Peers matter: The moderating role of social influence on information security policy compliance

By: Adel Yazdanmehra, Jingguo Wang, and Zhiyong Yang

Abstract:

Information security in an organization largely depends on employee compliance with information security policy (ISP). Previous studies have mainly explored the effects of command-and-control and self-regulatory approaches on employee ISP compliance. However, how social influence at both individual and organizational levels impacts the effectiveness of these two approaches has not been adequately explored. This study proposes a social contingency model in which a rules-oriented ethical climate (employee perception of a rules-adherence environment) at the organizational level and susceptibility to interpersonal influence (employees observing common practices via peer interactions) at the individual level interact with both command-and-control and self-regulatory approaches to affect ISP compliance. Using employee survey data, we found that these two social influence factors weaken the effects of both command-and-control and self-regulatory approaches on ISP compliance. Theoretical and practical implications are also discussed.

Keywords: command-and-control approach | information security policy compliance | rules-oriented ethical climate | self-regulatory approach | susceptibility to interpersonal influence

Article:

1 INTRODUCTION

A primary strategy for addressing security threats to an organization's information resources is to adopt and enforce information security policies (ISPs). An ISP includes standards and procedures for and responsibilities of information resource users, with the goal of preventing noncompliance and thereby reducing information security incidents. To enforce an ISP, organizations often implement a variety of deterrence measures such as sanctions and monitoring (D'Arcy & Herath, 2011; D'Arcy, Hovav, & Galletta, 2009) and the effects of such measures on ISP compliance have drawn close attention in the literature (Warkentin & Willison, 2009). During the period between 1990 and 2004, deterrence theory was the single most cited topic in information security compliance literature (D'Arcy & Herath, 2011). In addition, studies have suggested that self-imposed sanctions such as those arising from personal values and moral beliefs are essential in predicting ISP compliance (Hsu, Shis, & Lowry, 2015; Nagin & Paternoster, 1993).

While deterrence can be viewed as external motivation for ISP compliance, researchers have also been interested in understanding the internal motivation of employees (Willison, Warkentin, & Johnston, 2018), especially the contentment arising from satisfactorily carrying out tasks (Ryan & Deci, 2000). Accordingly, recent studies have extended their scope of research to include not only deterrence but also such factors as personal self-sanctions, personal norms, personal ethics (Guo & Yuan, 2012; Li, Sarathy, Zhang, & Luo, 2014; Li, Zhang, & Sarathy, 2010; Yazdanmehr & Wang, 2016), moral beliefs (Cheng, Li, Li, Holm, & Zhai, 2013; D'Arcy & Devaraj, 2012; Hovav & D'Arcy, 2012; Hu, Xu, Dinev, & Ling, 2011; Ifinedo, 2014; Vance & Siponen, 2012), moral commitment (D'Arcy et al., 2009; Son & Park, 2016), shame and neutralization techniques (Silic, Barlow, & Back, 2017; Siponen & Vance, 2010), and self-regulatory approaches (Li et al., 2014; Son, 2011).

The basic premise of the literature cited above is that employee ISP compliance is instrumentally and/or normatively motivated (Tyler & Blader, 2005). More specifically, the instrumental view states that employees are rational self-interested actors (Becker, 1968) and a decision not to comply relies on weighing costs and gains (Paternoster & Simpson, 1996; Tyler & Blader, 2005). Therefore, organizations actively enforce rules to increase compliance by either (a) providing incentives to encourage compliance and/or sanctions to discourage noncompliance, or (b) implementing a surveillance mechanism (eg, computer monitoring) to enhance the chances of discovering noncompliance (Sutinen & Kuperan, 1999; Tyler, 1990; Tyler & Blader, 2005). This embodies the command-and-control approach.

In contrast to the instrumental view, the normative perspective argues that individuals are mostly concerned with fairness and equity and will usually behave based on self-monitoring, judgmental choice, and self-reactive influences (Bandura, 1986, 1991). Self-monitoring requires individuals to monitor their own behaviour and the associated underlying circumstances. Judgmental choice allows individuals to evaluate their behaviour against personal standards. Self-reactive influences may drive individuals to choose actions that generate positive self-reactions, such as self-respect and self-satisfaction (Bandura, 1991). Consequently, if compliance behavior is appropriate based on the parameters mentioned above, employees may consider it to be intrinsically desirable and feel personally obligated to abide by the rules (Tyler, 1990). This mindset reflects a self-regulatory approach in which the internal desire to comply is rooted in the perceived legitimacy of organizational rules and value congruence with organizational rules (Tyler & Blader, 2005).

When examining rule-following behaviour among employees, Tyler and Blader (2005) showed that both instrumental and normative motivations work together in shaping compliance with organizational policies. However, in the ISP context, there are mixed and even contradictory findings with respect to the effects of command-and-control and self-regulatory approaches (see Appendix C for an extensive review of the relevant literature). A handful of studies support the influence of the command-and-control approach—mostly via the threat of sanctions (Chen, Ramamurthy, & Wen, 2012; D'Arcy & Devaraj, 2012; Johnston, Warkentin, McBride, & Carter, 2016; Li, & Luo, X. (Robert), Zhang, J.,, & Sarathy, R., 2018; Siponen, Pahnila, & Mahmood, 2010), whereas others have indicated that deterrence has no effect (Guo & Yuan, 2012; Hu et al., 2011; Li et al., 2010; Moody, Siponen, & Pahnila, 2018; Silic et al., 2017; Siponen & Vance, 2010; Son, 2011; Vance & Siponen, 2012).

With respect to the self-regulatory approach, although some studies have shown the effectiveness of intrinsic motives on ISP compliance (Guo & Yuan, 2012; Li et al., 2014, 2010; Son, 2011; Yazdanmehr & Wang, 2016), others have called those findings into question (Alzahrani, Johnson, & Altamimi, 2018; Moody et al., 2018; Silic et al., 2017; Son & Park, 2016). To reconcile these mixed results, there have been calls to investigate the boundary conditions reflected by contextual and dispositional factors, as presented in the Literature Review section of this paper (Chen, Wu, Chen, & Teng, 2018; Clarke & Cornish, 1985; D'Arcy & Herath, 2011; Johnston et al., 2016; Paternoster, 1987).

In this study, we contest the assertation that social influence may set up boundaries for the effect of command-and-control and self-regulatory approaches on employee ISP compliance. Prior studies have suggested that the effect of social influence on compliance is determined by individual perception of what peers think about compliance and the extent to which an individual is open to social influence (Akers, Krohn, Lanza-Kaduce, & Radosevich, 1979; Sutinen & Kuperan, 1999). This implies that both (a) the work environment, represented by employees' common perceptions, norms, and behaviours in terms of compliance, and (b) employee propensity to seek and observe others' compliance behaviours can serve as critical boundary conditions on the effectiveness of command-and-control and self-regulatory approaches. Notably, the effects we propose are generally consistent with the information security and criminology literature in terms of their emphasis on investigating the boundary-related role of contextual and dispositional factors (Chen, Wu, et al., 2018; Clarke & Cornish, 1985; D'Arcy & Herath, 2011; Johnston et al., 2016; Paternoster, 1987).

In extending the framework of Tyler and Blader (2005), we propose a social contingency model that investigates the moderating roles of both individual- and organizational-level social influence on how command-and-control and self-regulatory approaches affect ISP compliance. From the standpoint of the command-and-control approach, employees act upon the premise that ISP violations are likely to be detected and punished. Through workplace socialization, they learn about organizational processes and rules (Trevino, 1992; Wenzel, 2004). The pressure of social influence may lead them to reconsider earlier perceptions of the likelihood of detection and the severity of sanctions, thus reducing the impact of such perceptions with respect to ISP violations (Workman & Gathegi, 2007).

From the perspective of the self-regulatory approach, the key elements in shaping an intrinsic desire to comply are individual perceptions of rule legitimacy and appropriateness, but these elements could be altered through socialization as organizational values become internalized and thereby reshape employees' personal values, ultimately leading to changed behaviour (Li et al., 2014; Wenzel, 2004; Yazdanmehr & Wang, 2016). By investigating the moderating effects of social influence, this study provides a new framework for reconcil inconsistencies related to the effects of command-and-control and self-regulatory approaches on employee ISP compliance indicated earlier.

Social influence can be observed whenever an individual changes their behaviour in response to cues from behaviour of others (Kelman, 1974), and in a company, it may be manifested at both individual and organizational levels (Hitt et al, 2007). Because organizational phenomena are complicated and multi-level, this study investigates social influence at both individual (e.g., personal traits) and organizational (e.g., organizational culture or norms) levels (Hitt et al, 2007). At the organizational level, we argue that a *rules-oriented ethical climate* signals that compliance with company rules and procedures is an expected, ethical behaviour. A rules-oriented ethical climate creates a powerful normative system that informs employees about common practices and priorities of the firm when facing ethical dilemmas (Barnett & Vaicys, 2000; Brass, Butterfield, & Skaggs, 1998; Gaertner, 1991; Victor & Cullen, 1988). At the individual level, we argue that *susceptibility to interpersonal influence*, reflecting the degree to which employees are receptive to interpersonal influences (Bearden, Netemeyer, & Teel, 1989), may modify the effects of command-and-control and self-regulatory approaches on ISP compliance.

In summary, the main objective of this study is to investigate the role of social influence at both individual and organizational levels on the efficacy of command-and-control and self-regulatory approaches to ISP compliance. This investigation can advance the understanding of why the command-and-control and/or self-regulatory approaches effectively promote ISP compliance in some situations but not in others. We theorize that both a rules-oriented ethical climate and susceptibility to interpersonal influence weaken the effects of command-and-control and self-regulatory approaches on ISP compliance. To the best of our knowledge, this study is among the first to examine the relative effectiveness of command-and-control and self-regulatory approaches from a social influence standpoint and to provide a deeper understanding of the phenomenon. From a practical perspective, our findings provide useful insights to managers the relative effectiveness of an organizational climate or designing an office layout to enhance ISP compliance.

2 LITERATURE REVIEW

In this section, we review relevant studies and discuss prior findings. Appendix C presents a more elaborate discussion of the mixed results related to the effect of command-and-control and self-regulatory approaches.

2.1 Command-and-control approach

The command-and-control approach comprises extrinsic enforcement of the rules through incentives and sanctions as well as implementation of detection mechanisms to ensure discovery of wrongdoing (Tyler, 2009). From an organizational perspective, this approach is meant to inform potential wrongdoers about: (a) the high probability that noncompliance will be detected (ie, detection of behaviour) and (b) potential punishment (ie, reaction to behaviour) that should outweigh possible benefits of noncompliance (Geerken & Gove, 1975). The command-and-control approach, often under the umbrella of general deterrence theory, has traditionally served as the primary strategy for investigating employee rule-following in the context of ISP compliance (D'Arcy & Herath, 2011; Son, 2011).

In practice, most organizations rely on sanctions to promote ISP compliance and rarely implement reward policies (D'Arcy et al., 2009; Herath & Rao, 2009b, Herath & Rao, 2009a; Li, & Luo, X. (Robert), Zhang, J.,, & Sarathy, R., 2018; Siponen & Vance, 2010; Straub, 1990). Therefore, a combination of organizational detection (often described in terms of sanctions certainty, detection probability, deterrent certainty, certainty of control, and computer monitoring) and reaction (often described in terms of perceived severity, sanction severity, deterrent severity, punishment severity, organizational sanctions, and severity of penalty) to ISP violations is often viewed as providing the main determinants of compliance behaviour (see Table C.1 in Appendix C for the complete list of the determinants). However, as discussed in detail in Appendix C, previous studies of the command-and-control approach have yielded mixed results (cf, Cram, D'Arcy, & Proudfoot, 2019 ; D'Arcy & Herath, 2011; Willison, Lowry, & Paternoster, 2018).

Some studies have suggested that moderating variables may explain the mixed results (Chen, Wu, et al., 2018; D'Arcy & Herath, 2011; Jacobs, 2010; Pogarsky, 2002), so in a consolidation effort Chen, Wu, et al. (2018) investigated the moderating roles of perceived self-efficacy, descriptive norms, and response cost on the relationship between deterrence and employee ISP compliance intention, and found that those variables did not moderate the relationship. Li, and Luo, X. (Robert), Zhang, J.,, and Sarathy, R. (2018) also tested the moderating effects of procedural justice and self-control on the relationships between perceived deterrence and benefits and Internet use policy (IUP) compliance intention, and again found that none of these variables significantly moderated the relationship. Moreover, Johnston et al. (2016) examined the moderating role of stability and plasticity meta-traits on the effectiveness of deterrence on ISP violation intentions. They found that employees with a higher stability meta-trait than average meta-trait were more sensitive to deterrence, whereas the moderating effects of plasticity were found to be rather mixed. Hovav and D'Arcy (2012) also examined the role of cultural differences with respect to effectiveness of deterrence in reducing information systems (IS) misuse intention and found patterns for South Korean employees to be opposite from those of United States employees. By extending this stream of research, we argue that the command-and-control approach is a social phenomenon whose effectiveness is sensitive to social influence.

2.2 Self-regulatory approach

The self-regulatory approach treats intrinsic desires as primary drivers of behaviour, with the intrinsic desire for compliance rooted in two types of employee perceptions: (a) value congruence, the extent to which the values of the organization are consistent with those of the employee, and (b) legitimacy, the extent to which the organization is led by legitimate authorities and structured around legitimate rules (Tyler, 1990; Tyler & Blader, 2005). High value congruence motivates compliance because individuals are able to remain in alignment with their personal values while working for the organization (Kranz & Haeussinger, 2014; Malhotra, Galletta, & Kirsch, 2008; Robinson & Darley, 1995). With respect to legitimacy, an individual will be more likely to be ISP-compliant when they perceive their superiors and organization policies to be legitimate (Tyler, 2006). Notably, while value congruence and legitimacy are correlated, they are distinct elements, each capturing a unique part of the self-regulatory approach (Tyler, 2006).

Previous literature has investigated the effect of other intrinsic mechanisms such as personal norms, moral beliefs, moral commitments—employee evaluation of the degree to which ISPviolations are morally acceptable and justifiable (D'Arcy et al., 2009), and shame—personal feelings of guilt or embarrassmentfollowing discovery by others of one's socially unacceptable actions (Paternoster & Simpson, 1996)—on employee ISP compliance (Hsu et al., 2015; Nagin & Paternoster, 1993; Siponen & Vance, 2010; Yazdanmehr & Wang, 2016). These concepts theoretically share some basic elements with the self-regulatory approach in that they are all associated with the roles of self-imposed punishments and rewards in driving employee compliance (Guo & Yuan, 2012).

The concept of the self-regulatory approach, however, is broader and more inclusive. For example, moral beliefs and personal norms, which refer to an individual's commitment to personal values (Vance & Siponen, 2010; Yazdanmehr & Wang, 2016), are similar to the “value congruence” component, the difference being that the value congruence implies that personal norms are congruent with organizational values. It should also be noted that perception of ISP characteristics can affect employee ISP compliance (Cram, Proudfoot, & D'Arcy, 2017), with employees more likely to follow organizational policies when they perceive them to be legitimate (Bijlsma-Frankema & Costa, 2010). This notion is captured by the legitimacy component of self-regulatory approach in this study. In addition, legitimacy has been viewed as closely related to moral commitment (Son, 2011).

Although in most cases intrinsic motives have been shown to affect ISP compliance, some studies have reported contradictory results. For example, Son (2011) showed that the effects of self-regulatory approach (as manifested by perceived value congruence and legitimacy) on ISP compliance are significant, whereas Alzahrani et al. (2018) found no such significant relationship between these two constructs and ISP compliance. Additionally, when examining the impact of moral commitment on ISP compliance, D'Arcy et al. (2009) discovered significant effects whereas Son and Park (2016) did not, focusing on the relationship between shame and ISP compliance, 2010Silic et al. (2017) reported only limited support for existence of the relationship, whereas Siponen and Vance (2010) stated that these two constructs are unrelated (please refer to Appendix C for more detail).

Although no research has examined potential moderators that might explain such mixed results, previous studies have investigated how contextual and dispositional factors may moderate the effect of intrinsic motives on ISP compliance behavior. Harrington (1996), for example, reported that denial of (personal)responsibility moderates the effect of IS codes of ethics on deterring computer abuse intention. More recently, Yazdanmehr and Wang (2016) showed that ascription of personal responsibility reinforces the impact of personal norms on ISP compliance. Intrinsic motives have also been examined in the form of moral disengagement[2] that reflects an employee's attempt to disengage from internal self-sanctions that guide their ISP compliance behavior (D'Arcy, Herath, & Shoss, 2014). The effect of this construct has been found susceptible to contextual (e.g., situational pressures,ethical climate) and dispositional (e.g., overpowered integrity) factors (Bandura, 1999; Batson & Thompson, 2001; Chen, Chau, & Li, 2018; Moore, Detert, Trevino, Baker, & Mayer, 2012).

3 THEORETICAL BACKGROUND

3.1 Rule compliance as a social phenomenon

As discussed earlier, in studying compliance behaviour in general, researchers have often examined the effectiveness of command-and-control and self-regulatory approaches rooted in instrumental and normative perspectives, respectively (Tyler, 1990). Simply put, the command-and-control approach holds that individuals are mainly motivated by self-interest and will respond to swift, tangible rewards and punishments associated with a particular act (Tyler, 1990). Organizations reflecting this perspective use external deterrent forces (eg, monitoring and sanctions) to influence employee perception of ISP noncompliance detection and reaction as a means to promote ISP compliance. In contrast, the self-regulatory approach maintains that employees are driven primarily by factors they consider to be legitimate and consistent with their personal values. It argues that individuals comply with rules to the degree that they perceive the rules to be acceptable (ie, legitimate) and consistent with their personal values (Sutinen & Kuperan, 1999; Tyler, 1990).

Rule compliance (with the ISP) can be considered to be a social phenomenon (Sutherland, Cressey, & Luckenbill, 1992; Tyler, 1990) because the perception of the rules-adherence environment and observed common practices among colleagues may affect employees' behaviour. In fact, individual behaviours are driven not just by isolated factors such as inner desires, but also by continuous interactions among cognitive, behavioural, and environmental determinants (Bandura, 1977, p. 11). To illustrate this idea, Latham and Saari (1979) stated:

> To show that behavior is determined only by cognitions, one would have to find a control group consisting of subjects who cannot think. Similarly, to prove empirical support for the argument that behavior is due to environmental consequences alone, one would have the impossible task of forming a control group for which there was no environment (p. 240).

As an antecedent of rule compliance behaviour, the impact of the command-and-control approach is a result of an employee's personal cost-benefit analysis (Becker, 1968) that may depend on how clearly organizations communicate the consequences of ISP violations (ie, the odds of detection and punishment severity). However, the mixed results regarding the efficacy of this approach suggest that other perceptual processes such as social influence must be in place (Williams & Hawkins, 1986). Accordingly, previous research suggests that through socialization, employees will develop a better understanding of the rules and procedures (Trevino, 1992; Wenzel, 2004) and may subsequently change their perceptions with respect to detection of and sanctions for violations. The effects of command-and-control approach may be modified (Williams & Hawkins, 1986; Workman & Gathegi, 2007). However, when an organization lacks commonly-accepted norms for rules and procedures or if its employees are not willing to seek others' opinions, there will most likely be no opportunity for them to process social cues. In other words, in the absence of any social influence, since employees cannot rely on social cues to make sense of the command-and-control approach and its implications, they tend to take sanctions and detections mechanism more seriously.

The success of self-regulatory approach is a function of an employee's intrinsic desire to comply with the ISP, which is rooted in a positive perception of value congruence and legitimacy of the rules. Therefore, any inconsistency may lead to resistance to the policies rather than compliance (Tyler, 1990). Organizational social norms can also partly shape employee values through socialization, using a process called internalization (Cialdini & Trost, 1998; Wenzel, 2004; Yazdanmehr & Wang, 2016). In other words, organizational social norms through an internalization process may alter the normative perception of the morality of compliance or noncompliance. Accordingly, employees are more likely to comply with rules if they believe in the legitimacy of the authorities who established them (Tyler, Callahan, & Frost, 2007). Notably, value congruence with and legitimacy of the rules may be increased or decreased through socialization—the linkage between employees and organization (Tyler & Blader, 2005). As a result, social influence can alter the effectiveness of self-regulatory approach by signalling to employees the acceptability of the rules and prompting them to revisit their views in terms of legitimacy of the rules and the authorities making them. The idea that employees often seek and observe cues about appropriate behaviour at work supports existence of social influence's moderating effect (Trevino, 1986).

Social influence in an organization is a broad concept and can be narrowed down to individual and organizational level (Hitt et al, 2007). At the organizational level, social influence manifests within an implicitly strong and definite climate, often referred to as a rules-oriented ethical climate (Victor & Cullen, 1988). Although the impact of social influence on employee ethical behaviour has been documented in the literature, little is known about its moderating role in the context of ISP compliance. Thus, this study explores a novel perspective to examine how a rules-oriented ethical climate might moderate the effects of command-and-control and self-regulatory approaches on ISP compliance.

At the individual level, social influence manifests through peer interactions during which employees witness acceptable and expected viewpoints, reasons for an actions, and logical consequences of expected behaviours. In fact, behavioural changes are often viewed as an outcomes of interactions in which individuals are perceived to be similar, eligible, or experts (Rashotte, 2007). Social interactions can also direct individual attention toward a particular social cue and cause a behaviour become more pronounced (Salancik & Pfeffer, 1978). Given these ideas, an individual's susceptibility to interpersonal influence denotes both a tendency to look to peers for identification of appropriate behaviours and a willingness to conform to peer expectations in terms of appropriate behaviour (cf, Bearden et al., 1989).

3.2 Rules-oriented ethical climate

In general, ethical climate refers to the shared perception of what is ethically appropriate and how ethical issues should be handled (Victor & Cullen, 1988). By providing standards, normative structures, policies, and routines, it communicates an organization's priorities on solutions to ethical dilemmas (Wyld & Jones, 1997). In an ethical climate, individuals have certain forms of experiences and relationships that may eventually affect their ethical judgement, including what constitutes an ethical issue, the gravity of an issue, and how to react (Ferrell & Gresham, 1985; Hunt & Vitell, 1986; Sutherland, Cressey, & Luckenbill, 1992; Trevino, 1986).

In a high level of ethical climate, employees are exposed to peers with consistent expectations about the most appropriate (ie, ethical) behaviours (Mischel, 1977), resulting in the formation of clear ethical judgments (Shin, 2012). Conversely, in a low level of ethical climate, employees are exposed to peers who may have inconsistent views regarding ethical behaviours, resulting in uncertainty in ethical judgment (Shin, 2012). One may thus expect a strong ethical climate to help employees make clear ethical judgments (Banerjee, Cronan, & Jones, 1998; Trevino, 1986). In particular, this may be important when they face an ethical dilemma wherein a conflict arises between an individual's own interests and collective rationality (eg, following a rules-oriented ethical climate) (Kahan, 1974; Pillutla & Chen, 1999).

Whether an ethical climate is uni- or multi-dimensional is debatable. In this study we mirror the many scholars who consider it to be multi-dimensional. Victor et al (1988) provide the most well-established classification, based on Kohlberg's (1981) moral development theory and Gouldner's (1957) moral philosophy. According to their typology, an ethical climate is comprised of two dimensions, namely ethical approach and ethical referent. An ethical referent, also known as an ethical criterion, has three subcategories: principle, benevolence, or egoism. The principle ethical criterion refers to consideration of the application and interpretation of the rules, whereas benevolence and egoism ethical criteria consider the well-being of others and individual self-interest, respectively (Victor & Cullen, 1988). An ethical referent, also called the locus of analysis, focuses on the individual, local, or cosmopolitan level. The individual level emphasizes the self as the prime referent (Victor & Cullen, 1988), whereas the local level stresses the immediate social context surrounding the individual (eg, organizational practices), and the cosmopolitan level extends beyond the immediate organization or group (eg, professional codes). Applying these criteria, Victor et al (1988) empirically classified ethical climate into five types: rules (company policies and procedures adherence), law and code (violation of laws), caring (welfare of others), instrumental (self-interest), and independence (personal beliefs adherence).

A rules-oriented ethical climate focuses on a company's policy and procedure adherence (Victor & Cullen, 1988). It can serve as a psychological tool for organizational-level social influence because (a) it is based on the ethical criterion of principle and the local locus of analysis (Victor & Cullen, 1988), the focus of this study; (b) it offers the best framework for demonstrating accepted and expected behaviours related to established rules and policies (ie, information security policies) (Chan, Woon, & Kankanhalli, 2005; Schneider, 1975; Victor & Cullen, 1988; Zhang, Luo, Liao, & Peng, 2015); and (c) it captures employee perception of organizational policies, code of ethics, and top management actions regarding ethics (Jaramillo, Mulki, & Solomon, 2006) typical of a unidimensional ethical climate (Shin, 2012).

It is noteworthy to mention that a rules-oriented ethical climate differs from the self-regulatory approach since it refers to employee perception of accepted behaviours regarding organizational rules (Victor & Cullen, 1988) rather than the self-regulatory concept that refers to an individual's intrinsic desire and inborn preference to follow the rules (Tyler & Blader, 2005). This intrinsic desire is conceptualized as acting independently of environmental contingencies (Tyler & Blader, 2005), whereas a rules-oriented ethical climate is a function of an organizational environment.

A strong rules-oriented ethical climate may lead to employees judging rule compliance as-- more of an ethics issue (ie, ethical decision frame). The absence of such a climate may lead to ambiguous understanding about whether compliance is an ethical matter and thus directs an employee's attention to the risks and punishments/rewards associated with rule compliance, or its legitimacy and value congruence (Tenbrunsel & Messick, 1999). Thus, the presence of an informational cue about the degree to which organization members follow the rules (eg, rules-oriented ethical climate) is likely to diminish the impact of other sources of reasoning (eg, the command-and-control and self-regulatory approaches) (cf, Tenbrunsel and Messick 1999).

3.3 Susceptibility to interpersonal influence

Interpersonal sources of influence refer to non-organizational personal contacts from which employees may consider obtaining information related to an issue at hand (Bearden et al., 1989; Mourali, Laroche, & Pons, 2005; Yang, Wang, & Mourali, 2015). Such sources may be peers with whom an individual interacts face-to-face and/or others with whom an employee would like to be associated, (eg, reference group) (Bearden et al., 1989). This study classifies susceptibility to interpersonal influence as a representation of social influence at the individual level because it most closely resembles an employee's tendency to seek information from and emulate norms of peers.

The main distinction between interpersonal influence and other sources of influence (eg, the command-and-control or self-regulatory approaches) is that during interpersonal exchanges, communicators have an opportunity to receive clarification and instant feedback (Mourali, Laroche, & Pons, 2005). Such a feature makes interpersonal communications an appealing source in the decision-making process. As such, employee tendency to be influenced by such an interpersonal source could play a significant role in modifying the impact of other sources of influence on their behaviour. In this study, we show that susceptibility to interpersonal influence diminishes the effects of command-and-control and self-regulatory approaches on ISP compliance.

Susceptibility to interpersonal influence has two dimensions, susceptibility to informational influence and susceptibility to normative influence (Bearden et al., 1989). Although they are distinct, each describes a specific phenomenon related to an individual's tendency to be influenced by others. The first dimension reflects an individual's tendency to seek out and accept information from others as a valid indication of reality. It may occur when an individual is actively requesting information from other knowledgeable people or when an individual makes an assumption based on observing the behaviour of others (Park & Lessig, 1977). The second dimension reflects an individual's tendency to observe and conform to expectations of others. It occurs when an individual attempts to identify with a reference group to enhance their own image in the eyes of others perceived as important (Bearden & Etzel, 1982; Kelman, 1961; Park & Lessig, 1977). This may also occur when an individual conforms to others' expectations and norms to gain rewards or avoid punishments (ie, utilitarian influence) (Bearden & Etzel, 1982; Burnkrant & Cousineau, 1975; Park & Lessig, 1977).

In the context of this study, susceptibility to interpersonal influence might take place when an employee tries to learn more about ISP compliance by seeking information from peers and/or when an employee conforms to others' expectations of compliance. Informational influence may be associated with behaviours such as talking to peers, asking for their advice, and sending inquiries to information security professionals. Normative influence may be linked to such behaviours as mirroring the behaviours of someone admire or seeking compliance-related approval from individuals perceived as important.

It should be noted that susceptibility to interpersonal influence differs from subjective norms or normative beliefs. Subjective norms refer to employee perception of what others of importance think they should do (Cialdini & Trost, 1998; Herath & Rao, 2009b; Yazdanmehr & Wang, 2016). However, susceptibility to interpersonal influence is measured by the frequency at which employees actively observe others' behaviour or seek information from others (Bearden et al., 1989). It can be asserted that susceptibility to interpersonal influence is an individual's tendency to be receptive of their peers' opinions (eg, subjective norms), one way to understand the difference between susceptibility to interpersonal influence and subjective norms. Previous research indicates that susceptibility to interpersonal influence is a key factor in shaping attitudes, norms, values, and aspirations in the context of smoking and drinking (Yang, Schaninger, & Laroche, 2013) as well as music piracy (Yang, Wang, & Mourali, 2015), and other fields. However, its role as a moderator in general and its interplay with command-and-control or self-regulatory approaches in particular has not yet been investigated.

4 HYPOTHESIS DEVELOPMENT

4.1 Effects of the command-and-control and self-regulatory approaches on ISP compliance

Previous research (Becker, 1968; Cornish & Clarke, 1986; Paternoster & Simpson, 1996) posited that employees are rational self-interested actors and engage in either ISP compliance or noncompliance to maximize benefits to themselves (Becker, 1968). In accordance with this view, an employee compliance decision is a function of perceived costs and gains (Becker, 1968; Cornish & Clarke, 1986; Paternoster & Simpson, 1996), so since the command-and-control approach involves implementation of detection systems and punishment following ISP noncompliance, we expect it to positively affect ISP compliance. For example, if a company is strict (eg, strong monitoring system along with severe punishments), employees (as rational self-interested actors) may consider the costs of ISP noncompliance to outweigh any benefits and thus comply with the ISP. Accordingly, we hypothesize:

> ***H1.*** The command-and-control approach is positively associated with employee ISP compliance.

We also expect the self-regulatory approach to be positively related to ISP compliance because it taps into employees' intrinsic desires to follow the ISP by activating feeling of personal responsibility to align their behaviour with organizational rules (Tyler, 2005). When employees perceive an organizational ISP to be legitimate, they are more likely to consider it as a legitimate policy and as a result follow it. Congruence between an employee's values (sense of right and wrong) and the organizational ISP can also enhance and endorse such values, thereby motivating ISP compliance, because employees tend to behave consistently with their values (Tyler & Blader, 2005). Consistent with this reasoning, Myyry, Siponen, Pahnila, Vartiainen, and Vance (2009) found that employee moral reasoning and values are key drivers of ISP compliance. Similarly, Yazdanmehr and Wang (2016) showed that personal norms regarding ISP lead to better ISP compliance. Moreover, Li et al. (2014) found in the context of Internet use that the self-regulatory approach is more effective than the command-and-control approach in promoting compliance with an Internet use policy. Similarly, Son (2011) reported that perceived legitimacy and value congruence contribute significantly to ISP compliance. Accordingly, we hypothesize:

> ***H2.*** The self-regulatory approach is positively associated with employee ISP compliance.

4.2 The moderating role of rules-oriented ethical climate

A rules-oriented ethical climate provides situational cues prompting an employee to understand that adherence to organizational policies is ethical (Messick, 1999; Shin, 2012). In an organization with a strong rules-oriented ethical climate, employees who engage in ISP decision-making have a clear understanding of what constitutes an ethical or unethical ISP-related behaviour (Shin, 2012). Such employees are more likely to base their ISP-related decisions on ethical considerations (ie, the ethical decision frame) (Tenbrunsel & Messick, 1999). Conversely, in an organization with a weak rules-oriented ethical climate, employees may not have a clear understanding of whether or not adhering to organizational policies is ethical (Shin, 2012). Therefore, they are more likely to rely on command-and-control and/or self-regulatory approaches as alternatives to ethical climate in their ISP decision-making.

Given that a rules-oriented ethical climate can play an important role in forming employee ISP-related decisions (Barnett & Schubert, 2002; Kramer & Messick, 1996), we argue that, in an organization with a strong rules-oriented ethical climate, employees deciding whether or not to comply with the ISP are generally expected to find solutions using environmental cues from such a climate (Barnett & Schubert, 2002; Kramer & Messick, 1996). This could weaken other drivers (ie, the command-and-control and self-regulatory approaches) affecting employee choices. Accordingly, we hypothesize:

> ***H3.*** A rules-oriented ethical climate negatively moderates the effect of command-and-control approach on ISP compliance, in such a way that the effect is less pronounced when an organization's rules-oriented ethical climate is high than low.

> ***H4.*** A rules-oriented ethical climate negatively moderates the effect of self-regulatory approach on ISP compliance, in such a way that the effect is less pronounced when an organization's rules-oriented ethical climate is high than low.

4.3 The moderating role of susceptibility to interpersonal influence

Employees with discernible levels of susceptibility to interpersonal influence may display different levels of responsiveness to the command-and-control approach. Relative to individuals with low levels of susceptibility to interpersonal influence, those with high levels tend to make decisions based on the information collected from others, mainly because of their desire to be accepted by others (Bonabeau, 2004), the desire to gain reputational benefits (Kuran, 1997; Sunstein, 1996) or the desire to project a positive self-image (Wrong, 1961). Moreover, mimicking the behaviours of important others helps people discount the perceived risk of ISP noncompliance (Wang, Yang, & Bhattacharjee, 2011). We expect that those with high susceptibility to interpersonal influence may emulate their peers and discount the effect of organizational sanction-based threats. They are probably more likely to view such behaviour as acceptable or believe that adopting it may enhance their self-image or social status. Thus, the command-and-control approach has less impact on employee ISP compliance for those with higher levels of susceptibility to interpersonal influence. Accordingly, we hypothesize:

> ***H5.*** Susceptibility to interpersonal influence negatively moderates the effect of command-and-control approach on ISP compliance in such a way that the effect is less pronounced when susceptibility to interpersonal influence is high than low.

Similarly, susceptibility to interpersonal influence can also undermine the impact of self-regulatory approach on ISP compliance. Those with a high level of susceptibility may regard making decisions based on one's inner feelings or beliefs as immature or selfish and as a result they often encouraged to sacrifice personal goals to maintain good relationships with others (Yang & Laroche, 2011). In contrast, employees with a low level of such susceptibility feel they have the autonomy to ignore social influence constraints (Mourali & Yang, 2013) and make decisions based on their own internal attitudes and thoughts without taking into account those of others (Yang, Wang, & Mourali, 2015). Translating these findings into our study context, it is expected that employees less susceptible to interpersonal influence would follow their own internal repertoire of values and assumptions (the self-regulatory approach) regarding ISP compliance, thereby resulting in a stronger impact of the self-regulatory approach on ISP compliance behaviour. Accordingly, we hypothesize:

> ***H6.*** Susceptibility to interpersonal influence negatively moderates the effect of self-regulatory approach on ISP compliance in such a way that the effect is less pronounced when susceptibility to interpersonal influence is high than low.

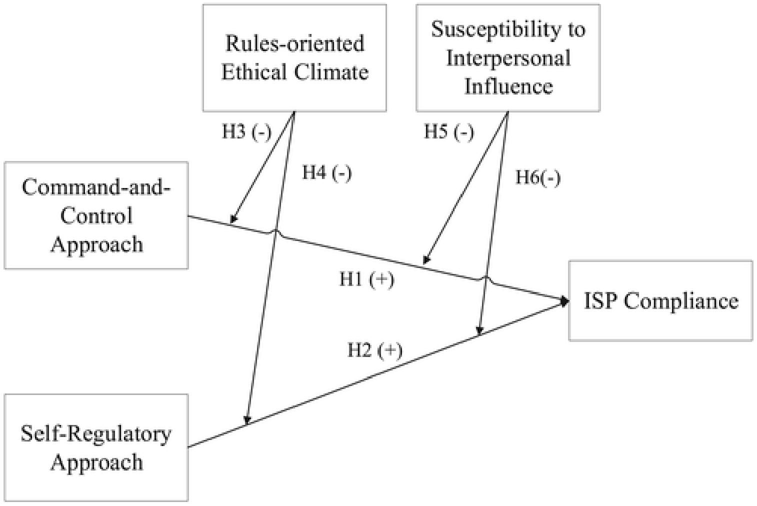

Rules-oriented Ethical Climate
Susceptibility to Interpersonal Influence
H3 (-)
H4 (-)
H5 (-)
H6(-)
Command-and-Control Approach
H1 (+)
ISP Compliance
H2 (+)
Self-Regulatory Approach

Figure 1. A social contingency model of ISP compliance

In this study, we propose a social contingency model of ISP compliance shown in Figure 1.

5 RESEARCH METHOD AND RESULTS

5.1 Data collection

We collected data from employees recruited through Amazon Mechanical Turk (or MTurk). MTurk is an online crowdsourcing labour market that provides a platform through which one can assign workers to do diverse tasks in exchange for payment adjusted to the quality of the finished task. Studies in the information systems literature (e.g., Steelman, Hammer, & Limayen, 2014, and Lowry, D'Arcy, Hammer, & Moody, 2016) have endorsed the reliability and validity of the results obtained via MTurk survey participants. We followed Steelman, Hammer, and Limayen's (2014) and Lowry, D'Arcy, Hammer, & Moody's (2016) guidelines in our data collection. To ensure targeting the correct respondents, we placed screening questions at the beginning of the survey and asked participants to indicate whether they were employed either part- or full-time at the time of completing the survey. For those who were full-time employees, we provided a brief explanation and illustrative examples of what constitutes information security policy. We filtered out participants whose organization either had no ISP in place or whose job did not require ISP compliance. The sample was restricted to United States residents. There were a total of 246 valid participants comprised of 124 men (50.4%) and 122 women (49.6%); 217 had full-time jobs (88.2%), while 29 had part-time jobs (11.8%), the average participant age was 39 (see Table A1 in Appendix A for more detailed demographic characteristics).

5.2 Measures

Pre-existing instruments from prior studies were adapted to our study. All the key constructs in the model were measured using multiple items. Consistent with the discussion in the theoretical background section, the command-and-control approach, the self-regulatory approach, and susceptibility to interpersonal influence were taken conceptually as second-order formative constructs, with all the first-order constructs measured in a reflective manner. Specifically, the self-regulatory approach construct has two dimensions, legitimacy and value congruence, and related measurement items were adapted from Tyler and Blader (2005). The command-and-control approach construct has two dimensions, detection and reaction to behaviour, and related items were also adapted from Tyler and Blader (2005).

The items for two dimensions of susceptibility to interpersonal influence are susceptibility to informational influence and susceptibility to normative influence, were adapted from Bearden et al. (1989). A rules-oriented ethical climate was assessed using Victor et al's (1988) scale. All items used a 7-point Likert scale. The measurement of ISP compliance behaviour was derived from Tyler and Blader (2005) and reworded to fit the ISP context.

Experienced IS faculty members (other than the authors) and PhD students with experience in survey-based research were asked to examine the measurement items to confirm their clarity. One hundred MBA students from a major university in the southwest United States carried out a pilot study, and appropriate modifications of the survey instruments were made consistent with the pilot study (see Table A2 in Appendix A for the final set of items).

6 DATA ANALYSIS AND RESULTS

We used structural equation modelling to test our model. To validate measurement scales and test the proposed model, a component-based partial least squares (PLS) approach was chosen because, unlike covariance-based approaches such as LISREL, PLS does not suffer from identification issues or non-normal distributed data (see Appendix E for further discussion on variables distribution) (Fornell & Bookstein, 1982).

6.1 Measurement validation

The Smart-PLS (version 3.2.6) software package (Ringle, Wende, & Becker, 2015) was used for analysis, and a bootstrapping procedure with 5000 resamples was used to estimate the path coefficient weights and their significance. Before testing the hypotheses, we examined the convergent validity, individual item reliability, composite reliability, and discriminant validity, to ensure the measurement quality of all principle constructs.

We calculated factor and cross-loadings (see Table A3 in Appendix A), average variance extracted (AVE) values, composite reliability, and Cronbach α for each construct (see Table A4 in Appendix A). The AVE values for all constructs were greater than the recommended minimum of 0.50, indicating that the items satisfied the convergent validity. The square root of each construct's AVE was higher than the construct's correlations, and all the other constructs and factor loadings for each item were higher than its cross-loadings on other constructs (at least 0.10). These results indicate satisfaction of discriminant validity (Hair, Black, Babin, & Anderson, 2009).

Composite reliability (Fornell & Larcker, 1981) and Cronbach α scores were calculated to confirm the scale reliability and internal consistency of the constructs. Composite reliability and Cronbach α values of .70 are recommended cut-offs (Gefen, Straub, & Boudreau, 2000; Nunnally & Bernstein, 1994), and both such values of all constructs were greater than.70 (see

Table A4 in Appendix A), suggesting that they all achieved acceptable reliability scores (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003).

Using the repeated indicators method (Chin, Marcolin, & Newsted, 2003; Lohmöller, 1989; Wold, 1982), we estimated the second-order formative variables of the command-and-control, the self-regulatory approach, and susceptibility to interpersonal influence. First, following a molecular approximation, we constructed first-order latent constructs and related them to their corresponding items. We then formed the second-order constructs by the repeated use of the manifest variables of the first-order latent constructs. The paths between the first- and the second-order constructs represent second-order loadings (see Table A5 in Appendix A for the loadings, composite reliability scores, and AVEs for the second-order constructs).

Given that multicollinearity may be a problem for measures of formative constructs (Jarvis, MacKenzie, & Podsakoff, 2003). It is suggested that formative measures should not have strong correlations, because high multicollinearity can destabilize the construct, and high correlations suggest that multiple measures may be tapping into a given dimension of the construct (Jarvis, MacKenzie, & Podsakoff, 2003; Petter, Straub, & Rai, 2007). In this study, since all VIFs are lower than the conservative 3.3 threshold, as shown in Table A.5 in Appendix A, none of the formative constructs suffers from multicollinearity (Diamantopoulos & Siguaw, 2006; Petter, Straub, & Rai, 2007).

The common method bias (CMB) could have affected the result integrity because both dependent and independent variables were gathered from the same participant. To investigate whether it is a concern, following Podsakoff et al. (2003) and Schwarz, Rizzuto, Carraher-Wolverton, Roldán, and Barrera-Barrera (2017), we employed several procedural and statistical approaches (see Table B.1 in Appendix B for the implemented procedural and statistical approaches) to remedy and control for presence of common method bias; these included Harman's single-factor test (Podsakoff & Organ, 1986), partial correlation procedures (partialling out social desirability and a "marker" variable; Podsakoff et al., 2003), and full collinearity assessment approach (Kock, 2015; Kock & Lynn, 2012). Based on the results, we conclude that CMB is not a major threat.

6.2 Hypothesis testing

Figure 2 shows the results of the PLS estimation. We controlled for the effects of age, gender, race, tenure, ISP knowledge, company information intensity, IT-related job, type of job, company size, social desirability bias, education, and ISP knowledge. Except for education ($b = -.15$, $P < .005$) and social desirability bias ($b = .11$, $P < .05$), none of the other variables had a significant effect on ISP compliance (all Ps > .15). These results showed that employees with lower education are more likely to comply with the organizational ISP.
H1 specifies that the command-and-control approach is positively associated with employee ISP compliance. Consistent with H1, the link from the command-and-control approach to ISP compliance was positive and significant ($b = .17$, $t = 2.49$, $P < .02$). H2 proposes that the self-regulatory approach is positively associated with employee ISP compliance, and the result supported this hypothesis ($b = .41$, $t = 5.13$, $P < .001$).

To test the moderating effects, we created multiplicative terms by cross-multiplying the items of relevant constructs (Chin et al, 2003). We standardized the items to prevent the potential issues of multicollinearity (Aiken, West, & Reno, 2014). We then calculated the coefficients using the bootstrapping technique. The PLS test results showed that a rules-oriented ethical climate negatively moderated both the effect of command-and-control approach (*b* = −.12, *t* = 2.88, *P* < .01) and the effect of self-regulatory approach (*b* = −.12, *t* = 2.82, *P* < .01) on ISP compliance, thereby supporting H3 and H4, respectively. Susceptibility to interpersonal influence was found to negatively moderate the effect of command-and-control approach (*b* = −.16, *t* = 3.35, *P* < .001) and the effect of self-regulatory approach (*b* = −.14, *t* = 2.68, *P* < .01) on ISP compliance as well, in support of H5 and H6, respectively. Notably, our proposed model explained 51% of the variance in ISP compliance.

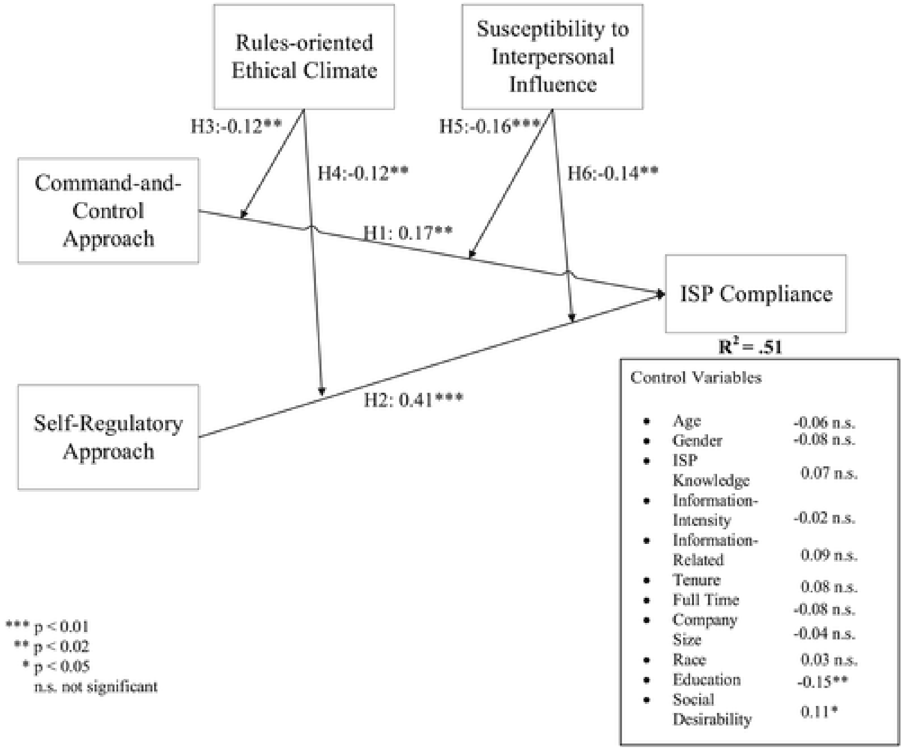


Figure 2. PLS results

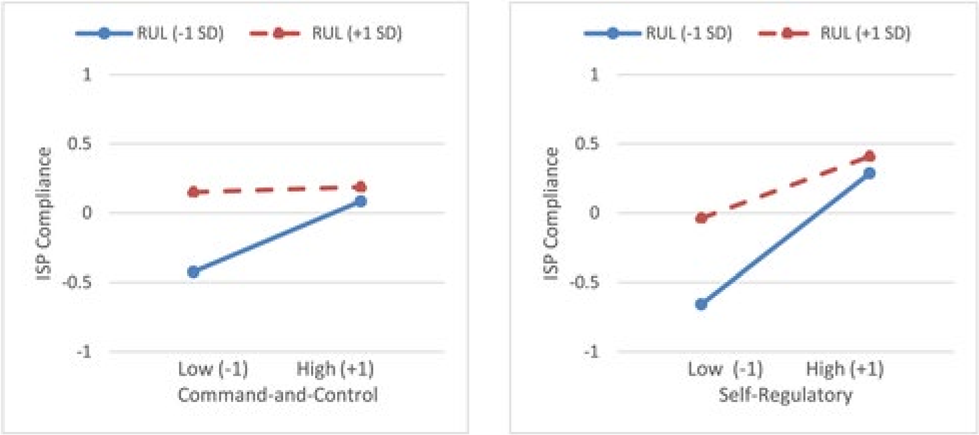
To test the importance of the moderating role of a rules-oriented ethical climate and susceptibility to interpersonal influence, we estimated the significance of the difference in variance explained between one model that contains the moderating effects (ie, the interaction model) and the other that does not have the moderating effects (ie, the main effects model), using the following F-statistics:

$$F(df_{Interaction} - df_{main}, N - df_{Interaction} - 1) = \frac{\Delta R^2 / (df_{Interaction} - df_{main})}{\left(1 - R^2_{Interaction}\right) / (N - df_{Interaction} - 1)}.$$

For the moderating effect of a rules-oriented ethical climate on the relationship between the command-and-control approach and ISP compliance, the *F*-value was 8.54 (*P* < .001). For the moderating effect on the relationship between the self-regulatory approach and ISP compliance, it was 14.94 ($P < .001$). Next, for the moderating effect of susceptibility to interpersonal influence on the relationship between the command-and-control approach and ISP compliance, the F-value was 12.61 ($P < .001$). Finally, for the moderating effect of susceptibility to interpersonal influence on the relationship between the self-regulatory approach and ISP compliance, it was 11.55 ($P < .001$).

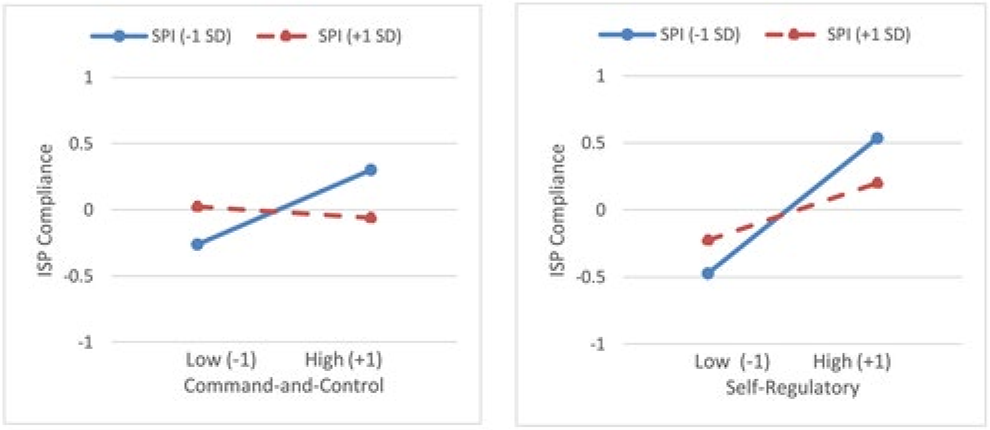
We further validated the moderating effect using Cohen's f^2, which compares the R^2 value of the interaction effect on the main effect with the following equation (Chin et al, 2003): $f^2 = (R^2_{Interaction} - R^2_{Main})/(1 - R^2_{Main})$ = (0.526-0.509)/(1-0.509)-0.04 for H3, (0.538-0.509)/(1-0.509)-0.06 for H4, (0.533-0.509)/(1-0.509)-0.05 for H5, and (0.531-0.509)/(1-0.509)-0.05 for H6, indicating that the effect size of H3, H4, H5, and H6 denotes a small to medium effect (Cohen, 2019). Overall, these results provide further support for H3, H4, H5, and H6. It is important to note that a small f^2 does not necessarily imply an unimportant effect, especially when the moderations result in meaningful changes in beta (Chin et al, 2003).

To illustrate the moderating effects, we plotted two regression lines for each independent variable (the command-and-control and self-regulatory approaches) based on the dependent variable (ISP compliance) when the moderating variables were low (one standard deviation below the mean) and high (one standard deviation above the mean). Figure 3 presents the moderating effect of a rules-oriented ethical climate, and Figure 4 illustrates the moderating role of susceptibility to interpersonal influence. These two figures indicate that the effects of command-and-control and self-regulatory approaches on ISP compliance are weaker when these two aspects of social influence are higher.



RUL: Rules-oriented ethical climate
Note: The scales represent the standardized value for the command-and-control approach, the self-regulatory approach, and ISP Compliance.

Figure 3. The moderating effect of rules-oriented ethical climate on the relationship between the command-and-control and self-regulatory approaches and ISP compliance



SPI: Susceptibility to Interpersonal Influence
Note: The scales represent the standardized value for the command-and-control approach, the self-regulatory approach, and ISP Compliance.

Figure 4. The moderating effect of susceptibility to interpersonal influence on the relationship between the command-and-control and self-regulatory approaches and ISP compliance

7 DISCUSSION

This study investigates the moderating roles of a rules-oriented ethical climate and susceptibility to interpersonal influence on the effects of command-and-control and self-regulation approaches on ISP compliance. Our results show that both the command-and-control and self-regulatory approaches are significant predictors of employee ISP compliance, supporting H1 and H2. Contrary to previous studies that have questioned the relevance of command-and-control approach in the presence of self-regulatory approach (eg, D'Arcy et al., 2009, Guo & Yuan, 2012, Hu et al., 2011, Li et al., 2010, Son, 2011), we found that both approaches predict employee ISP compliance. This finding is consistent with those of prior research (eg D'Arcy & Devaraj, 2012, Yazdanmehr & Wang, 2016). Also, consistent with previous studies (see Cram et al.'s 2019 meta-analysis for further discussion), the effect of the self-regulatory approach was shown to be more important than that of the command-and-control approach, as suggested by its larger standardized path coefficient, *t*-statistic value, and the *t*-test results, indicating that the difference between the coefficients is statistically significant at $p < 0.01$.

The results also support our argument that ISP compliance could be a social phenomenon. We found the moderating effects of social influence at both organizational (ie, rules-oriented ethical climate) and individual (ie, susceptibility to interpersonal influence) levels. In particular, the command-and-control and self-regulatory approaches are more effective when a rules-oriented ethical climate is perceived to be low (vs high) in the organization, supporting H3 and H4. Furthermore, the effect of command-and-control approach and of the self-regulatory approach on ISP compliance are less significant for employees high (vs low) in susceptibility to interpersonal influence, supporting H5 and H6.

As indicated by the slope analysis of the moderation results (see Figures 3 and 4), when there is a strong presence of rules-oriented ethical climate or when employees are highly sensitive to interpersonal influence, the command-and-control approach does not predict employee ISP compliance. Though this is not true for the self-regulation approach since the effect is weak.

Additionally, as depicted in Figure 3, the level of ISP compliance is consistently higher for employees who perceived a strong rules-oriented ethical climate, suggesting a direct effect of a rules-oriented ethical climate on ISP compliance. However, a direct effect of susceptibility to interpersonal influence is not apparent. Thus, as shown in Figure 4, there is a cross-over phenomenon between the lines of low and high susceptibility to interpersonal influence with respect to the effects of command-and-control and self-regulatory approaches. Interestingly, when susceptibility to interpersonal influence is high, the command-and-control approach may create a boomerang effect and push employees to become less likely to comply with the ISP, opposite to the intention of the command-and-control approach.

7.1 Contributions to Theory

This research contributes to the information security literature in several ways. First, by including two important aspects of social influence as contingent factors in the model, the study advances the understanding of the well-established effects of command-and-control and self-regulatory approaches on ISP compliance. As has been noted, a common strategy to enforce ISP compliance relies on the deterrence effect of sanctions, but recent literature has produced mixed findings in terms of effectiveness (see D'Arcy and Herath (2011) and Sommestad, Hallberg, Lundholm and Bengtsson (2014) for reviews).

Although some studies found that deterrence effectively promotes ISP compliance (Y. Chen et al., 2012; D'Arcy & Devaraj, 2012; Johnston et al., 2016), others reported that deterrence has no such effect (Guo & Yuan, 2012; Herath & Rao, 2009b; Hu et al., 2011; Li et al., 2010; Siponen & Vance, 2010; Son, 2011; Vance & Siponen, 2012). By taking social influence factors into account, our study sheds light on contingency factors that may affect the efficacy of deterrence and therefore help reconcile some of the mixed findings found in the literature. Our study also confirmed that the effect of deterrence could vary across individuals as suggested in some other studies (Jacobs, 2010; Mann et al, 2003; Piquero, Moffitt, & Wright, 2009).

Also, in addition to using a command-and-control approach, some practitioners strive to educate employees in the hope that they will consider the ISP to be legitimate and internalize the rules into their own value system; these strategies fall under the self-regulatory approach. Even though research interest in this domain is growing (Ifinedo, 2014; Li et al., 2014; Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009; Vance & Siponen, 2010), the extant literature has not yet considered the effect of social influence on the effectiveness of self-regulatory approach in motivating ISP compliance. Our study is among the first to provide such a framework.

In information security literature, most studies conceptualize social influence as subjective norms or normative beliefs (Bulgurcu, Cavusoglu, & Benbasat, 2010; Cheng et al., 2013; Herath & Rao, 2009b, Herath & Rao, 2009a; Ifinedo, 2012) and/or descriptive norms (Cheng et al., 2013; Herath & Rao, 2009b). By extending this line of research, our study enriches the concept of social influence in providing a novel perspective of investigating it at both the organizational (via rules-oriented ethical climate) and individual (via susceptibility to interpersonal influence) level. These two contigencies provide a better and somewhat different representation of social influence in the organization. A rules-oriented ethical climate, unlike descriptive norms, clearly indicates that a common behaviour among employees is compliance with rules and procedures.

In addition, susceptibility to interpersonal influence, unlike subjective norms, does not assume that all employees have equal tendency to be receptive to social influence nor does it specify the favourable norms as do subjective norms. In summary, our study suggests that social influence could be used as a contingency factor for future research on information security compliance.

Overall, our findings align with the notion that social influence plays an important role in employee compliance behaviour (Bulgurcu, Cavusoglu, & Benbasat, 2010; Cheng et al., 2013; Herath & Rao, 2009b, Herath & Rao, 2009a; Ifinedo, 2012). However, our study departs from the previous approach in that, instead of being additive, such as D'Arcy and Devaraj's (2012) inclusion of "the need for social approval trait" as a determinant of ISP violations, it brings the contingency effects of social influence into focus. The results address the gap in the literature on relevant moderators (eg, D'Arcy & Herath, 2011 and Jones, 1991). They complement previous studies that are either unsuccessful in showing the contingency effects (eg, Johnston et al., 2016 and Li et al, 2018) or investigated such contingencies at one level (Hovav & D'Arcy, 2012; Yazdanmehr & Wang, 2016).

7.2 Implications for Practice

Apart from theoretical contributions, this research has several implications for information security practices in organizations. First, we have shown that employee compliance stems from the perception that ISP violations are likely to be detected and punished, and from the degree to which they believe the rules to be legitimate and consistent with their values (Tyler & Blader, 2005). The results also indicate that the self-regulatory approach is more effective, suggesting that it may be prudent for organizations to pay more attention and devote more effort to developing legitimacy of information security policies and establishing strategies to promote employee internalization of organizations values. Although investigating how to establish legitimacy or trigger value internalization is beyond the scope of our study, it deserves future investigation. Despite the findings of lower efficacy, the command-and-control approach remains a vital component in promoting compliance, so organizations should not altogether abandon this approach.

As a second point, this study revealed the important role of social influence as a contingency to the effects of command-and-control and self-regulatory approaches. The results suggest that implementation of either or both approaches may be less effective if social influence is not considered. Managers should therefore consider leveraging key factors, namely a rules-oriented ethical climate and susceptibility to interpersonal influence, when either enforcing the command-and-control approach or investing in the self-regulatory approach.

As our findings suggest, a rules-oriented ethical climate establishes a boundary related to the effects of both the command-and-control and self-regulatory approaches on ISP compliance. In an organization with a strong rules-oriented ethical climate, further investment in such approaches may not be a wise choice. In contrast, in an organization with a weak rules-oriented ethical climate, it would be advisable to implement robust command-and-control and/or self-regulatory approaches to support ISP compliance.

Our findings also indicate that susceptibility to interpersonal influence can significantly impact the effectiveness of command-and-control and self-regulatory approaches, because those who exhibit high degrees of susceptibility to interpersonal influence are more likely to observe their peers for cues of accepted behaviours. Therefore, to appeal to such employees, managers should communicate that other employees in the organization comply with the ISP. For example, employees susceptible to interpersonal influences often look to their peers' ISP decisions when making decision on ISP-related issues; an effective strategy would be to provide such employees with the possibility of interacting with those exhibiting high levels of ISP compliance.

7.3 Limitations and future research

Our study has limitations that deserve consideration. The first is rooted in its cross-sectional design that provides the least support for the causal directions proposed in our model. The proposed causality is basedboth on theory and the empirical findings documented in previous research. It may be compelling to investigate the stability of social influence and whether its change over time significantly influences ISP compliance; future research could use more objective data to capture the frequency of employee interactions. Specifically, it may be fruitful for future researchers to examine employee interactions with supervisors and teammates.

Although the results suggested that social desirability does not change the significance of the hypothesized paths, the relationship between ISP compliance and social desirability was significant ($b = .11$, $P < .05$). Despite efforts to mitigate the effect of social desirability on the findings by controlling its effect in our hypothesis testing, we believe that because of the nature of our study (ISP compliance), it is possible that social desirability bias skewed the responses towards ISP compliance. Thus, we suggest that future studies implement approaches designed to mitigate such an effect.

It should be mentioned that, although our sample size was sufficient to test our theoretical framework, a larger sample size could provide more statistical power and performance, in particular for looking into moderating paths. Indeed, these results should be interpreted with caution, since our participants were exclusively drawn from employees residing in the United States, and almost 73% came from the same ethnic group, limiting the generalizability of our findings. Also, almost 24% of our participants came from the retail industry, with the rest mostly from mostly from information technology, financial services, health care, telecommunications, manufacturing, and government. Given the varying level of regulatory requirements across different industries, future studies could focus their design on particular industries.

In this study, in evaluating a rules-oriented ethical climate, we relied on employees to estimate others' attitudes or behaviors (regarding rules and compliance) based on social projection (Gerard & Orive, 1987). However, the accuracy of social projection has been questioned because employees may evaluate attitudes of their peers differently than the peers themselves (Gerard & Orive, 1987).

Culture has been shown to be an influential factor that alters employee compliance (e.g., Hovav & D'Arcy, 2012). Our sample was taken from a population with a Western cultural background, and their concept of compliance with policies may differ from that found in Eastern cultures (c.f., Hu et al., 2011). Thus, the impact of national culture may threaten the generalizability of these results to other cultures (e.g., Eastern). Future studies may consider cross-cultural design to validate our model.Behaviors (e.g., ISP compliance) are also inherently hierarchical in the organizational context (c.f., Guo,Yuan, Archer, & Connelly, 2011).

This study overlooks the role that group-level factors may play in ISP compliance. For example, it has been suggested such that achieving higher ISP compliance could be the result of a group effort (e.g., Dourish & Anderson, 2006; Hsu et al., 2015). Thus. it may be fruitful for future researchers to incorporate groups (e.g., teams, departments, and work groups) into their research design to examine how group-level factors may interact with individual-level variables to affect ISP compliance. Future research may thus investigate and consider the variances of perceptions regarding social influence into the equation. One possible approach would be to provide a better understanding of the role of social influence by using perceptual composition measures that account for such differences among individuals.

Finally, we must acknowledge that other types of ethical climates (caring, law and code, instrumental, and independence) could be relevant within the context of this study. However, as mentioned in the theoretical background section, for this study a rules-oriented ethical climate was deemed to be the most relevant. As a result, for the purpose of providing a phenomenon that represents social influence regarding rule-following at the organizational level, including all five ethical climates seemed excessive and beyond our scope. Nevertheless, we do suggest future studies investigating other ethical climates to provide better understanding of their roles at the organizational level.

7.4 Conclusion

Approaches to motivating employees to comply with an ISP have drawn attention from both practitioners and researchers. The main objective of this study was to test the moderating effect of social influence at the individual and organizational levels—rules-ethical climate and susceptibility to interpersonal influence, respectively—on the effect of command-and-control and self-regulatory approaches in motivating employee ISP compliance. Our results show that when a rules-oriented ethical climate or susceptibility to interpersonal influence is higher, the effectiveness of command-and-control and self-regulatory approaches in motivating employee compliance tends to be diminished. This study contributes to the literature by investigating the boundary conditions under which the rule-following approaches are more or less effective.

ENDNOTES

1. We acknowledge that past studies have investigated motivational factors associated with ISP compliance, noncompliance, violation, abuse, shadow, and misuse. Collectively, we refer to this body of research as ISP compliance research.
2. It should be noted that we do not argue that moral disengagement and moral values can be used interchangeably. We are simply stating that studies have investigated the role of morality through the lens of moral disengagement, and the effect of moral disengagement is found to be contingent on the contextual and dispositional factors. The theoretical distinction between moral disengagement and moral values is beyond the scope of this study and

requires further empirical investigations. Further, it is noteworthy to mention that neutralization is conceptually similar to the theory of moral disengagement from both criminology (Clarke, 1997) and information security (Willison & Warkentin, 2013) perspectives. It refers to employee attempts to rationalize their motivations to downplay their guilt or shame for engaging in ISP violations and consequently make them seem like a normal and necessary action (Siponen & Vance, 2010). Neutralization is also regarded as sensitive to social and situational factors (cf, Barlow, Warkentin, Ormond, & Dennis, 2018; Hinduja, 2007; Willison & Warkentin, 2013).

3. It has been suggested that measurement model misspecification may bias the structural estimates, unduly sway the results of the analysis (Jarvis, MacKenzie, & Podsakoff, 2012). Therefore, we also modeled the second-order constructs as reflective measurements but did not find significant differences in the results between the formative and the reflective models.
4. Cohen (2019) defined effect sizes of 0.02 as small, 0.15 as medium, and 0.35 as large.
5. Subjective norms reflect the opinion of important others (eg, supervisor) about whether one should comply. They are stable and often based on cognitive beliefs at the interpersonal level. Descriptive norms reflect others' compliance behaviour. They are based on the perceptions of peer behaviour and thus are at the intrapersonal level.

References

Aiken, L. S., West, S. G., & Reno, R. R. (1991). *Multiple Regression: Testing and Interpreting Interactions*. Newbury Park, CA: Sage.

Akers, R. L., Krohn, M. D., Lanza-Kaduce, L., & Radosevich, M. (1979). Social Learning and Deviant Behavior: A Specific Test of a General Theory. *American Sociological Review*, **44**(4), 636– 655.

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.

Alzahrani, A., Johnson, C., & Altamimi, S. (2018). Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation. In *4th International Conference on Information Management* (pp. 128– 132).

Bala, H., & Venkatesh, V. (2013). Changes in employees' job characteristics during an enterprise system implementation: A latent growth modeling perspective. *MIS Quarterly*, **37**(4), 1113– 1140.

Balozian, P., Leidner, D., & Warkentin, M. (2017). Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems*, 1– 14.

Bandura, A. (1977). *Social learning theory*. New York, NY: General Learning Press.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, NJ: Prentice-Hall.

Bandura, A. (1991). Social Cognitive Theory of Self-Regulation. *Organization Behavior and Human Decision Processes*, **50**(2), 248– 287.

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

Banerjee, D., Cronan, T. P., & Jones, T. W. (1998). Modeling IT Ethics: A Study in Situational Ethics. *MIS Quarterly*, **22**(1), 31– 60.

Bansal, G., Green, W., Hodorff, K., & Marshall, K. (2016). *Moral beliefs and organizational information security policy compliance: The role of gender. Proceedings of the Eleventh Midwest United States Association for Information Systems.*

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers and Security*, *39*(PART B), 145–159.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, **19**, 689– 715.

Barnett, T., & Schubert, E. (2002). Perceptions of the ethical work climate and covenantal relationships. *Journal of Business Ethics*, **36**(3), 279– 290.

Barnett, T., & Vaicys, C. (2000). The Moderating Effect of Individuals' Perceptions of Ethical Work Climate on Ethical Judgments and Behavioral Intentions. *Journal of Business Ethics*, **27**(4), 351– 362.

Batson, C. D., & Thompson, E. R. (2001). Why don't moral people act morally? Motivational considerations. *Current Directions in Psychological Science*, **10**(2), 54– 57.

Bearden, W. O., & Etzel, M. J. (1982). Reference Group Influence on Product and Brand Purchase. *Journal of Consumer Research*, **9**(2), 183– 194.

Bearden, W. O., Netemeyer, R. G., & Teel, J. E. (1989). Measurement of consumer susceptibility to interpersonal influence. *Journal of Consumer Research*, **15**(4), 473– 481.

Becker, G. (1968). Crime and Punishment: An Economic Approach. In *Essays in the Economics of Crime and Punishment* (Vol. **76**) (pp. 1– 54). UMI.

Belsley, D., Kuh, E., & Welsch, R. (1980). *Regression Diagnostics: Identifying Influential Data and Sources of Collinearity*. New York, NY: John Wiley & Sons.

Bijlsma-Frankema, K. M., & Costa, A. C. (2010). Consequences and antecedents of managerial and employee legitimacy interpretations of control: A natural open system approach. In *Organizational control* (pp. 396– 433). Cambridge, UK: Cambridge University Press.

Bloch, P. H., Ridgway, N. M., & Sherrell, D. L. (1989). Extending the concept of shopping: An investigation of browsing activity. *Journal of the Academy of Marketing Science*, **17**(1), 13– 21.

Bonabeau, E. (2004). The perils of the imitation age. *Harvard Business Review*, **82**(6), 45– 54.

Brass, D. J., Butterfield, K. D., & Skaggs, B. C. (1998). Relationships and unethical behavior: A social network perspective. *Academy of Management Review*, **23**(1), 14– 31.

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

Burnkrant, R. E., & Cousineau, A. (1975). Informational and normative social influence in buyer behavior. *Journal of Consumer Research*, **2**(3), 206– 215.

Carte, T. A., & Russell, C. J. (2003). In pursuit of moderation: Nine common errors and their solutions. *MIS Quarterly*, **27**(3), 479– 501.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security at the Workplace: Linking InformationSecurity Climate to Compliant Behavior. *Journal of Information Privacy andSecurity*, **1**(3), 18– 41.

Chen, H., Chau, P. Y. K., & Li, W. (2018). *The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior*. *Information Technology and People.*

Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information and Management*, **55**(8), 1049– 1060.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, **29**(3), 157– 188.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers and Security*, *39*(PART B), 447–459.

Chin, W. W. (1998). Issues and opinion on structural equation modeling. *MIS Quarterly*, **22**(1), 1– 10.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. *Information Systems Research*, **14**(2), 189– 217.

Chin, W. W., Thatcher, J. B., & Wright, R. T. (2012). Assessing common method bias: Problems with the ULMC technique. *MIS Quarterly*, **36**(3), 1003– 1019.

Cialdini, R. B., & Trost, M. R. (1998). *Social influence: Social norms, conformity and compliance. The Handbook of Social Psychology*, Vols. 1 and 2 (pp. 151– 192).

Clarke, R. (1997). *Situational crime prevention: Successful case studies* (2nd ed.). Albany, NY: Harrow and Heston.

Clarke, R., & Cornish, D. (1985). Modelling offenders' decisions: a framework for policy and research. In M. A. Tonry (Ed.), *Crime and Justice: An Annual Review of Research* (Vol. **6**) (pp. 147– 185). Chicago, IL: University of Chicago Press.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences (Vol. 2nd)*. New York, NY: Routledge.

Cornish, D., & Clarke, R. (1986). The reasoning criminal: rational choice perspectives on offending. *Criminology*, **25**(4), 933– 948.

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy Compliance. *MIS Quarterly*, **43**(2), 525– 554.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, **26**(6), 605– 641.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, **43**(6), 1091– 1124.

D'Arcy, J., & Herath, T. (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**(6), 643– 658.

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.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, **20**(1), 79– 98.

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, **29**, 43– 69.

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.

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management*, **17**(4), 263– 282.

Dourish, P., & Anderson, K. (2006). Collective information practice: exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction*, **21**(3), 319– 342.

Falk, R., & Miller, N. (1992). *A primer for soft modeling*. Akron, OH: University of Akron Press.

Ferrell, O. C., & Gresham, L. G. (1985). A contingency framework for understanding ethical decision make in marketing. *Journal of Marketing*, **49**(3), 87– 96.

Fornell, C., & Bookstein, F. L. (1982). Two Structural Equation Models: LISREL and PLS Applied to Consumer Exit-Voice Theory. *Journal of Marketing Research*, **19**(4), 440– 452.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, **18**(1), 39– 50.

Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and deterrence. *European Journal of Information Systems*, **25**(2), 91– 109.

Gaertner, K. (1991). The effect of ethical climate on managers' decisions. In *In Morality, Rationality, and Efficiency: New Perspectives on Socio-economics*. Armonk, NY: Sharpe.

Geerken, M., & Gove, W. (1975). Deterrence: Some theoretical considerations. *Law and Society Review*, **9**(3), 497– 513.

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, **4**(7), 1– 7.

Gerard, H. B., & Orive, R. (1987). The dynamics of opinion formation. In *Advances in experimental social psychology* (Vol. **20**) (pp. 171– 202). Elsevier.

Goodhue, D. L., Lewis, W., & Thompson, R. (2012). Does PLS have advantages for small sample size or non-normal data? *MIS Quarterly*, **36**(3), 981–A16.

Gouldner, A. W. (1957). Cosmopolitans and Locals:Toward an Analysis of Latent Social Roles. *Administrative Science Quarterly*, **2**(3), 281– 306.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information and Management*, **49**(6), 320– 326.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, **28**(2), 203– 236.

Guo, Y., Bao, Y., Stuart, B. J., & Le-Nguyen, K. (2018). To sell or not to sell: Exploring sellers' trust and risk of chargeback fraud in cross-border electronic commerce. *Information Systems Journal*, **28**(2), 359– 383.

Hair, J. F., Black, W. C., & Babin, B. J. (2010). *Multivariate data analysis: A global perspective. In* (Global ed.). Upper Saddle River, NJ: Pearson Education.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R., & Tatham, R. (2006). *Multivariate data analysis with readings* (6th ed.). Englewood Cliffs, NJ: Prentice Hall.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2009). *Multivariate data analysis*. Upper Saddle River, NJ: Prentice Hall.

Harrington, S. J. S. J. (1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly*, **20**(3), 257– 278.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, **47**(2), 154– 165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, **18**(2), 106– 125.

Herath, T., Yim, M.-S., D'Arcy, J., Nam, K., & Rao, H. R. (2018). Examining employee security violations: moral disengagement and its environmental influences. *Information Technology and People*, **31**(6), 280– 299.

Hinduja, S. (2007). Neutralization theory and online software piracy: An empirical analysis. *Ethics and Information Technology*, **9**(3), 187– 204.

Hitt, M. A., Beamish, P. W., Jackson, S. E., Mathieu, J. E., Hitf, M. A., & Jackson, S. E. (2007). Building Theoretical and Empirical Bridges across Levels: Multilevel Research in Management. *The Academy of Management Journal*, **50**(6), 1385– 1399.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information and Management*, **49**(2), 99– 110.

Hsu, J. S.-C., Shis, S.-P., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, **26**(2), 282– 300.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (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., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, **54**(6), 54– 60.

Hunt, S. D., & Vitell, S. (1986). A General Theory of Marketing Ethics. *Journal of Macromarketing*, **6**(1), 5– 16.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, **31**(1), 83– 95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, **51**(1), 69– 79.

Jacobs, B. A. (2010). Deterrence and Deterrability*. *Criminology*, **48**(2), 417– 441.

Jaramillo, F., Mulki, J., & Solomon, P. (2006). The Role of Ethical Climate on Salesperson's Role Stress, Job Attitudes, Turnover Intention, and Job Performance. *Journal of Personal Selling and Sales Management*, **26**(3), 271– 282.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research. *Journal of Consumer Research*, **30**(2), 199– 218.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2012). The negative consequences of measurement model misspecification: Aresponse to Aguirre-Urreta and Marakas. *MIS Quarterly*, **36**(1), 139– 146.

Jehn, K. A. (1995). A multimethod examination of the benefits and detriments of intragroup conflict. *Administrative Science Quarterly*, **40**(2), 256– 282.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, **25**(3), 1– 21.

Jones, T. M. (1991). Ethical decision making by individuals in organizations: An issue-contingent model. *The Academy of Management Review*, **16**(2), 366– 395.

Kahan, J. P. (1974). Rationality, the Prisoner's Dilemma, and Population. *Journal of Social Issues*, **30**(4), 189– 210.

Kelman, H. C. (1961). Processes of Opinion Change. *The Public Opinion Quarterly*, **25**(1), 57– 78.

Kelman, H. C. (1974). Further thoughts on the 5 processes of compliance, identification, and internalization. *Perspectives on Social Power*, 125– 171.

Kim, J., Park, E. H., & Baskerville, R. L. (2016). A model of emotion and computer abuse. *Information and Management*, **53**(1), 91– 108.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of E-Collaboration*, **11**(4), 1– 10.

Kock, N., & Lynn, G. S. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems*, **13**(7), 546– 580.

Kohlberg, L. (1981). *The philosophy of moral development: Moral stages and the ideal of justice*. San Francisco: Harper and Row.

Kramer, R. M., & Messick, D. M. (1996). Ethical cognition and the framing of organizational dilemmas: Decision makers as intuitive lawyers. In *Codes of conduct: Behavioural research into business ethics* (pp. 59– 85). New York: Russell Sage.

Kranz, J. J., & Haeussinger, F. J. (2014). Why Deterrence is not Enough: The Role of Endogenous Motivations on Employees' Information Security Behavior. Proceedings of the 35th International Conference on Information Systems.

Kuran, T. (1997). *Private truths, public lies: The social consequences of preference falsification*. Harvard University Press.

Latham, G. P., & Saari, L. M. (1979). Application of social-learning theory to training supervisors through behavioral modeling. *Journal of Applied Psychology*, **64**(3), 239– 246.

Li, H., & Luo, X. (Robert), Zhang, J., & Sarathy, R. (2018). Self-control, organizational context, and rational choice in Internet abuses at work. *Information and Management*, **55**(3), 358– 367.

Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, **24**(6), 479– 502.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, **48**(4), 635– 645.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, **31**(1), 59– 87.

Lilliefors, H. W. (1967). On the Kolmogorov-Smirnov test for normality with mean and variance unknown. *Journal of the American Statistical Association*, **62**(318), 399– 402.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, **86**(1), 114– 121.

Lohmöller, J.-B. (1989). *Latent variable path modeling with partial least squares*. Heidelberg: Physica-Verlag.

Lowry, P. B., D'Arcy, J., Hammer, B., & Moody, G. D. (2016). "Cargo Cult" science in traditional organization and information systems survey research. *The Journal of Strategic Information Systems*, **25**(3), 232– 240.

Mackenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, **35**(2), 293– 334.

Malhotra, Y., Galletta, D. F., & Kirsch, L. J. (2008). How Endogenous Motivations Influence User Intentions: Beyond the Dichotomy of Extrinsic and Intrinsic User Motivations. *Journal of Management Information Systems*, **25**(1), 267– 300.

Mann, R. E., Smart, R. G., Stoduto, G., Adlaf, E. M., Vingilis, E., Beirness, D., … Asbridge, M. (2003). The effects of drinking-driving laws: A test of the differential deterrence hypothesis. *Addiction*, **98**(11), 1531– 1536.

Messick, D. M. (1999). Alternative logics for decisionmaking in social settings. *Journal of Economic Behavior & Organization*, **39**(1), 11– 28.

Mischel, W. (1977). The interaction of person and situation. In *Personality at the cross-roads: Current issues in interactional psychology* (pp. 333– 352). Hillsdale, NJ: Lawrence Erlbaum Associates.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, **42**(1), 285– 311.

Moore, C., Detert, J. R., Trevino, L. K., Baker, V. L., & Mayer, D. M. (2012). Why employees do bad things: Moral disengagement and unethical organizational behavior. *Personnel Psychology*, **65**(1), 1– 48.

Mourali, M., Laroche, M., & Pons, F. (2005). Antecedents of Consumer Relative Preference for Interpersonal Information Sources in Pre-Purchase Search. *Journal of Consumer Behaviour*, **4**(5), 307– 318.

Mourali, M., & Yang, Z. (2013). The Dual Role of Power in Resisting Social Influence. *Journal of Consumer Research*, **40**(3), 539– 554.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, **18**(2), 126– 139.

Nagin, D. S., & Paternoster, R. (1993). Enduring individual differences and rational choice theories of crime. *Law & Society Review*, **27**(3), 467– 496.

Neter, J., Wasserman, W., & Kutner, M. H. (1989). *Applied linear regression models*. Homewood, IL: Irwin.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric Theory* (3rd ed.). New York, NY: McGraw-Hill.

Park, C. W., & Lessig, V. P. (1977). Students and Housewives: Differences in Susceptibility to Reference Group Influence. *Journalof Consumer Research*, **4**(2), 102– 110.

Paternoster, R. (1987). The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues. *Justice Quarterly*, **4**(2), 173– 217.

Paternoster, R., & Simpson, S. (1996). Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime. *Law & Society Review*, **30**(3), 549– 583.

Petter, S., Straub, D., & Rai, A. (2007). Specifying Formative Constructs in Information Systems Research. *MIS Quarterly*, **31**(4), 623– 656.

Pillutla, M. M., & Chen, X.-P. (1999). Social Norms and Cooperation in Social Dilemmas: The Effects of Context and Feedback. *Organizational Behavior and Human Decision Processes*, **78**(2), 81– 103.

Piquero, A. R., Moffitt, T. E., & Wright, B. E. (2007). Self-Control and Criminal Career Dimensions. *Journal of Contemporary Criminal Justice*, **23**(1), 72– 89.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y. Y., & Podsakoff, N. P. (2003). Common method biases in behavioural research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, **88**(5), 879– 903.

Podsakoff, P. M., & Organ, D. W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management*, **12**(4), 531– 544.

Pogarsky, G. (2002). Identifying “deterrable”offenders: Implications for research on deterrence. *Justice Quarterly*, **19**(3), 431– 452.

Rashotte, L. (2007). Social influence. *The Blackwell Encyclopedia of Social Psychology*, **9**, 562– 563.

Ringle, C., Wende, S., & Becker, J. (2015). SmartPLS 3. SmartPLS GmbH, http://www.Smartpls.Com.

Robinson, P. H., & Darley, J. M. (1995). *Justice, liability, and blame: Community views and the criminal law*. Boulder, CO: Westview Press.

Rönkkö, M., & Ylitalo, J. (2011). PLS marker variable approach to diagnosing and controlling for method variance. *ICIS 2011 Proceedings.*

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, **55**(1), 68– 78.

Salancik, G. R., & Pfeffer, J. (1978). A social information processing approach to job attitudes and task design. *Administrative Science Quarterly*, **23**(2), 224– 253.

Sarker, S., Ahuja, M., & Sarker, S. (2018). Work–life conflict of globally distributed software development personnel: An empirical investigation using border theory. *Information Systems Research*, **29**(1), 103– 126.

Schneider, B. (1975). Organizational Climates: An essay. *Personnel Psychology*, **28**, 447– 479.

Schwarz, A., Rizzuto, T., Carraher-Wolverton, C., Roldán, J. L., & Barrera-Barrera, R. (2017). Examining the impact and detection of the “urban legend” of common method bias. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, **48**(1), 93– 119.

Shin, Y. (2012). CEO Ethical Leadership, Ethical Climate, Climate Strength, and Collective Organizational Citizenship Behavior. *Journal of Business Ethics*, **108**(3), 299– 313.

Shu, L. L., Gino, F., & Bazerman, M. H. (2011). Dishonest deed, clear conscience: When cheating leads to moral disengagement and motivated forgetting. *Personality and Social Psychology Bulletin*, **37**(3), 330– 349.

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information and Management*, **54**(8), 1023– 1037.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *IEEE Computer Society*, **43**(2), 64– 71.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, **34**(3), 487– 502.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, **22**(1), 42– 75.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, **48**(7), 296– 302.

Son, J.-Y., & Park, J. (2016). Procedural justice to enhance compliance with non-work-related computing (NWRC) rules: Its determinants and interaction with privacy concerns. *International Journal of Information Management*, **36**, 309– 321.

Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data collection in the digital age: Innovation alternatives to student samples. *MIS Quarterly*, **38**(2), 355– 378.

Strahan, R., & Gerbasi, K. C. (1972). Short, homogeneous versions of the Marlow-Crowne Social Desirability Scale. *Journal of Clinical Psychology*, **28**(2), 191– 193.

Straub, D. (1990). Effective IS security: An empirical study. *Information Systems Research*, **1**(3), 255– 276.

Sunstein, C. R. (1996). Social Norms and Social Roles. *Columbia Law Review*, **96**(4), 903– 968.

Sutherland, E., Cressey, D., & Luckenbill, D. (1992). *Principles of criminology*. Rowman & Littlefield.

Sutinen, J. G., & Kuperan, K. (1999). A Socio-Economic Theory of Regulatory Compliance. *International Journal of Social Economics*, **2**(3), 174– 193.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, **22**(6), 664– 670.

Templier, M., & Paré, G. (2015). A framework for guiding and evaluating literature reviews. *Communications of the Association for Information Systems*, **37**(6), 112– 137.

Tenbrunsel, A. E., & Messick, D. M. (1999). Sanctioning Systems, Decision Frames, and Cooperation. *Administrative Science Quarterly*, **44**(4), 684– 707.

Trevino, L. K. (1986). Ethical decision making in organizations: A person-situation interactionist model. *Academy of Management Review*, **11**(3), 601– 617.

Trevino, L. K. (1992). The Social Effects of Punishment in Organizations: a Justice Perspective. *Academy of Management Review*, **17**(4), 647– 676.

Tyler, T. R. (1990). *Why People Obey the Law*. New Haven: Yale University Press.

Tyler, T. R. (2005). Promoting Employee Policy Adherence and Rule Following in Work Settings: The Value of Self-Regulatory Approaches. *70 Brooklyn Law Review*, **1312**(4), 1287– 1312.

Tyler, T. R. (2006). Psychological Perspectives on Legitimacy and Legitimation. *Annual Review of Psychology*, **57**(1), 375– 400.

Tyler, T. R. (2009). Self-regulatory approaches to white-collar crime: The importance of legitimacy and procedural justice. In *The Criminology of White-Collar Crime* (pp. 195– 216).

Tyler, T. R., & Blader, S. L. (2005). Can Businesses Effectively Regulate Employee Conduct? the Antecedents of Rule Following in Work Settings. *Academy of Management Journal*, **48**(6), 1143– 1158.

Tyler, T. R., Callahan, P. E., & Frost, J. (2007). Armed, and Dangerous (?): Motivating Rule Adherence Among Agents of Social Control. *Law & Society Review*, **41**(2), 457– 492.

Vance, A., & Siponen, M. (2010). *Why do employees violate is security policies? insights from multiple theoretical perspectives*. University of Oulu.

Vance, A., & Siponen, M. (2012). IS security policy violations. *Journal of Organizational and End User Computing*, **24**(1), 21– 41.

Victor, B., & Cullen, J. B. (1988). The organizational bases of ethical work climates. *Administrative Science Quarterly*, **33**(1), 101– 125.

Wang, J., Yang, Z., & Bhattacharjee, S. (2011). Same Coin, Different Sides: Differential Impact of Social Learning on Two Facets of Music Piracy. *Journal of Management Information Systems*, **28**(3), 343– 384.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, **18**(2), 101– 105.

Wenzel, M. (2004). The social side of sanctions: personal and social norms as moderators of deterrence. *Law and Human Behavior*, **28**(5), 547– 567.

Williams, K. R., & Hawkins, R. (1986). Perceptual Research on General Deterrence: A Critical Review. *Law & Society Review*, **20**(4), 545– 572.

Willison, R., Lowry, P. B., & Paternoster, R. (2018). A tale of two deterrents: Considering the role of absolute and restrictive deterrence to inspire new directions in behavioral and organizational security research. *Journal of the Association for Information Systems*, **19**(12), 1187– 1216.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, **37**(1), 1– 20.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, **28**(2), 266– 293.

Wold, H. (1982). Soft modelling: the basic design and some extensions. In K. G. Jöres (Ed.), *Systems Under Indirect Observation: Causality, Structure and Prediction*, Part II (pp. 1– 53). Amesterdam: North Holland.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology*, **58**(c), 212– 222.

Wrong, D. H. (1961). The Oversocialized Conception of Man in Modern Sociology. *American Sociological Review*, **26**(2), 183– 193.

Wyld, D. C., & Jones, C. A. (1997). The Importance of Context: The Ethical Work Climate Construct and Models of Ethical Decision Making -- An Agenda for Research. *Journal of Business Ethics*, **16**(4), 465– 472.

Yang, Z., & Laroche, M. (2011). Parental responsiveness and adolescent susceptibility to peer influence: Across-cultural investigation. *Journal of Business Research*, **64**(9), 979– 987.

Yang, Z., Schaninger, C. M., & Laroche, M. (2013). Demarketing teen tobacco and alcohol use: Negative peer influence and longitudinal roles of parenting and self-esteem. *Journal of Business Research*, **66**(4), 559– 567.

Yang, Z., Wang, J., & Mourali, M. (2015). Effect of peer influence on unauthorized music downloading and sharing: The moderating role of self-construal. *Journal of Business Research*, **68**(3), 516– 525.

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, **92**, 36– 46.

Zhang, H., Luo, X., Liao, Q., & Peng, L. (2015). Does IT team climate matter? An empirical study of the impact of co-workers and the Confucian work ethic on deviance behavior. *Information and Management*, **52**(6), 658– 667.

Biographies

Adel Yazdanmehr is an Assistant Professor of Information Systems at Baruch College, The City University of New York. He received his PhD in Management Information Systems from The University of Texas at Arlington, MS in Business Analytics from the University of Texas at Dallas, MBA from Mazandaran University of Science and Technology, and BS in Software Engineering from University of Isfahan. His current research interests are mainly in the behavioural aspect of information assurance and role of Web 2.0 technologies in Healthcare IT. His work has appeared in *Decision Support Systems* journal as well as *International Conference on Information Systems, and Dewald Roode Workshop on Information Systems Security Research (IFIP).*

Jingguo Wang is a Professor of Information Systems at the University of Texas at Arlington. He received his PhD in Management Science and Systems from the State University of New York at Buffalo. His current research interests are in the areas of cybercrime and information security, information search, and decision making. His work has been published in *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *ACM Transactions on Management Information Systems*, *IEEE Transactions on Systems*, *Man and Cybernetics (Part C)*, *European Journal of Operational Research*, and *Decision Support Systems*, among others. His research has been supported by University of Texas at Arlington and the National Science Foundation.

Zhiyong Yang is a Professor of Marketing and Head of the Department of Marketing, Entrepreneurship, Sustainable Tourism and Hospitality in the Bryan School of Business and Economics and has published over 30 articles in leading scholarly journals, including the Journal of Marketing, Journal of Consumer Research, Journal of Experimental Social Psychology, Journal of Management Information Systems, Journal of the Academy of Marketing Science, and Journal of Retailing. Zhiyong serves on the guest editorship and the editorial review boards of several reputed journals. The research by Zhiyong has been funded by Statistics Canada, Fonds québécois de la recherche sur la société et la culture of Canada, the National Science Foundation of China, and the Association for Consumer Research. He also received competitive research awards from Harvard Center for Risk Analysis, the University of Texas-Arlington, and Cardiff University. Before entering academia, Zhiyong spent over 10 years in industry, holding a number of industry positions, including project manager, marketing manager, and vice-president with major corporations. Zhiyong served on the President Advisory Committee at the University of Texas-Arlington from 2017 to 2018. He has given consumer insights seminars to industry professionals from North America, Europe, and China.

APPENDIX A

Table A1. Demographic characteristics of participants

	Total	Percentage		Total	Percentage
Gender			IT-Related Job		
Male	124	50.4	Yes	106	43.1
Female	122	49.6	No	140	56.9
Age			Type of job		
18-25 y	26	10.6	Full-time	217	88.2
26-35 y	93	37.8	Part-time	29	11.8
36-45 y	62	25.2	Race		
46-55 y	34	13.8	White/Caucasian	180	73.2
56-65 y	28	11.4	African American	25	10.2
66-85 y	3	1.2	Asian	17	6.9
Education			Hispanic	16	6.5
Less than high school	0	0.0	Native American	3	1.2
High school graduate	15	6.1	Other	5	2.0
Some college	58	23.6	Position		
College graduate	124	50.4	Upper management	7	2.8
Post-graduate education	49	19.9	Middle management	56	22.8
Company size			Lower management	58	23.6
Fewer than 500 employees	89	36.2	Non-management	125	50.8
500-999	46	18.7	Tenure		
1000-4999	34	13.8	Less than 1 year	14	5.7
5000-10 000	12	4.9	1-5 y	138	56.1
10 000+ employees	65	26.4	6-10 y	49	19.9
Industry			11-15 y	20	8.1
Information Technology	20	8.1	15+ y	25	10.2
Financial Services	24	9.8	Information intensiveness		
Health care	29	11.8	Not information intensive at all	3	1.2
Telecommunications	18	7.3	Some	42	17.1
Retail	59	24.0	Quite a bit	75	30.5
Manufacturing	14	5.7	An extreme amount	72	29.3
Government	33	13.4	Highly information intensive	54	22.0
Other	49	19.9			

Table A2. Measurement items

ISP Compliance Behaviour (Tyler & Blader, 2005)

- How often do you comply with your organization's ISP?
- How often do you use your organization's ISP to guide you how to access to and use information assets?
- How often do you follow the organization's ISP about how you should use information systems related resources?
- How often do you follow the requirement of your organization's ISP?
- How often do you do as your organization's ISP request?

Rules-oriented Ethical Climate (Victor & Cullen, 1988)

- Successful people in this company go by the book.
- Everyone is expected to stick by company rules and procedures.
- Successful people in this company strictly obey the company policies.

Reaction to Behaviour (Tyler & Blader, 2005)

- If you are caught breaking the organization's ISP, how much does it hurt your pay or your chances for promotion?
- If you were caught breaking the organization's ISP, how much would your organization care?

Detection of Behaviour (Tyler & Blader, 2005)

- How closely is your work monitored by your organization?
- How easy is it for your organization to observe whether or not you follow the organization's ISP?
- How often is your organization paying attention to whether or not you follow the organization's ISP?

Value Congruence (Tyler & Blader, 2005)

- I find that my values and the values where I work are very similar.
- What my company stands for is important to me.
- I agree with the values that define the goals of my company.
- I think that my employer acts very ethically.
- I find that my values and the values where I work are very similar.

Legitimacy (Tyler & Blader, 2005)

- People should support their organizational ISP.
- It is wrong to break organizational ISP, even if you can get away with it.
- Companies are most successful when employees follow their organizational ISP.
- Work organizations are most effective when people follow their organizational ISP.
- Respect for organizational ISP is an important value for employees to have.
- An employee should accept the organizational ISP, even when he or she thinks that those policies are wrong.

Susceptibility to Informational Influence (Bearden, Netemeyer, & Teel, 1989)

- To make sure that I correctly follow the organization's ISP, I often observe what others do.
- I often consult with other people to help choose the correct way to comply with the organization's ISP.
- If I am uncertain whether my action will violate the organization's ISP or not, I often ask my coworkers about it.
- When I do not know how to comply with a particular information security policy, I usually ask friends or coworkers.
- If I am uncertain whether my action will comply with the organization's ISP or not, I often ask my coworkers about it.

Susceptibility to Normative Influence (Bearden et al., 1989)

- I usually comply with the organization's ISP that I think others will approve of.
- I achieve a sense of belonging by complying with the same information security policies that others comply with.
- If others can see my compliance behaviour, I will often comply with the policies that they expect me to comply with.
- To maintain a good relationship with my coworkers, I often comply with those policies that they comply with.
- I feel that complying with a particular ISP policy will enhance my image.

ISP Knowledge (Bloch, Ridgway, & Sherrell, 1989)

- How would most of your coworkers characterize you with regard to the level of KNOWLEDGE you have about your organization's information security policies?
- How would other employees characterize you with regard to the level of KNOWLEDGE you have about your organization's information security policies?

Table A3. Factor loadings, cross-loadings, and item-level VIFs

	COM	RUL	DB	RB	VC	LG	SII	SNI	KN	VIF
Com1	**0.92**	0.58	0.32	0.42	0.35	0.66	0.26	0.20	0.23	4.4
Com2	**0.71**	0.38	0.24	0.27	0.28	0.45	0.29	0.16	0.21	1.7
Com3	**0.86**	0.49	0.31	0.43	0.27	0.57	0.27	0.22	0.24	2.7
Com4	**0.93**	0.52	0.33	0.39	0.32	0.62	0.22	0.19	0.11	5.8
Com5	**0.90**	0.52	0.32	0.39	0.33	0.63	0.24	0.17	0.14	4.2
RUL1	0.49	**0.90**	0.37	0.38	0.48	0.48	0.27	0.26	0.10	2.6
RUL2	0.54	**0.86**	0.37	0.45	0.45	0.55	0.23	0.20	0.21	1.8
RUL3	0.51	**0.90**	0.39	0.40	0.50	0.50	0.32	0.26	0.13	2.7
DB1	0.27	0.35	**0.82**	0.47	0.21	0.33	0.22	0.28	0.18	1.6
DB2	0.27	0.30	**0.86**	0.47	0.29	0.32	0.23	0.20	0.17	1.9
DB3	0.36	0.43	**0.89**	0.61	0.32	0.43	0.35	0.26	0.20	2.1
RB1	0.37	0.40	0.54	**0.94**	0.19	0.38	0.26	0.26	0.12	2.6
RB2	0.47	0.47	0.61	**0.95**	0.23	0.45	0.28	0.23	0.15	2.6
VC1	0.32	0.50	0.31	0.21	**0.92**	0.44	0.28	0.24	0.26	4.9
VC2	0.34	0.44	0.33	0.24	**0.90**	0.46	0.31	0.29	0.27	4.3
VC3	0.35	0.49	0.29	0.20	**0.94**	0.45	0.28	0.27	0.29	5.7
VC4	0.32	0.54	0.26	0.18	**0.86**	0.38	0.27	0.20	0.21	2.8
VC5	0.30	0.47	0.27	0.18	**0.94**	0.43	0.27	0.22	0.23	5.5
LG1	0.62	0.48	0.28	0.37	0.42	**0.84**	0.34	0.25	0.16	2.5
LG2	0.62	0.50	0.40	0.44	0.42	**0.84**	0.29	0.19	0.16	2.7
LG3	0.58	0.51	0.41	0.42	0.44	**0.87**	0.42	0.32	0.15	6.1
LG4	0.54	0.48	0.37	0.37	0.41	**0.87**	0.36	0.30	0.17	6.0
LG5	0.60	0.52	0.37	0.39	0.38	**0.90**	0.32	0.23	0.13	3.7
LG6	0.52	0.45	0.32	0.23	0.34	**0.77**	0.17	0.17	0.17	2.0
SII1	0.15	0.26	0.29	0.24	0.25	0.26	**0.82**	0.42	0.08	2.9
SII2	0.20	0.27	0.28	0.25	0.27	0.29	**0.85**	0.43	0.11	1.8
SII3	0.29	0.22	0.22	0.21	0.22	0.34	**0.87**	0.23	0.05	3.2
SII4	0.30	0.27	0.27	0.25	0.28	0.35	**0.85**	0.31	0.04	3.0
SII5	0.32	0.30	0.27	0.27	0.30	0.39	**0.88**	0.25	0.08	3.6
SNI1	0.18	0.19	0.21	0.23	0.25	0.24	0.34	**0.83**	0.12	2.1
SNI2	0.31	0.33	0.30	0.31	0.33	0.36	0.36	**0.87**	0.17	2.6
SNI3	0.11	0.20	0.19	0.19	0.16	0.23	0.27	**0.87**	0.06	3.1
SNI4	0.12	0.20	0.25	0.14	0.21	0.22	0.34	**0.88**	0.07	3.3
SNI5	0.19	0.21	0.26	0.23	0.18	0.17	0.34	**0.80**	0.04	2.0
KN1	0.20	0.18	0.19	0.14	0.27	0.18	0.09	0.13	**0.93**	1.9
KN2	0.18	0.13	0.20	0.11	0.24	0.16	0.07	0.07	**0.91**	1.9

Note. Bold values represent the the indicators' loading values on their respective construct.
Abbreviations: COM, ISP compliance; DB, detection of behaviour; KN, ISP knowledge; LG, legitimacy; RB, reaction to behaviour; RUL, rules-oriented ethical climate; SII, susceptibility to Informational Influence; SNI, susceptibility to normative influence; VC, value congruence.

Table A4. Reliability, average variance extracted, and construct correlation matrix

	AVE	CR	α	COM	RUL	RB	DB	VC	LG	SNI	SII	KN
COM	0.92	0.94	0.75	**0.87**								
RUL	0.86	0.92	0.78	0.58	**0.89**							
RB	0.88	0.94	0.89	0.44	0.46	**0.95**						
DB	0.82	0.89	0.73	0.35	0.43	0.61	**0.86**					

	AVE	CR	α	COM	RUL	RB	DB	VC	LG	SNI	SII	KN
VC	0.95	0.96	0.83	0.36	0.54	0.22	0.32	**0.91**				
LG	0.92	0.94	0.72	0.68	0.58	0.44	0.42	0.47	**0.85**			
SNI	0.90	0.93	0.72	0.22	0.27	0.26	0.29	0.27	0.29	**0.85**		
SII	0.91	0.93	0.73	0.29	0.31	0.29	0.31	0.31	0.38	0.39	**0.85**	
KN	0.82	0.92	0.85	0.21	0.17	0.14	0.21	0.28	0.19	0.11	0.09	**0.92**

Note. Bold values represent the square root of (AVE) values.
Abbreviations: AVE, average variance extracted; COM, ISP compliance behaviour; CR, composite reliability; DB, detection of behaviour; KN, ISP knowledge; LG, legitimacy; RB, reaction to behaviour; RUL, rules-oriented ethical climate; SII, susceptibility to informational influence; SNI, susceptibility to normative influence; VC, value congruence; α, Cronbach α.

Table A5. Constructs reliability, average variance extracted, and VIF for second-order constructs

	The Command-and-Control Approach	The Self-Regulatory Approach	Susceptibility to Interpersonal Influence	VIF
AVE	0.64	0.57	0.50	
CR	0.90	0.93	0.91	
α	0.86	0.92	0.89	
RB	0.50			1.58
DB	0.62			1.58
LG		0.66		1.29
VC		0.50		1.29
SII			0.62	1.18
SNI			0.58	1.18

Abbreviations: AVE, average variance extracted; CR, composite reliability; DB, detection of behaviour; LG, legitimacy; RB, reaction to behaviour; SII, susceptibility to informational influence; SNI, susceptibility to normative influence; VC, value congruence; α, Cronbach α.

APPENDIX B

Table B1 summarizes the procedural and statistical approaches suggested by previous studies to remedy and control for CMB.

The third approach suggested by Schwarz et al. (2017) is the unmeasured latent method factor technique (Podsakoff et al., 2003), which adds a first-order factor into the model with all the measuring items as indicators. Although this method is helpful, as it does not require any prior measurement of the specific factor responsible for method effects, it is not directly applicable to PLS (Rönkkö & Ylitalo, 2011). Liang, Saraf, Hu, and Xue (2007) have proposed a technique to incorporate this method with PLS analysis, which once gained popularity in Information Systems journals. However, the Liang's proposed method has been criticized for being ineffective in either detecting or controlling for CMB (Chin, Thatcher, & Wright, 2012). Thus, instead of the former method, we included a full collinearity assessment (Kock, 2015; Kock & Lynn, 2012), which has also recently been used in Guo, Bao, Stuart, and Le-Nguyen (2018). The results of the assessment are summarized in Table B4. The VIF values of all constructs were well below the cut-off of 10 (all VIFs below 2.5), as recommended by previous research (Belsley, Kuh, & Welsch, 1980, p. 93; Hair, Black, Babin, Anderson, & Tatham, 2006, p. 230; Neter, Wasserman, & Kutner, 1989, p. 409). Thus, the full collinearity assessment did not suggest that CMB is a concern in our data.

Table B1. The approaches used in this study to detect and control for common method biases

Techniques	**Actions We Took In Our Study**
Procedural remedies (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003; Schwarz, Rizzuto, Carraher-Wolverton, Roldán, & Barrera-Barrera, 2017)	
Protecting respondent anonymity and reducing evaluation apprehension	We let participants know that their responses would be confidential, assured them that there are no right or wrong answers, and asked them to answer questions as truthfully as possible.
Counterbalancing question order	We randomized the orders of the items within each survey block. In addition, we randomized the survey blocks.
Improving scale items	We used pre-validated reliable items from the literature (please refer to the discussion of measurement).
Provide no explanation, definitions, and examples before measuring items	In order to avoid forcing respondents' attention to the correct construct scope (and as a result creating artificially high internal consistency and scale reliability; aka priming effect), we did not provide any explanation, definitions, or examples for all the constructs measured in our survey.
Not using neutral valence items	We refrained from using items with neutral valence answers to avoid the potential bias caused by item embeddedness.
Statistical remedies	
Harman's single factor test (Podsakoff & Organ, 1986)	The exploratory factor analysis of all the measurement items yielded eleven factors, which explained 71.51% of the data variance. No single factor accounted for the majority of the variance—the factor with the largest variance explained 27.43% of the data variance. Thus, we can conclude that CMB is not a major threat to our findings.
Partial correlation procedures: a. *Partialling out social desirability* (Podsakoff et al., 2003)	We assessed social desirability bias through a short version of the Marlowe–Crowne social desirability scale (Strahan & Gerbasi, 1972). In the analysis, we partialled out the effect of social desirability from the predictor and criterion variables and compared the differences in the partial correlation between the predictor and criterion variables. Results showed that the differences were not significant, suggesting that CMB is not a major concern.
b. *Partialling out a "marker" variable or correlational marker approach* (Lindell & Whitney, 2001; Podsakoff et al., 2003; Rönkkö & Ylitalo, 2011)	Since our survey did not include any item that was designed to be completely unrelated to the constructs, we identified three potential marker variables, all of which were theoretically unrelated to any factor in the model. The first marker variable we used was interpersonal conflict, since (a) it is theoretically unrelated to other constructs; (b) it was weakly correlated with other items in our data ($\bar{x}r = 0.10$); and (c) it was measured in the same fashion as other variables in the model (Rönkkö & Ylitalo, 2011). Results showed that all significant correlations stayed significant after incorporating this marker variable into the partial correlation analysis of the model (Lindell & Whitney, 2001). We also included this marker variable as a control variable in the model and linked it to all endogenous constructs. The difference in the two comparative models, one with the marker variable and the other without this marker variable was minor ($\Delta\beta < .01$). Also, all the significant paths stayed significant, indicating that CMB is not a major issue.
	Following Sarker, Ahuja, and Sarker (2018), we chose both industry, which reflects the industry participants' organization belonged to, and the company's expected annual revenue, the perception of participants about the annual revenue of their company, as the second and third mark variables. We found that the inclusion of the marker variables did not change the pattern of results. Again, all

Techniques	**Actions We Took In Our Study**
	significant correlations stayed significant. Taken together, these results indicated that CMB is not a major issue in our data.
Full Collinearity Assessment Approach (Kock, 2015; Kock & Lynn, 2012)	Following Kock (2015), we conducted full collinearity test and found that all VIFs were lower than 5. Thus, CMB does not appear to be of serious concern in our data.

In summary, to control for the effect of CMB, we followed Schwarz et al. (2017) to identify and test the procedural sources of common method bias, including (a) ambiguous or complex items, (b) format of the scales and choice of scale anchors, (c) negatively worded or reverse coded items, (d) item priming effects, (e) item embeddedness, (f) positive and negative affectivity traits, and (g) transient mood state. Among the mentioned sources of CMB, Schwarz et al. (2017) found four sources, namely ambiguous or complex items, format of the scales and choice of scale anchors, item priming effects, and item embeddedness, have a significant impact on their proposed structural model.

We followed several procedural remedies suggested by Podsakoff et al. (2003) and Mackenzie et al. (2011) and later employed by Bala and Venkatesh (2013). Our remedies overlap with those remedies identified by Schwarz et al. (2017) to reduce the sources of bias for the structural model. For instance, we used established prevalidated reliable items to avoid the source of bias caused by the ambiguity and scale format; we ensured the anonymity of participants and randomized the order of items to mitigate the order effect; also, we did not provide any explanation, definitions, or examples for the constructs used in our survey, avoiding the bias caused by the priming effect; finally, we refrained from using items with neutral valence answers, avoiding the bias caused by item embeddedness.

Later, Schwarz et al. (2017) investigated the effectiveness of the popular techniques in detecting CMB. They mainly focused on (a) Harman's single factor model approach, (b) the CFA marker technique, and (c) the unmeasured latent method factor technique. Similarly, we followed Harman's single factor model approach and found that the exploratory factor analysis of all the measurement items yielded 11 factors, which explained 71.51% of the data variance. No single factor explained the majority of the variance—the factor with the largest variance accounted for 27.43% of the data variance. Thus, we concluded that CMB is not a major threat. This approach has been criticized by its insensitivity and the fact that the lack of one dominant factor does not mean that the data is not contaminated by method bias (Podsakoff et al., 2003). Thus, it is often accompanied by other techniques.

The CFA marker approach is part of partial correlation procedures designed to control for common method biases. Partial correlation procedures include (a) partialling out social desirability, (b) partialling out a “marker” variable, and (c) partialling out a general factor score (Podsakoff et al., 2003). They consider a measure of the assumed source of method variance as a covariate in the statistical analysis. In this study, we partialled out the effect of social desirability from the predictor and criterion variables and compared the differences in the partial correlation between the predictor and criterion variables. The results showed that the differences were not significant, suggesting that CMB is not a major concern (see Table B2).

Partialling out social desirability is limited since it only controls for the portion of CMB that is related to social desirability. Thus, we further employed the “partialling out a marker variable” approach, which is also discussed in Podsakoff et al. (2003) and Schwarz et al. (2017). The basic assumption behind this approach is that if a variable is unrelated to any other constructs in the model, it can be used as a marker variable, and any relationship between the marker variable and other variables can be linked to CMB (Lindell & Whitney, 2001). Thus, partialling out the average correlation between the marker variable and the other variables should remedy the possible effect of CMB. The marker variable technique could not be used in our study in its original form as it is not compatible with PLS (c.f., Rönkkö and Ylitalo (2011) for further discussion). Thus, we followed the guidelines suggested by Rönkkö and Ylitalo (2011) for employing marker variable method (Lindell & Whitney, 2001) in PLS.

Table B2. Partialling out social desirability

Coefficients			
	Without Desirability	**With Desirability**	**Differences**
CC- > COM	0.161	0.168	0.007
SR- > COM	0.407	0.394	−0.013
CC × RUL- > COM	−0.117***	−0.120***	−0.003
CC × SPI- > COM	−0.162***	−0.162***	0.000
SR × RUL- > COM	−0.121***	−0.125***	−0.004
SR × SPI- > COM	−0.145***	−0.146***	−0.001

Coefficients			
	Without Desirability	**With Desirability**	**Differences**
KN- > COM	0.079	0.067	−0.012
Position- > COM	0.05	0.039	−0.011
Age	−0.05	−0.056	−0.006
Info. Related- > COM	0.072	0.083	0.011
Gender- > COM	−0.068	−0.076	−0.008
Info. Intensity- > COM	−0.028	−0.02	0.008
Education- > COM	−0.148	−0.146	0.002
Tenure- > COM	0.087	0.079	−0.008
Race- > COM	0.022	0.028	0.006
Company Size- > COM	−0.044	−0.044	0.000
Fulltime- > COM	−0.07	−0.082	−0.012
Desirability- > COM		0.107	
R^2			
R^2	0.493	0.503	

Abbreviations: COM, ISP compliance behaviour; DB, detection of behaviour; KN, ISP knowledge; LG, legitimacy; RUL, rules-oriented ethical climate; RB, reaction to behaviour; SII: susceptibility to informational influence; SNI, susceptibility to normative influence; VC, value congruence.

*** $P < 0.001$;

** $P < 0.01$;

* $P < 0.5$.

We chose interpersonal conflict as a marker variable since (a) it is theoretically unrelated to other constructs; (b) it is weakly correlated with the other items ($\bar{x}r = 0.10$); and (c) it is measured in the same fashion as other variables in our model (Rönkkö & Ylitalo, 2011). The interpersonal conflict—"*How often do your colleagues at your organization engage in criticizing their coworkers?*" is from Jehn (1995). Following Sarker et al. (2018), we also used industry as another marker variable—the industry to which the participants' organization belonged—as it is expected to be unrelated directly to ISP compliance. Following their approach, we also used a third marker variable, the company's expected annual revenue—the perception of participants about the annual revenue of their company—as a variable that is considered to be unrelated directly to ISP compliance. As reported in Table B3, none of the three marker variables changed the significance of any of the relationships in the model, suggesting that CMB is not a major concern.

Table B3. Partialling out a "marker" variable

Coefficients				
	Base Model	**Marker = Revenue**	**Marker = Industry**	**Marker = Conflict**
CC- > COM	0.168**	0.170**	0.169**	0.172**
SR- > COM	0.394***	0.393***	0.391***	0.379***
CC × RUL- > COM	−0.120***	−0.119**	−0.121***	−0.120**
CC × SPI- > COM	−0.162***	−0.163***	−0.156***	−0.159***
SR × RUL- > COM	−0.125***	−0.124**	−0.122***	−0.132**
SR × SPI- > COM	−0.146***	−0.145**	−0.141***	−0.149**
KN- > COM	0.067	0.065	0.069	0.068
Position- > COM	0.039	0.043	0.039	0.044
Age	−0.056	−0.054	−0.044	−0.063
Info. Related- > COM	0.083	0.078	0.079	0.082
Gender- > COM	−0.076	−0.070	−0.080	−0.077
Info. Intensity- > COM	−0.020	−0.019	−0.031	−0.017
Education- > COM	−0.146**	−0.144**	−0.156**	−0.145**
Tenure- > COM	0.079	0.071	0.080	0.085
Race- > COM	0.028	0.029	0.034	0.031

Coefficients				
	Base Model	**Marker = Revenue**	**Marker = Industry**	**Marker = Conflict**
Company Size- > COM	−0.044	−0.065	−0.046	−0.040
Fulltime- > COM	−0.082	−0.080	−0.075	−0.083
Desirability- > COM	0.107**	0.114**	0.104**	0.102
Marker- > COM		0.054	−0.068	−0.066
R^2				
R^2	0.503	0.505	0.507	0.507

COM: ISP Compliance Behaviour; RUL: Rules-oriented ethical Climate; VC: Value Congruence; LG: Legitimacy; DB: Detection of Behaviour;

RB: Reaction to Behaviour; SII: Susceptibility to Informational Influence; SNI: Susceptibility to Normative Influence; KN: ISP Knowledge.

*** $P < 0.001$;

** $P < 0.01$;

* $P < 0.5$.

Table B4. Full collinearity assessment approach

IV/DV	**COM**	**RUL**	**RB**	**DB**	**VC**	**LG**	**SNI**	**SII**	**KN**
COM		2.0	2.1	2.1	2.1	1.7	2.1	2.1	2.1
RUL	1.9		2.0	2.0	1.8	2.0	2.0	2.0	2.1
RB	1.8	1.8		1.4	1.8	1.9	1.8	1.9	1.9
DB	1.8	1.8	1.4		1.8	1.8	1.7	1.8	1.7
VC	1.6	1.4	1.6	1.6		1.6	1.6	1.6	1.6
LG	1.8	2.3	2.4	2.3	2.2		2.3	2.3	2.3
SNI	1.2	1.2	1.2	1.2	1.2	1.2		1.2	1.3
SII	1.3	1.3	1.3	1.3	1.3	1.3	1.2		1.3
KN	1.1	1.1	1.1	1.1	1.1	1.1	1.1	1.1	

Abbreviations: COM, ISP compliance behaviour; RUL: Rules-oriented ethical Climate; VC: Value Congruence; LG: Legitimacy; DB: Detection of Behaviour; RB: Reaction to Behaviour; SII: Susceptibility to Informational Influence; SNI: Susceptibility to Normative Influence; KN: ISP Knowledge.

We conducted a literature review (see Table C1) to elaborate and establish several of the arguments in our manuscript. The main goal of this review was to identify studies that dealt with extrinsic and/or intrinsic motivations (as conceptualized in or related to our manuscript) and employee security behaviour. In doing so, we agree with Willison, Lowry, et al (2018), and Cram et al. (2019) point that a literature review should be inclusive so that it offers a balanced understanding of phenomenon, here extrinsic and intrinsic motivations, as without considering the whole of the literature, our understanding would be more positively skewed towards the significant results reported in top-tier journals. Our study tries to provide a solution to reconcile the competing results of the command-and-control and self-regulatory approaches. However, the self-regulatory approach in comparison with the command-and-control approach has drawn less attention, to make matters worse, many top-tier peer-reviewed journals do not publish studies with mixed or insignificant results as they expect significant results. As such, the current understanding of this phenomenon may be biased. Given the current state of information security with regards the topic of our study, we also included the conferences and low-tier journals in our literature review (Templier & Paré, 2015).

APPENDIX C

C.1. Literature review

Table C1. Summary of reviewed articles

	Theories	C-C Related Constructs	S-R Related Constructs	Contextual and Dispositional Moderators	Explanation of The Mixed Results (if any)	Mixed Results
Moody et al. (2018)	TN; HBM; TRA; PMT; TIB; GDT; EPMT; TPB; TSR; EPPM; CBT	Deterrents	Role Values		They investigated and compared 11 theories. They integrated elements across these extant theories and proposed a unified model, called it, the unified model of information security policy compliance (UMISPC). They reported that deterrents and rewards were not significant in reducing ISP violations scenarios. Their analysis resulted in debuting moral considerations and social norms as separate constructs. They combined a few items of each construct and proposed a construct called role values. They reported that role values have a significant impact on reducing ISP violations scenarios. They associated the insignificant results of deterrents with the lack of deterrent experience in the context of their scenarios (eg, password sharing) as well as the significant impact of role values.	Yes. (C-C)
Li et al (2018)	RCT	Perceived Deterrence; Perceived Benefits		Self-Control; Procedural Justice	They found that perceived deterrence (combined both perceived certainty and severity of sanctions) as well as perceived benefits, marginally and fully predicts employee intention to comply with the IUP, respectively. They investigated the moderating effect of procedural justice and self-control on the path between perceived deterrence and benefits. They found that none of the moderating variables significantly moderate the relationship between perceived deterrence and IUP compliance intention. However, both variables moderate the effect of perceived benefits and IUP compliance intention. They stated that the effect of perceived benefits could override that of deterrence.	Yes. (C-C)
X. Chen et al (2018)	GDT; DT	Perceived Severity		Perceived Self-Efficacy; Descriptive Norms; Response Cost	They investigated the moderating role of perceived self-efficacy, descriptive norms, and response cost on the relationship between perceived severity of sanctions and employee ISP compliance intention. They found statistical significance for the direct relationship but none of the moderators. Further, they showed that controlling for the investigated variables, the impact of sanction severity on employee ISP compliance intention was disappeared. Finally, they showed that perceived efficacy and descriptive norms mediate the impact of sanction severity on employee ISP compliance intention.	Yes. (C-C)

	Theories	C-C Related Constructs	S-R Related Constructs	Contextual and Dispositional Moderators	Explanation of The Mixed Results (if any)	Mixed Results
H. Chen et al (2018)	SCT; OEC		Moral Disengagement	Organizational Ethical Climate	They showed that moral disengagement predicts intention to violate ISP. Further, they showed that ethical climate moderates the relationship between moral disengagement and ISP violation intention.	No.
Alzahrani et al. (2018)	Determination Theory		Perceived Legitimacy; Perceived Value Congruence		They used the self-determination theory to investigate employee ISP compliance intentions. The found that autonomy, competence, and the concept of relatedness positively impact employee ISP compliance intentions. Further, they found that perceived value congruence had a negative whereas perceived legitimacy had no impact on employee ISP compliance intentions. These results are surprising as the negative effect of value congruence is at odds with previous studies in the literature. Further, unlike the findings of previous studies, perceived legitimacy had no impact on employee ISP compliance intention. They associated their results to the different set of variables in the model compared to previous models and suggested further investigations. Their data was gathered from a 500 fortune company in the Middle East.	Yes. (S-R)
Balozian, Leidner, and Warkentin (2017)	Persuasion Theory; GDT	Sanction Certainty; Sanction Severity		Position (Employee VS Manager)	They found that employee positions (lower vs. higher levels) influence ISP compliance, if each group is prompted by tailored strategies (participating in the ISP decision-making process vs. enhancing the meaningfulness of policy compliance). Further, they showed that severity and certainty of sanctions (termed as coercive approach) do not affect ISP compliance of employees (ie, lower level) and a combination of employees and managers, whereas severity of sanctions is significant in motivating ISP compliance of managers (ie, higher level). They stated that the severity and certainty of sanctions, when tested alone, were significant; however, when tested together with other variables (ie, participation, meaningfulness, express confidence) in the model, lost their significance and power.	Yes. (C-C)
Silic et al. (2017)	GDT NT	Informal & Formal Sanction (Severity & Certainty)	Neutralization; Shame (Severity & Certainty)		They examined the role of shame, neutralization, and deterrence. They found that sanctions did not deter Shadow IT intentions. They found that neutralization (metaphor of the ledger) but not shame is significant in predicting Shadow IT intentions and actual Shadow IT usage. They explained that neutralization reduces the shame that employees feel towards violating Shadow IT policies, making its impact insignificant. Further, they associated the lack of significance for deterrence with their situations where the Shadow IT was viewed with less stigma.	Yes. (C-C) (S-R)

	Theories	C-C Related Constructs	S-R Related Constructs	Contextual and Dispositional Moderators	Explanation of The Mixed Results (if any)	Mixed Results
D'Arcy and Lowry (2019)	RCT; TPB	Computer Monitoring	Moral Beliefs		They investigated cognitive-affective drivers of employee daily ISP compliance. Among many factors, they tested the perceived computer monitoring as a proxy for sanctions and found that it is significant in predicting attitude towards compliance. They also investigated the role of moral beliefs and reported that moral beliefs significantly predict employee daily ISP compliance.	No.
Kim, Park, and Baskerville (2016)	Computer Crime Opportunity Structure; Theory of Emotion Process		Morality		They integrated abuse opportunity structure and emotion process theories and proposed a model to investigate the effects of organizational and individual factors on computer abuse intent. They found that morality, defined as a trigger of internal regulation, and abuse-positive affect, which refers to pleasant-activated feelings, has a significant negative effect on abuse intent.	No.
Son and Park (2016)	PJT	Deterrent Severity; Deterrent Certainty	Moral Commitment; Procedural Justice	Privacy Concerns	They investigated and found that procedural justice, the belief that the organization is fair in rules creation and implementation, contributes to employee willingness to comply with non-work-related computing (NWRC) rules. In their analysis, they controlled for moral commitment and certainty and severity of sanctions. Among these, only perceived certainty of sanctions found to be significant. Surprisingly, moral commitment was not significant. They also found that privacy concerns weaken the impact of procedural justice belief on compliance intention.	Yes. (C-C) (S-R)
Yazdanmehr and Wang (2016)	Norma Activation Theory; Social Norms Theory	Deterrence	Personal Norms	Ascription of Personal Responsibility: Awareness of Consequence	They test the role of personal norms in predicting ISP compliance behaviour. They found that personal norms predict employee ISP compliance, and its effect is moderated by ascription of personal responsibility but not awareness of consequences. They controlled for the deterrence, the combination of perceived certainty and severity of sanctions, and found that it predicts the employee ISP compliance.	No.
finedo (2016)	GDT RCT	Sanction Severity; Detection Probability			They found that perceived severity but not perceived detection of sanctions predicts ISP behavioural intention. They associated their insignificant results with the research design and possible other contextual or extraneous influences (such as neutralization techniques).	Yes. (C-C)
Johnston et al. (2016)	PMT GDT	Sanction Perception (Sanction Severity & Certainly)		Stability & Plasticity Meta-Traits	They examined general deterrence and protection motivation factors in predicting ISP violation intentions. They found that threat vulnerability, sanction severity, and sanction certainty are significant predictors of policy violation intentions. They investigated the moderating effects of dispositional factors (stability and plasticity) on the path between threat and coping appraisals as well as sanction perceptions on ISP violation	No.

	Theories	C-C Related Constructs	S-R Related Constructs	Contextual and Dispositional Moderators	Explanation of The Mixed Results (if any)	Mixed Results
					intentions. They found that employees with higher stability meta-trait are more sensitive than average ones to threat vulnerability as well as to both severity and certainty of sanctions. They showed that the moderating effect of plasticity meta-trait is mixed such that it does not moderate the effect of threat, self-efficacy, and sanction severity, whereas it moderates the effect of response efficacy and sanction certainty.	
Foth (2016)	GDT TPB	Detection Certainty Punishment Severity			He extended the model of TPB and GDT by adding the gender variable to the model. He investigated the role of attitudes, subjective norms, and perceived behavioural control on employee intentions to comply with data protection regulations. He found that above-mentioned variables are significant in predicting compliance intentions. He included the deterrence elements and found that certainty of detection (but not severity of punishment) predicts employee compliance intention. Also, he found a significant difference between the genders in compliance intention.	Yes. (C-C)
Bansal, Green, Hodorff, and Marshall (2016)	Prospect Theory	Moral Beliefs		Gender	They showed that moral beliefs and understandability of ISP significantly lower employee ISP violation intentions. In addition, they found that gender moderates the relationship between understandability of ISP and employee ISP violation intentions. In their post-hoc analysis, they showed that the moderation effect of gender itself is contingent upon the underlying neutralization scenario such that for both neutralization scenarios together gender did not moderate the relationship between the impact of moral beliefs and employee ISP violation intentions. However, for one scenario (ie, necessity), the moderating effect of gender was not significant. And, for the other scenario (ie, metaphor of the ledger), the effect of moral beliefs and understandability were significant only for females.	Yes. (S-R)
Li et al. (2014)	Organizational justice	Sanction Certainty; Sanction Severity	Personal Ethics		They integrated the intrinsic self-regulatory approach with an extrinsic sanction-based command-and-control approach to evaluating employee IUP compliance intention. They found that perceived certainty but not severity of sanctions significantly predicts employee IUP compliance intention. They found that personal norms (referred to as personal ethics) are more effective than the sanction-based command-and-control approach in encouraging employee IUP compliance intention. They stated that the possible reason for the insignificance of perceived severity of sanctions was because the employees might not have perceived the sanctions for internet abuses to be severe.	Yes. (C-C)

	Theories	C-C Related Constructs	S-R Related Constructs	Contextual and Dispositional Moderators	Explanation of The Mixed Results (if any)	Mixed Results
Ifinedo (2014)	TPB; SCT; SBT	Detection Probability; Sanction Severity	Personal Norms		He found that perceived certainty and severity of sanctions do not predict ISP compliance intentions, whereas subjective norms do so. They found that attitude towards ISP compliance (which is predicted by personal norms, attachment, commitment, and involvement) is significant in predicting ISP compliance intentions.	Yes. (C-C)
Cheng et al. (2013)	DT; Social Control Theory	Perceived Certainty; Perceived Severity	Belief		They found that severity of sanctions but not certainty of detections significantly predict employee ISP violation intentions. Also, they found that belief was negatively related to employee ISP violation intentions. They associated the insignificant results of certainty of detections with the context of their scenarios (eg, leaving workstations without logging out) in which the sanction may not be perceived to be relevant.	Yes. (C-C)
Barlow, Warkentin, Ormond, and Dennis (2013)	GDT; NT	Communication of Deterrent Sanctions	Defence of Necessity; Denial of Injury; Metaphor of The Ledger		They tested the neutralization techniques as well as deterrent sanctions together in the same model. They found that deterrent sanctions are significant in reducing IT policy violation. In addition, they found that convincing employees to not using neutralization would lower IT policy violations and be as strong as providing information about deterrent sanctions. They showed that some neutralization types (ie, defence of necessity) might be more powerful than others (denial of injury and metaphor of the ledger), depending on the circumstances.	No.
D'Arcy and Devaraj (2012)	GDT	Deterrence	Moral Beliefs	Employment Level	Using scenarios, they found that deterrence (severity and certainty of sanctions) is significant in both directly and indirectly deterring technology misuse intention. They found moral beliefs and a predisposition towards the need for social approval are significant in reducing technology misuse intention. They argued that anticipated feelings of social and self-disapproval are critical considerations involving technology misuse decision-making process. They showed that employment level moderates effect of perceptions of the punishment on technology misuse	No.
Y. Chen et al. (2012)	Compliance Theory; GDT	Severity of Punishment; Certainty of Control			They found that severity of punishment, significance of reward, and certainty of control were all significant in deterring employees from security policy violation. They highlighted that reward enforcement could be an alternative for organizations where sanctions do not successfully prevent violations.	No.
Guo and Yuan (2012)	Organizational Sanctions	Organizational Sanctions	Personal Self-Sanctions		Workgroup sanctions but not organizational sanctions significantly reduce employee security violations. The effect of personal self-sanctions was significant in reducing employee security violations. They found that the effect of organizational sanctions becomes insignificant when self-sanctions and workgroup sanctions were included in the model.	Yes. (C-C)

	Theories	C-C Related Constructs	S-R Related Constructs	Contextual and Dispositional Moderators	Explanation of The Mixed Results (if any)	Mixed Results
Hu, Dinev, Hart, and Cooke (2012)	TPB		Individual Beliefs		They found that employee cognitive beliefs about compliance with ISP fully mediates the relationship between the top management participation and organizational culture and employee behavioural intentions. In addition, they found that top management participation in information security initiatives significantly (directly and indirectly) predicts an employees' attitudes towards, subjective norm of, and perceived behavioural control over compliance with ISP. Moreover, they found that the top management participation impacts organizational culture which in turn influences employees' attitudes towards and perceived behavioural control over ISP compliance.	No.
Hovav and D'Arcy (2012)	GDT	Certainty of Detection; Severity of Sanctions	Moral Beliefs	National Culture	They examined the effect of perceived certainty of detection and severity of sanctions in the United States and South Korea. They showed that moral belief has a significant negative impact on IS misuse intention for both samples. They investigated the moderating role of culture on the path between deterrence and IS misuse intention. They found that certainty of detection but not severity of sanctions was significant in reducing IS misuse intention for the US participants, whereas the results were opposite for the South Korean participants. They associated the disparity of their results to the cultural differences between two countries.	Yes. (C-C)
Vance and Siponen (2012)	RCT	Informal & Formal Sanction (Severity & Certainty)	Moral Beliefs		Their results suggested that formal sanctions (such as penalties) and informal sanctions (such as lost respect in the eyes of management and coworkers) do not deter employee ISP violation intentions. They found that moral beliefs are an excellent predictor of ISP violation intentions. They justified that the insignificant results may be due to the fact that employees perceive penalties and lack of respect to be minor issues.	Yes. (C-C)
Guo, Yuan, Archer, and Connelly (2011)	Composite Behaviour Model	Perceived Sanctions (Combination of Certainty & Severity of Sanctions)			They found that perceived sanctions (combining both certainty and severity of sanctions) were not significant in predicting the attitude towards non-malicious security violation intentions, which itself predicting non-malicious security violation intentions. They reasoned that since end-users are usually evaluated on their job performance but not on the level of compliance with the ISP, deterrence theory might not provide enough evidence about non-malicious security violation intentions.	Yes. (C-C)
Son (2011)	GDT, Intrinsic & Extrinsic Motivation Models	Certainty of Sanctions; Severity of Sanctions	Legitimacy; Value Congruence		He found that both certainty and severity of sanctions are not significant in predicting actual ISP compliance. He found that perceived legitimacy and value congruence are significant in predicting actual ISP compliance. He	Yes. (C-C)

	Theories	C-C Related Constructs	S-R Related Constructs	Contextual and Dispositional Moderators	Explanation of The Mixed Results (if any)	Mixed Results
					stated that the results are consistent with those in many studies that have used GDT.	
Hu et al. (2011)	GDT; RCT; Self-Control Theory	Certainty, Severity, Celerity Of Sanctions (As A Second-Ordered Formative Construct)	Moral Belief		They tested the effect of perceived certainty, severity, and celerity of sanctions both directly and indirectly on the intention to commit computer misconduct using two separate models. They found that perceived certainty, severity, and celerity of sanctions (as a second-ordered formative construct) were insignificant in predicting employee intention to commit computer misconduct, whereas they were significant on predicting the perceived formal and informal risks, which themselves predicted intention to commit computer misconduct. They showed that employees with strong moral beliefs are less likely to commit computer misconduct even if the chance of conducting such acts are present. They argued that their insignificant results of general deterrence variables are due to the fact that offenders may mainly think about positive consequences and little about the negative consequences of computer misconducts.	Yes. (C-C)
Li et al. (2010)	RCT	Detection Probability; Sanction Severity	Personal Norms		They found that detection probability but not sanction severity predict IUP intention. Also. they found that personal norms significantly predict IUP intention. They tested the effect of personal norms in moderating the effect of deterrence components and explained that for those with very low personal norms, perceived sanction severity is significant whereas, for those with high personal norms, severe sanctions may erode the trust or loyalty towards a firm, causing hostility towards compliance intention.	Yes. (C-C)
Siponen et al. (2010)	PMT; GDT; TRA; INT	Deterrences			They found that deterrences (combination of perceived certainty, severity, and celerity) but not rewards predict employee ISP compliance.	No.
Siponen and Vance (2010)	NT; GDT	Informal & Formal Sanction (Severity & Certainty)	Neutralization; Shame		They found that formal and informal sanctions were not significant in explaining intention to violate the ISP. In addition, they showed that neutralization but not shame predicts intention to violate the ISP. They stated that the effects of formal sanctions, informal sanctions, and shame were overshadowed by employee neutralization technique.	Yes. (C-C) (S-R)
D'Arcy et al. (2009)	GDT	Severity of Sanctions; Certainty of Detection	Moral Commitment		They found that the severity of sanctions, but not certainty of detection, significantly impact employee IS misuse intention. They found that moral commitment, as a control variable, to have a significant relationship with IS misuse intention. They associated the insignificant results of certainty of sanctions with the fact that in the context of their scenarios (eg, password sharing), sanctions may not be perceived to be relevant. Further, in their post-hoc analysis, they hinted the possible role of moral commitment in	Yes. (C-C)

	Theories	C-C Related Constructs	S-R Related Constructs	Contextual and Dispositional Moderators	Explanation of The Mixed Results (if any)	Mixed Results
					influencing the effect of perceived certainty of detection and severity of punishments; Such that, those with high moral commitment may be more susceptible to sanctions regardless of the punishment, whereas those with low moral commitment may be more concerned with the punishments resulted from their wrongdoings.	
Herath and Rao (2009a)	GDT; Agency Theory	Severity of Penalty; Certainly of Detection			In two separate studies, they showed that perceived certainty of detection, but not severity of sanctions, predicts employee ISP compliance intention. In fact, they found that severity of sanctions has a negative impact on ISP compliance intention. Herath and Rao (2009a) suggested that sanctions may result in hostilities, disrupting the cooperation that they impose. They pointed out that their mixed results may be due to the fact that employees do not take the penalties seriously or think penalties do not apply to them. Herath and Rao (2009b) have not provided any insights into the insignificant results.	Yes. (C-C)
Herath and Rao (2009b)	GDT; PMT	Punishment Severity; Detection Certainty				Yes. (C-C)
Myyry et al. (2009)	Theory of Cognitive Moral Development; Theory of Motivational Types of Values		Moral Reasoning (Preconventional, Conventional &, Postconventional reasoning) Moral Values (Openness to change & Conservation)		They integrated the theory of cognitive moral development and the theory of motivational types of values to propose a model. They examined the influence of moral reasoning and values on compliance with ISP. They found that moral reasoning (Preconventional) and moral values (Openness to change) significantly predict both hypothetical and actual ISP compliance.	No.
	Health					

Abbreviations: CBT, control balance theory; C-C, the command-and-control approach; DT, deterrability theory; EPMT, extended protection motivation theory; EPPM, extended parallel processing model; GDT, general deterrence theory; HBM, health belief model; INT, innovation diffusion theory; OEC, organization ethical climate theory; PJT, procedural justice theory; PMT, protection motivation theory; RCT, rational choice theory; SCT, social cognition theory; SPT, social bond theory; S-R, the self-regulatory approach; TIB, theory of interpersonal behaviour; TN, techniques of neutralization; TPB, theory of planned behaviour; TRA, theory of reasoned action; TSR, theory of self-regulation.

We used several article repositories namely EBSCO, Web of Science, AIS Library, and Google Scholar to find the relevant articles. We used the following search terms (deterrence, deterrence theory, deterrent, general deterrence theory, the command-and-control approach, the self-regulatory approach, severity of sanctions, severity of punishments, certainty of detection, monitoring, reaction to behaviour, detection of behaviour, shame, morality, moral values, moral commitment, personal norms, personal ethics, perceived legitimacy, and value congruence, AND "information security, information security policy, information security policy compliance, information security policy noncompliance, information security policy violations, and information security misuse." We limited our search to the past decade (2009-2018). We only included empirical studies and excluded the conceptual pieces. We included studies that incorporated exact or conceptually similar elements of the command-and-control or the self-regulatory approach in their model, regardless of the theory or whether these elements were central focus or control variables. The summary of the articles is provided in Table C1. We also summarized our observation of the possible reason that previous studies regarding the command-and-control and the self-regulatory approaches are inconclusive.

C.2. Summary of literature

C.2.1. Evidence and sources of the command-and-control approach mixed results

It has been suggested that studies using general deterrence theory (GDT) (or its elements) enjoyed quite mixed results (cf, D'Arcy & Herath, 2011; Willison, Lowry, et al, 2018). The mixed results often have been related to several factors such as the extent and variety of constructs that have been considered alongside GDT elements. These variables are mostly related to intrinsic motivations, as they have been shown to have better prediction power, overriding the effect of GDT elements in the model. These variables were presented as personal personal self-sanctions, norms, ethics (Guo & Yuan, 2012; Li et al., 2014, 2010; Yazdanmehr & Wang, 2016), moral beliefs (Cheng, Li, Li, Holm, & Zhai, 2013; D'Arcy & Devaraj, 2012; Hovav & D'Arcy, 2012; Hu et al., 2011; Ifinedo, 2014; Vance & Siponen, 2012), moral commitment (D'Arcy, Hovav, & Galletta, 2009; Son & Park, 2016), shame and neutralization techniques (Silic, Barlow, & Back, 2017; Siponen & Vance, 2010), and self-regulatory approach (Li et al., 2014; Son, 2011). The common cited reason regarding the insignificant results of GDT is the context of the study, in which ISP violations are not perceived seriously (Cheng et al., 2013; Herath & Rao, 2009a; Hu et al., 2011; Li et al., 2014; Moody, Siponen, & Pahnila, 2018; Vance & Siponen, 2012). For instance, it has been suggested that sharing password or leaving workstations without logging out often perceived as minor violations that do not warrant severe punishments (Cheng et al., 2013; Moody et al., 2018). In the same vein, it has been suggested that the mixed results are due to the lack of investigating dispositional and contextual moderating variables (D'Arcy & Herath, 2011). Following this suggestion, for instance, in a recent effort to consolidate these mixed results, Chen et al (2018) investigated the moderating roles of perceived self-efficacy, descriptive norms, and response cost on the path between deterrence (ie, perceived severity of sanctions) and employee ISP compliance intention. However, their effort was inconclusive as none of the variables examined in their study moderated this path. In another study, Hovav and D'Arcy (2012) examined the role of cultural differences in the effectiveness of deterrence on reducing IS misuse intention and found inconsistency in the effect of deterrence between South Koreans and Americans.

C.2.2. Evidence and sources of the self-regulatory approach mixed results

Intrinsic motivations (sometimes referred to as informal sanctions, cf, Siponen & Vance, 2010) are based on the assessment of how carrying out the task provides feeling of contentment (Ryan & Deci, 2000), suggesting that the reward is in engaging in tasks itself, and the punishment is self-imposed, whereas the self-imposed costs often include moral beliefs, moral commitments, and/or shame (Hsu, Shis, & Lowry, 2015; Nagin & Paternoster, 1993). In comparison with extrinsic motivations, they have drawn less attention. Many studies have reported intrinsic motivations significantly predict employee compliance behaviour; however, there are studies that reported mixed results.

For instance, perceived legitimacy and value congruence have been shown to be significant in motivating employee ISP compliance (Son, 2011). However, Alzahrani, Johnson, and Altamimi, (2018) have included the perceived value congruence and legitimacy in their investigation of the role of self-determination theory in encouraging ISP compliance intentions. They found that value congruence had an unexpected negative impact on employee ISP compliance intention, whereas perceived legitimacy had no impact on employee ISP compliance intentions. These studies have not provided any specific reasoning for their insignificant results.

In other instances, the effect shame, which refers to the feeling of guilt or embarrassment as if others know one's socially unacceptable actions (Paternoster & Simpson, 1996), on employee ISP violations has been shown to be inconclusive. Siponen and Vance (2010) have shown that shame is ineffective in deterring employee ISP violation intentions. They associated the insignificant effect of shame with the significant effect of neutralization, overshadowing the effect of shame. Moral beliefs, moral commitment, personal norms, and personal self-sanctions in most cases have been shown to predict employee ISP and IUP compliance (D'Arcy & Lowry, 2019; Li et al., 2014, 2010; Yazdanmehr & Wang, 2016), and ISP misuse and ISP violation intentions (D'Arcy et al., 2009; D'Arcy & Devaraj, 2012; Guo & Yuan, 2012; Hovav & D'Arcy, 2012; Hu et al., 2011; Vance & Siponen, 2012). However, in a recent study done by Son and Park (2016), moral commitment (measured using the scale adopted form D'Arcy et al., 2009) was shown to be insignificant in predicting employee ISP compliance. Surprisingly, there are not well-accepted explanations regarding the mixed results of intrinsic motives. However, it has been suggested that the effect of intrinsic motives on (un)ethical behaviour can be moderated by contextual and dispositional factors (Ferrell & Gresham, 1985; Jones, 1991; Trevino, 1986).

Intrinsic motives have also been studied through the lens of moral disengagement (D'Arcy et al., 2014) or neutralization (Siponen & Vance, 2010). There are a few studies that investigated and confirmed the contributing role of moral disengagement mechanisms 6 (Bandura, 1999) in ISP violation intentions (Chen, Wu, et al., 2018; D'Arcy et al., 2014; Herath, Yim, D'Arcy, Nam, & Rao, 2018). Moral disengagement mechanisms have been suggested to be susceptible to contextual factors (Batson & Thompson, 2001; Moore et al., 2012). Thus, they may be facilitated under certain situations (eg, work environment with high uncertainty) (D'Arcy et al., 2014; Shu, Gino, & Bazerman, 2011). Indeed, it has been suggested that differences in contextual factors such as organizational culture are the salient drivers of moral disengagement on employee ISP violation intentions (Herath et al., 2018). Neutralization 7 is noted to be conceptually similar to the theory of moral disengagement by both criminology (Clarke, 1997) and information security (Willison & Warkentin, 2013) researchers. It allows potential violators to ignore the pressure of personal norms (Sykes & Matza, 1957), enabling them to violate the ISP without experiencing any guilt or shame (Willison, Warkentin, & Johnston, 2018). Similar to moral disengagement mechanisms, it has been argued that social or situational stimulus must be present in order to prompt individuals to engage in the neutralization techniques (Barlow, Warkentin, Ormond, & Dennis, 2018; Hinduja, 2007; Willison & Warkentin, 2013; Willison, Warkentin, et al, 2018). Altogether, reviewing the past studies hint to the notion that contextual and dispositional factors are important enablers or disablers of intrinsic motives on employee ISP compliance. However, there is not much effort in investigating such factors, in particular from social influence perspective.

APPENDIX D

Statistical significance of any tested hypothesis is influenced by various factors such as sample size, number of indicators, and the variance of indicators (eg, Chin, 1998). The sample size of 246 should be adequate following the guidelines of Falk and Miller (1992) that suggest a 5:1 ratio of cases to the maximum number of manifest indicators in any single block of the model is reasonable. By their guidelines, our sample size requirement should be at least 165 (33 indicators times 5). Our sample size of 246 exceeds this threshold. The sample size was adequate to detect the significance of all hypotheses tested in this study. However, interaction hypotheses (H3-H6) were not as large as the direct hypotheses (H1-H2). It should be noted that a larger sample size might provide more statistical power and performance, in particular for moderating paths.

Prior to running the study, we decided to achieve the power of 0.80 for detecting a medium to large effect size ($f_2 \geq 0.05$) at α= .05 in a multiple regression. Using G*Power, we estimated the sample size required to achieve this power and found the required sample size is 159. After conducting the study, however, we found that the lowest effect size (0.04), due to the moderation hypothesis H3. To detect a smaller moderation effect, a larger sample size is needed (Carte & Russell, 2003). Using G*Power, we estimated that a sample size of 246 provides only 0.88 power to detect the effect of 0.03 at α = .05. However, our sample size can provide 0.94 power to detect an effect of 0.05 at α = .05 or.97 power to detect an effect of 0.06 at α = .05.

APPENDIX E

Normality is a requirement of SEM. Table E1 provides the descriptive statistics of the main variables used in our study. The skewness test of the variables along with visual inspection of the variable histograms suggests that most of our latent variables are rather skewed. The skewness and kurtosis range from −1 to +1 is considered acceptable. However, skewness and kurtosis values of some of our latent variables are not within the acceptable range. Further, the Kolmogorov-Smirnov (KS) test for normality, which has been suggested for small sample sizes (Lilliefors, 1967), showed that none of the KS statistics significances was greater than 0.05, indicating the distribution of variables was not normal. Departures from normality, theoretically, weaken the strength of SEM analysis. However, Hair, Black, and Babin (2010) stated that such a departure is not a major issue when sample sizes are greater than 200. Further, it has been suggested that PLS analysis is robust against departures from normality (Gefen et al., 2000; Goodhue, Lewis, & Thompson, 2012).

Table E1. Variable distribution

	COM	RUL	RB	DB	VC	LG	SII	SNI
Mean	6.065	5.573	4.978	5.440	5.380	5.864	4.480	4.472
Min	2	1	1	1.667	1	1	1	1
Max	7	7	7	7	7	7	7	7
Std. Deviation	.910	1.150	1.407	1.173	1.250	.892	1.602	1.613
Skewness	−.943	−.975	−.429	−.690	−1.254	−1.123	−.347	−.516
Kurtosis	.892	.876	−.312	−.069	1.659	2.925	−.685	−.455

Abbreviations: COM, ISP compliance behaviour; DB, detection of behaviour; LG, legitimacy; RB, reaction to behaviour; RUL, rules-oriented ethical climate; SII, susceptibility to informational influence; SNI, susceptibility to normative influence; VC, value congruence.

Table E2. Kolmogorov-Smirnov* test

	Statistic	*df*	Sig.**
COM	.152	246	.000
RUL	.165	246	.000
DB	.146	246	.000
RB	.104	246	.000
VC	.154	246	.000
LG	.120	246	.000
SII	.091	246	.000
SNI	.088	246	.000

Abbreviations: COM, ISP compliance behaviour; DB, detection of behaviour; LG, legitimacy; RB, reaction to behaviour; RUL, rules-oriented ethical climate; SII, susceptibility to informational influence; SNI, susceptibility to normative influence; VC, value congruence.

* Lilliefors significance correction.

** Significance values greater.05 indicate normal distribution.

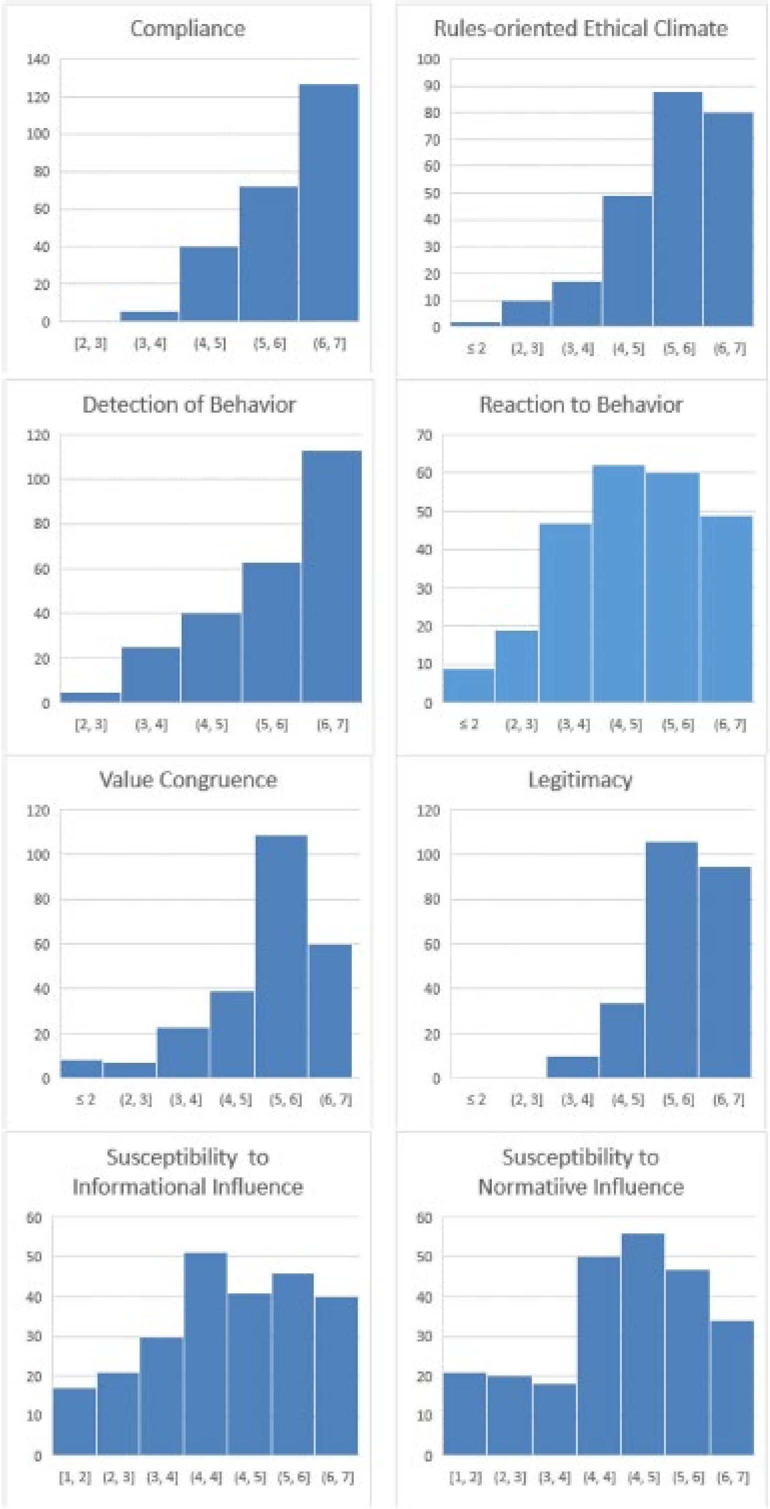


Figure E1. Variable distribution histograms