boss et al. 2009) rather than from a pure deterrence perspective (e.g. D'arcy, Hovav, and Galletta 2009).

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by Australian Research Council [Grant Number LP1101001228].

References

Abawajy, J. 2014. "User Preference of Cyber Security Awareness Delivery Methods." *Behaviour & Information Technology* 33 (3): 237–248.

Ajzen, I. 1991. "Theory of Planned Behaviour." *Organizational Behavior and Human Decision Processes* 50 (2): 179–211.

Ajzen, I., and M. Fishbein. 1980. "Prediction of Goal-Directed Behavior: Attitudes, Intentions, and Perceived Behavioral Control." *Journal of Experimental Social Psychology* 22: 453–474.

Alavi, R., R. Alavi, S. Islam, S. Islam, H. Mouratidis, and H. Mouratidis. 2016. "An Information Security Risk-Driven Investment Model for Analysing Human Factors." *Information and Computer Security* 24 (2): 205–227.

AlHogail, A. 2015. "Design and Validation of Information Security Culture Framework." *Computers in Human Behavior* 49: 567–575.

Alhogail, A., A. Mirza, and S. H. Bakry. 2015. "A Comprehensive Human Factor Framework for Information Security in Organizations." *Journal of Theoretical and Applied Information Technology* 78 (2): 201.

Alnatheer, M., T. Chan, and K. Nelson. 2012. Understanding and measuring information security culture." In *Proceedings of Pacific Asia Conference on Information Systems*. http://aisel.aisnet.org/pacis2012/144.

Alvesson, M., and D. Kärreman. 2004. "Interfaces of Control. Technocratic and Socio-Ideological Control in a Global Management Consultancy Firm." *Accounting, Organizations and Society* 29: 423–444.

Boss, S. R., L. J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss. 2009. "If Someone is Watching, I'll do What I'm Asked: Mandatoriness, Control, and Information Security." *European Journal of Information Systems* 18 (2): 151–164.

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

Chan, J., C. Devery, and S. Doran. 2003. *Fair Cop: Learning the Art of Policing*. Toronto: University of Toronto.

Chen, Y., K. Ramamurthy, and K. W. Wen. 2013. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?" *Journal of Management Information Systems*, 29 (3): 157–188. Winter 2012–13.

Chen, Y. A. N., K. R. A. M. Ramamurthy, and K. W. Wen. 2015. "Impacts of Comprehensive Information Security Programs on Information Security Culture." *Journal of Computer Information Systems* 55 (3): 11–19.

Chin, W. W. 1998. "The Partial Least Squares Approach for Structural Equation Modelling." In *Modern Methods for Business Research*, edited by G. A. Macoulides, 295–336. Hillsdale, NJ: Lawrence Erlbaum Associates.

Chin, W. W. 2010. "How to Write up and Report PLS Analyses." In *Handbook of Partial Least Squares*, edited by V. E. Vinzi, W. W. Chine, J. Hensler, and H. Wang, 655–690. Berlin: Springer.

Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences*. 2nd ed. Hillsdale, NJ: Lawrence Earlbaum Associates.

Dang-Pham, D., S. Pittayachawan, and V. Bruno. 2016. "Factors of People-Centric Security Climate: Conceptual Model and Exploratory Study in Vietnam." *arXiv preprint arXiv:1606.00884*.

D'arcy, J., and T. Herath. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings." *European Journal of Information Systems* 20: 643–658.

D'arcy, J., A. Hovav, and D. Galletta. 2009. "User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach." *Information Systems Research* 20 (1): 79–98.

Da Veiga, A., and N. Martins. 2015. "Improving the Information Security Culture Through Monitoring and Implementation Actions Illustrated Through a Case Study." *Computers & Security* 49: 162–176.

Dhillon, G., R. Syed, and C. Pedron. 2016. "Interpreting Information Security Culture: An Organizational Transformation Case Study." *Computers & Security* 56: 63–69.

Flores, W., and M. Ekstedt. 2016. "Shaping Intention to Resist Social Engineering Through Transformational Leadership, Information Security Culture and Awareness." *Computers & Security* 59: 26–44.

Fornell, C., and D. F. Larcker. 1981. “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error.” *Journal of Marketing Research* 18: 39–50.

Gefen, D., and D. Straub. 2005. “A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example.” *Communications of the Association for Information Systems* 16: 91–109.

Gefen, D., D. Straub, and E. Rigdon. 2011. “An Update and Extension to SEM Guidelines for Administrative and Social Science Research.” *MIS Quarterly* 35 (2): iii–xiv.

Guo, K. H., Y. Yuan, N. P. Archer, and C. E. Connelly. 2011. “Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model.” *Journal of Management Information Systems* 28 (2): 203–236.

Hair, J. F., W. C. Black, B. J. Babin, R. E. Anderson, and R. l. Tatham. 2006. *Multivariate Data Analysis*. New Jersey: Prentice Hall.

Hair, J. F., M. Sarstedt, C. M. Ringle, and J. A. Mena. 2012. “An Assessment of the use of Partial Least Squares Structural Equation Modeling in Marketing Research.” *Journal of the Academy of Marketing Science* 40 (3): 414–433.

Hannah, D. R., and K. Robertson. 2015. “Why and How Do Employees Break and Bend Confidential Information Protection Rules?” *Journal of Management Studies* 52 (3): 381–413.

Hedström, K., E. Kolkowska, F. Karlsson, and J. P. Allen. 2011. “Value Conflicts for Information Security Management.” *Journal of Strategic Information Systems* 20: 373–384.

Henseler, J., C. M. Ringle, and R. Sinkovics. 2009. “The Use of Partial Least Squares Path Modeling in International Marketing.” *Advances in International Marketing* 20: 277–319.

Herath, T., and H. Rao. 2009a. “Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness.” *Decision Support Systems* 47 (2): 154–165.

Herath, T., and H. Rao. 2009b. “Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations.” *European Journal of Information Systems* 18 (2): 106–125.

Hu, L., and P. M. Bentler. 1999. “Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives.” *Structural Equation Modeling* 6 (1): 1–55.

Hu, Q., T. Dhinev, P. Hart, and D. Cooke. 2012. “Managing Employee Compliance with Information Security Policies: The Critical Role of top Management and Organizational Culture.” *Decision Sciences* 43 (4): 615–660.

Hu, Q., P. Hart, and D. Cooke. 2007. “The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective.” *Journal of Strategic Information Systems* 16 (2): 153–172.

Hulland, J. 1999. “Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies.” *Strategic Management Journal* 20 (2): 195–204.

Ifinedo, P. 2014. “Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition.” *Information and Management* 51: 69–79.

ISACA. 2009. *Business Model for Information Security*. Rolling Meadows, IL.

Jarrahi, M. H., and S. Sawyer. 2015. “Theorizing on the Take-up of Social Technologies, Organizational Policies and Norms, and Consultants’ Knowledge-Sharing Practices.” *Journal of the Association for Information Science and Technology* 66 (1): 162–179.

Johnston, A. C., M. Warkentin, M. McBride, and L. Carter. 2016. “Dispositional and Situational Factors: Influences on Information Security Policy Violations.” *European Journal of Information Systems* 25 (3): 231–251.

Kayworth, T., and D. Whitten. 2010. “Effective Information Security Requires a Balance of Social and Technology Factors.” *MIS Quarterly Executive* 9 (3): 163–175.

Kirsch, L., and S. Boss, 2007. “The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines.” In *ICIS 2007 Proceedings*. http://Aisel.Aisnet.Org/Icis2007/103.

Knapp, K. J., T. E. Marshall, R. K. Rainer, and F. N. Ford. 2006. “Information Security: Management’s Effect on Culture and Policy.” *Information Management & Computer Security* 14 (1): 24–36.

Kreiner, Glen E., Elaine C. Hollensbe, and Mathew L. Sheep. 2006. “Where Is the ‘Me’ Among the ‘We’? Identity Work and the Search for Optimal Balance.” *Academy of Management Journal* 49 (5): 1031–1057.

Lee, H., and B. Choi. 2003. “Knowledge Management Enablers, Processes, and Organizational Performance: An Integrative View and Empirical Examination.” *Journal of Management Information Systems* 20 (1): 179–228.

Lowry, P. B., and G. D. Moody. 2015. “Proposing the Control-Reactance Compliance Model (CRCM) to Explain Opposing Motivations to Comply with Organisational Information Security Policies.” *Information Systems Journal* 25 (5): 433–463.

Marcoulides, G. A., and C. Saunders. 2006. “Editor’s Comments: PLS: A Silver Bullet?” *MIS Quarterly* 30 (2): Iii–IIx.

McGill, T., and N. Thompson. 2017. “Old Risks, New Challenges: Exploring Differences in Security Between Home Computer and Mobile Device Use.” *Behaviour & Information Technology*, doi:10.1080/0144929X.2017.1352028.

Meade, A. W., and S. B. Craig. 2012. “Identifying Careless Responses in Survey Data.” *Psychological Methods* 17 (3): 437–455.

Merchant, K., and W. A. Van Der Stede. 2007. *Management Control Systems*. 2nd ed. Harlow: Prentice Hall.

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

Nicholson, G., G. Kiel, and S. Kiel-Chisholm. 2011. “The Contribution of Social Norms to the Global Financial Crisis: A Systemic Actor Focused Model and Proposal for Regulatory Change.” *Corporate Governance: An International Review* 19 (5): 471–488.

Nunnally, J. C. 1978. *Psychometric Theory*. 2nd ed. New York: McGraw-Hill.

Ouchi, W. 1979. “A Conceptual Framework for the Design of Organizational Control Mechanisms.” *Management Science* 25 (9): 833–848.

Pahnila, S., M. Siponen, and A. Mahmood. 2007. "Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study." Paper presented at the 11th Pacific Asia Conference on Information Systems, Auckland, New Zealand, July 3–6, 2007.

Podsakoff, P. M., S. B. Mackenzie, J. Y. Lee, and N. P. Podsakoff. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies." *Journal of Applied Psychology* 88 (5): 879–903.

Porter, L. E., and T. Prenzler. 2016. "The Code of Silence and Ethical Perception." *Policing: An International Journal of Police Strategies & Management* 39 (2): 370–386.

PriceWaterhouseCoopers (PWC). 2014. *Global State of Information Security® Survey*.

Puhakainen, P., and M. Siponen. 2010. "Improving Employees" Compliance Through Information Systems Security Training: An Action Research Study." *MIS Quarterly* 34 (4): 757–778.

Rhee, H.-S., C. Kim, and Y. Ryu. 2009. "Self-efficacy in Information Security: Its Influence on End Users" Information Security Practice Behaviour." *Computers & Security* 28: 816–828.

Ringle, C. M., S. Wende, and J.-M. Becker. 2015. SmartPLS 3. Bönningstedt: SmartPLS. http://www.smartpls.com.

Safa, N., M. Sookhak, R. Von Solms, S. Furnell, N. Abdul Ghani, and T. Herawan. 2015. "Information Security Conscious Care Behaviour Formation in Organizations." *Computers & Security* 53: 65–78.

Siponen, M., A. Mahmood, and S. Pahnila. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study." *Information and Management* 51 (2): 217–224.

Siponen, M., S. Pahnila, and M. A. Mahmood. 2010. "Compliance with Information Security Policies: An Empirical Investigation." *Computer* 43 (2): 64–71.

Soomro, Z. A., M. H. Shah, and J. Ahmed. 2016. "Information Security Management Needs More Holistic Approach: A Literature Review." *International Journal of Information Management* 36 (2): 215–225.

Spector, P. E. 2006. "Method Variance in Organizational Research Truth or Urban Legend?" *Organizational Research Methods* 9 (2): 221–232.

Straub, D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study." *MIS Quarterly* 14 (1): 45–60.

Straub, D., and R. Welke. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making." *MIS Quarterly* 22 (4): 441–469.

Tsohou, A., M. Karyda, and S. Kokolakis. 2015. "Analyzing the Role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs." *Computers & Security* 52: 128–141.

Vance, A., M. Siponen, and S. Pahnila. 2012. "Motivating Information Security Compliance: Insights From Habit and Protection Motivation Theory." *Information & Management* 49 (3): 190–198.

Vinzi, V. E., L. Trinchera, and S. Amato. 2010. "PLS Path Modeling: From Foundations to Recent Developments and Open Issues for Model Assessment and Improvement." In *Handbook of Partial Least Squares*, edited by V. E. Vinzi, W. W. Chine, J. Hensler, and H. Wang, 47–82. Berlin: Springer.

Wang, H., A. S. Tsui, and K. R. Xin. 2011. "CEO Leadership Behaviors, Organizational Performance, and Employees' Attitudes." *The Leadership Quarterly* 22: 92–105.

Warkentin, M. E., A. C. Johnston, and J. Shropshire. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention." *European Journal of Information Systems* 20: 267–284.

Workman, M., W. H. Bommer, and D. Straub. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test." *Computers in Human Behavior* 24 (6): 2799–2816.

Workman, M., W. H. Bommer, and D. Straub. 2009. "The amplification effects of procedural justice on a threat control model of information systems security behaviours." *Behaviour & Information Technology* 28 (6): 563–575.

Appendix: Study Constructs and Measurement Items

Mediating/Dependent Variables

Construct	Items adapted from	Final Version of Items [All on Strongly disagree-Strongly agree 7-point scale with exception of attitude construct]
Attitude	Bulgurcu, Cavusoglu, and Benbasat (2010)	To me, securing information the way my organisation requires and/or expects me to is Unnecessary … Necessary Harmful … Beneficial Unimportant … Important Worthless … Valuable
Self-Efficacy	Bulgurcu, Cavusoglu, and Benbasat (2010) and Workman, Bommer, and Straub (2008)	I have the necessary skills to secure information the way my organisation requires and/or expects me to. I have the necessary knowledge to secure information the way my organisation requires and/or expects me to. I have the necessary competencies to secure information the way my organisation requires and/or expects me to. For me, securing information the way my organisation requires and/or expects me to is hard.
Norms	Bulgurcu, Cavusoglu, and Benbasat (2010)	My work-unit colleagues think I should secure information the way the organisation requires and/or expects me to. Senior management thinks I should secure information the way the organisation requires and/or expects me to. My direct manager thinks I should secure information the way the organisation requires and/or expects me to.

Independent Variables

In the following questions, information management refers to obtaining, handling, storing, exchanging and using information securely.

Specification	D'arcy, Hovav, and Galletta (2009), Boss et al. (2009) and Lee and Choi (2003)	My organisation has specific guidelines that describe how to manage information in the course of day-to-day duties. I am required to know a lot of existing written procedures to manage information There are many information management tasks and activities that are not covered by formal policies and procedures (reverse coded) Information management rules and procedures are typically written.
Monitoring and Evaluation	D'arcy, Hovav, and Galletta (2009) and Boss et al. (2009)	My organisation regularly monitors employee computing activities to see how well employees follow information management policies and procedures. Managers in my work area regularly evaluate the information management behaviour of employees. When it comes to information management, my organisation actively monitors the behaviour of employees. Managers in my work area formally evaluate the information management behaviour of employees. There are many information management tasks, activities and behaviours that are not monitored by the organisation (reverse coded). Managers in my work area assess whether employees follow information management policies and procedures. There are many information management behaviours that are not formally evaluated or assessed by Managers in my work area (reverse coded).
Rewards	Boss et al. (2009)	My pay raises and/or promotions depend on whether I manage information the way the organisation requires and/or expects me to. I will receive personal mention if I manage information the way the organisation requires and/or expects me to. I will be given rewards (monetary or non-monetary) for managing information the way the organisation requires and/or expects me to.
Sanctions	Bulgurcu, Cavusoglu, and Benbasat (2010)	I will probably be punished or demoted if I don't manage information the way the organisation requires and/or expects me to. I will receive personal reprimand if I don't manage information the way the organisation requires and/or expects me to. I will incur penalties (monetary or non-monetary) if I don't manage information the way the organisation requires and/or expects me to.
Senior Management Support	Knapp et al. (2006)	Senior management considers information management an important organisational priority. Senior management is interested in information management issues. Senior management's words and actions demonstrate that information management is a priority. Visible support for information management goals by senior management is obvious.