Ethical leadership and employee information security policy (ISP) violation: exploring dual-mediation paths

Botong Xue and Feng Xu
Mississippi State University, Mississippi State, Mississippi, USA
Xin Luo
The University of New Mexico, Albuquerque, New Mexico, USA, and
Merrill Warkentin
Mississippi State University, Mississippi State, Mississippi, USA

Received 16 February 2021
Revised 30 April 2021
13 June 2021
Accepted 16 June 2021

Abstract

Purpose – A growing number of studies have investigated the effect of ethical leadership on behavioral outcome of employees. However, considering the important role of ethics in IS security, the security literature lacks a theoretical and empirical investigation of the relationship between ethical leadership and employees' security behavior, such as information security policy (ISP) violation. Drawing on social learning and social exchange theories, this paper empirically tests the impact of ethical leadership on employees' ISP violation intention through both information security climate (i.e. from a moral manager's perspective) and affective commitment (i.e. from a moral person's perspective).

Design/methodology/approach – The research was developed based on social learning theory and social exchange theory. To measure the variables in the model, the authors used and adapted measurement items from previous studies. The authors conducted a scenario-based survey with 339 valid responses to test and validate the research model.

Findings – Results indicated that information security climate fully mediates the relationship between ethical leadership and ISP violation intention. The authors also found that information security climate enhances the negative effect of affective commitment on ISP violation intention.

Originality/value – This research contributes to the literature of information security by introducing the role of ethical leadership and integrating two theories into our research model. This study also calls attention to how information security climate and affective commitment mediate the relationship between ethical leadership and employees' ISP violation intention. The theory-driven study provides important pragmatic guidance for enhancing the understanding of the importance of ethical leadership in information systems security research.

Keywords Ethical leadership, ISP violation intention, Information security climate, Affective commitment, Insider threat

Paper type Research paper

1. Introduction

Mitigating security threats and safeguarding information security has become an important organizational strategic agenda. Among a variety of security threats, employees' information security policy (ISP) violation has been deemed to be a major concern to organizations (Chen *et al.*, 2021; Luo *et al.*, 2020; Moody *et al.*, 2018; Siponen and Vance, 2010). Academics and

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 1 No. 1, 2021
pp. 5-23
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-02-2021-0002

practitioners have recognized the significant negative outcomes of employees' ISP violation behavior. Employees' security policy violations might result in significant financial losses caused by security breaches, privacy violations, legal liabilities and the like (Cheng *et al.*, 2013; Chu *et al.*, 2015). According to the Data Breach Investigations Report 2020, more than 32,000 information security incidents have occurred in over 81 countries, with 28% of them involving organizational insiders (Verizon, 2020). Worse yet, according to PWC (2018), insider incidents across industries cost an average of 8.76m US dollars.

To address concerns about insider threats, previous security research has identified a variety of antecedents to employees' ISP compliance or violation behavior (Bulgurcu *et al.*, 2010; D'Arcy *et al.*, 2009; Johnston and Warkentin, 2010; Mutchler and Warkentin, 2020; Siponen and Vance, 2010; Warkentin and Willison, 2009; Lin and Luo, 2021; Li *et al.*, 2021; Ho and Warkentin, 2017). Among these antecedents, ethics or moral-related factors, such as moral beliefs, ethical climate and employees' personal ethics (Li *et al.*, 2014; Siponen *et al.*, 2012), have been considered significant in influencing employees' security behaviors. Due to the critical role of organizational ethics or morality in affecting employees' security behaviors, managers must exemplify ethics for employees to anchor the issue of information security in the organization (Feng *et al.*, 2019). However, the aspect of managers' ethics has received relatively scarce attention in IS security research.

To advance this line of research, this study aims to investigate the role of a specific leadership dimension – ethical leadership – in influencing employees' ISP violation. Previous studies have empirically examined the impact of ethical leadership on a variety of employees behaviors, such as deviant behavior (Mo and Shi, 2017; Resick *et al.*, 2013), employee misconduct (Mayer *et al.*, 2010), unethical behavior (Moore *et al.*, 2019; Schaubroeck *et al.*, 2012), citizenship behavior (Newman *et al.*, 2014) and ethical behavior (Huang and Paterson, 2017; Lu and Lin, 2014). The mediating factors influencing the underlying mechanism between ethical leadership and employees' workplace behaviors have been identified, including trust (Mo and Shi, 2017; Newman *et al.*, 2014), justice (Walumbwa *et al.*, 2017) and ethical climate or ethical culture (Demirtas and Akdogan, 2015; Huang and Paterson, 2017; Lu and Lin, 2014; Schaubroeck *et al.*, 2012). Taken together, we conjecture that ethical leadership can influence employees' security behaviors by promoting appropriate and ethical conduct through personal actions and interpersonal relationships in the workplace.

Conceptualized as "the demonstration of normatively appropriate conduct through personal actions and interpersonal relationships, and the promotion of such conduct to followers through two-way communication, reinforcement, and decision-making" (Brown *et al.*, 2005, p. 120), *ethical leadership* subsumes two dimensions to influence employees' behaviors: a moral person and a moral manager. In essence, a moral person who is honest, trustworthy, caring and concerned for employees has been found to be more associated with employees' positive work attitudes, such as satisfaction and commitment (Brown and Treviño, 2006; Neves and Story, 2015), whereas a moral manager who promotes principles through communications, rewards and punishments is more related to external regulations, such as controlled motivation (Bavik *et al.*, 2018) and procedural justice (Newman *et al.*, 2014).

Grounded in the social learning theory and the social exchange theory, this paper is an early attempt to explore the influence of ethical leadership on employees' ISP violation intention through two mediation mechanisms. Our study makes several theoretical and practical contributions. First, this paper contributes to ethical leadership and IS security research. We conducted an empirical study to investigate the influence of ethical leadership on employees' ISP violation intention. Although ethics-related factors have been studied, this research is one of the first studies to gauge the influence of ethical leadership on employees' ISP-related behavior. Second, embracing the theoretical lenses of the social learning theory and the social exchange theory, this study identifies information security climate and

organizational affective commitment as two critical mediators that influence the relationship between ethical leadership and employees' ISP violation intention. Investigating the role of ethical leadership in the context of information security provides important insights into how to effectively manage employees' information security behaviors and significantly improves organizational information security performance.

2. Theoretical framework and hypothesis development

2.1 ISP violation and ethical leadership

Employee engagement in ISP violation, as a specific organizational deviant behavior, has been identified as one of the major issues leading to security incidents. Previous studies have identified a variety of individual and organizational factors that influence employees' ISP violation or compliance behavior, such as fear appeals and sanction (Herath and Rao, 2009; Johnston *et al.*, 2015; Li *et al.*, 2014; Wall and Warkentin, 2019), neutralization (Siponen and Vance, 2010; Trinkle *et al.*, 2021), security-related stress (D'Arcy *et al.*, 2014), moral beliefs (Siponen *et al.*, 2012), personal ethics (Li *et al.*, 2014), top management and leadership (Hu *et al.*, 2012; Guhr *et al.*, 2019; Feng *et al.*, 2019), and organizational justice (Willison *et al.*, 2018; Xu *et al.*, 2019; Ormond *et al.*, 2019). Among these factors, explaining the influence of management leadership on employees' security behavior has become an important focus in IS security research.

Previous research has identified the paramount role of ethics in affecting employees' security behaviors. For example, Li *et al.* (2014) found that personal ethics significantly improve user's Internet usage policy compliance intention. Vance *et al.* (2020) suggested that moral beliefs negatively influence employees' ISP violation. Given the significance of ethics in IS security, managers should be able to promote ethics to individual employees to increase employees' ISP compliance behavior. However, as an essential component of ethical leaders, ethical leadership has not been well investigated in IS security research.

The role of ethical leadership in influencing employees' behaviors has been investigated in previous leadership or organizational behavior research (Bavik *et al.*, 2018; Gerpott *et al.*, 2019; Kacmar *et al.*, 2011; Lu and Lin, 2014; Mo and Shi, 2017; Neubert *et al.*, 2009; van Gils *et al.*, 2015; Wang and Sung, 2016; Zhu *et al.*, 2004). For example, Mo and Shi (2017) found a negative effect of ethical leadership on employees' deviant behavior, and Resick *et al.* (2013) studied the effects of ethical leadership on deviant behavior and organizational citizenship behavior (OCB). Other research has sought to enhance the understanding of ethical leadership through a focus on specific behaviors. For example, Bavik *et al.* (2018) examined how ethical leadership influences employees' knowledge sharing behavior. The authors found that the relationship is mediated by moral identity and control motivation. Cheng *et al.* (2019) investigated the mediation effect of perception of organizational politics on the relationship between ethical leadership and Internet whistleblowing.

Although previous research has identified a variety of behavioral outcomes associated with ethical leadership, the relationship between ethical leadership and information security behavior has not been thoroughly investigated. Based on the social learning theory and the social exchange theory, we seek to identify the mechanisms of how ethical leadership influences employees' ISP violation intention through two separate paths. The research model and hypothesized relationships among constructs are shown in Figure 1.

There are two important pillars consisting of the role of ethical leadership, including conceptualizing an ethical leader as a moral person and a moral manager (Treviño *et al.*, 2000). A moral person is a leader who can be trusted and who will make decisions in a fair and balanced way, while a moral manager is a leader who frequently conveys ethics to employees through two-way communication and disciplines unethical behaviors (Treviño *et al.*, 2000).

In the following section, we presented the development of hypotheses based on the previous literature and discuss the roles of a moral person and moral manager separately.

2.2 A moral manager: the mediating role of information security climate

A leader has been identified as a person who is influential and trustworthy among the organization and an effective role model for employees. As a moral manager, an ethical leader could perform a reward and punishment action aligned with his/her moral principles to regulate and influence employees' behaviors (Brown *et al.*, 2005). Social learning theory suggested that individuals will be influenced by the role models and learn which behaviors are appropriate and acceptable (Bandura, 1977). In the organization, employees will perform and behave by observing behaviors from the role model and learn from people who are influential and creditworthy. Social learning theory also suggests that employees can learn by direct or vicarious experience with the consequences of their actions (Manz and Sims Jr, 1981). Employees might experience their own punishment or witness their coworkers' actions being punished for violating organizational policy (Bandura, 1977). The corresponding rewards or punishments in the organization can form a shared work climate that highlights the appropriate and acceptable behaviors in the organization and then influence employees' workplace behaviors.

According to the social learning theory, pertaining research has suggested a positive relationship between ethical leadership and employees' perception of ethical climate (Mayer *et al.*, 2010) and ethical culture (Schaubroeck *et al.*, 2012). In the information security context, information security climate is defined as "employees" perception of the current organizational state in terms of information security as evidenced through dealings with internal and external stakeholders" (Chan *et al.*, 2005) (p. 25), where the more emphasis and attention related to information security in the organization is perceived by employees, the stronger information security climate will be. As the authorized party in the organization, the leader can perform the punishment and reward action toward the employee based on the established ISP to regulate the employees' ISP compliance behavior (Lebek *et al.*, 2014). By observing and witnessing the rewards and punishments of corresponding security behaviors, the collective effect of employees' ethical perceptions creates a climate that emphasizes the importance of information security and shows what type of security behaviors are acceptable to the organization. Thus, we hypothesize that:

H1. Ethical leadership positively influences employees' perception of information security climate.

In addition, previous research found that organizational climate and ethical culture play important mediating roles in the relationships between ethical leadership and employees' behaviors (Demirtas and Akdogan, 2015). For example, Mayer *et al.* (2010) suggested that the

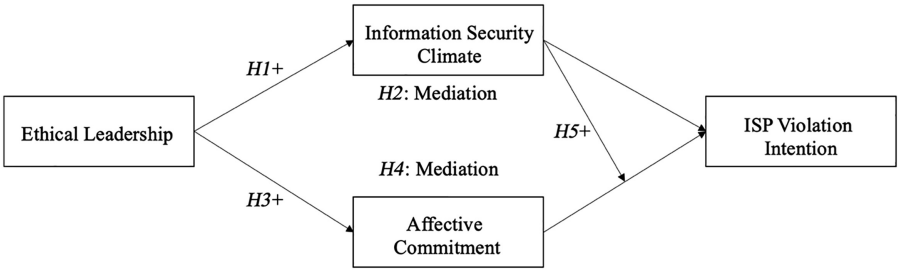

Figure 1.
Research model

relationship between ethical leadership and employees' misconduct behavior is mediated by ethical climate. Previous research suggested that ethical climate could provide cues about whether behaviors are acceptable or not in the organization and negatively influences employees' unethical behaviors (Demirtas and Akdogan, 2015). In this research, we argue that information security climate also conveys information to employees about what behaviors are inappropriate and plays a mediating role.

Previous studies have investigated the effect of information security climate on employees' information security behavior. For example, Chan *et al.* (2005) and Goo *et al.* (2014) found that information security climate positively influences employees' policy compliance behavior. An ethical leader, as a moral manager, rewards appropriate security behaviors and disciplines the inappropriate security behaviors in the organization. The rewards and sanctions enforced ethical standards (Brown *et al.*, 2005). Employees will learn how past violation behavior was disciplined and shape the shared understandings about ISP, that is, information security climate. When employees perceived a stronger information security climate, they are less likely to violate ISP. Previous research suggested that a leader in the organization will influence followers' behavior by creating a climate that emphasizes the rule and policy (Wimbush *et al.*, 1994). Thus, we hypothesize:

H2. Information security climate mediates the relationship between ethical leadership and employee ISP violation intention.

2.3 A moral person: the mediating role of affective commitment

From the perspective of a moral person, an ethical leader influences employees' behaviors through reciprocity (Brown *et al.*, 2005). A moral person is honest, integral, just and can be trusted (Brown *et al.*, 2005), where employees perceive positive treatment from their leader. Ethical leaders who are responsible for coordinating work, evaluating employees' performance and assigning resources are regarded as agents of the organization (Eisenberger, *et al.*, 1986). Therefore, the exchanged benefits occur between employees and the organization. Previous studies have found a positive relationship between ethical leadership and employees' positive organizational behaviors based on social exchange theory (Kacmar *et al.*, 2011; Mo and Shi, 2017; Newman *et al.*, 2014). According to social exchange theory, employees who received positive treatment from ethical leaders tend to respond with benefits of support or relationship investment (Aryee *et al.*, 2002), and when employees are in a high-quality leader-member exchange relationship, they are more likely to be effective workers (Sparrowe and Liden, 1997). Previous research suggests that employees reciprocate positive treatment from ethical leadership by stimulating the emotional bond employees to develop with the organization, particularly affective commitment (Allen and Meyer, 1990).

Affective commitment is a type of organizational commitment that is emotional and affective in which the individual employee strongly identifies with the organization and wishes to be involved with and part of the organization. The influence of ethical leadership on affective commitment has been well-documented in previous research (Neubert *et al.*, 2009). Previous research suggests that since the moral person focuses on caring for the people, openness to input, integrity and other aspects (Treviño *et al.*, 2000), the employee will perceive more belongingness and affective commitment to the organization because their socioemotional demand has been satisfied (Neubert *et al.*, 2009). Brown and Treviño (2006) also suggested a positive relationship between ethical leadership and follower work attitude and proposed that ethical leaders create follower's organizational commitment. Following previous evidence, we hypothesize that:

H3. Ethical leadership positively influences employees' affective commitment.

Furthermore, affective commitment has been considered as a mediating factor influencing the relationship between ethical leadership and employees' behavior in previous research. For example, Neves and Story (2015) investigated the mediation effect of affective commitment between ethical leadership and employee deviance. Kim and Brymer (2011) found a mediation effect of affective organizational commitment between ethical eldership and employee turnover intention. Previous IS security research has investigated the role of affective commitment to the organization in influencing employees' security behaviors. For example, Goo *et al.* (2014) investigated a positive relationship between affective commitment and employees' ISP compliance intention. Posey *et al.* (2015) found that affective commitment has a positive impact on employees' motivation to engage in protective security behavior. Thus, we propose that ethical leadership should influence employees' ISP violation intention through an increase in affective commitment. We consider that employees who perceived positive treatment from ethical leaders will be more committed to the organization. Employees with a high affective commitment will reduce the ISP violation behavior as a result of reciprocity. Thus, we hypothesize:

H4. Affective commitment mediates the relationship between ethical leadership and ISP violation intention.

2.4 The interactive effect of information security climate and affective commitment

Although information security climate and affective commitment are treated as distinct pathways for explaining the role of ethical leadership, these two mediating factors might interact to influence individuals' outcomes. For example, Li *et al.* (2016) investigated the moderating effect of organizational competitive climate on the relationship between affective commitment and job performance. Tepper *et al.* (2008) investigated the moderation effect of norms toward organization deviance on the influence of affective commitment on organization deviance.

We argue that the information security climate moderates the effect of affective commitment on employees' ISP violation behavior. When individuals perceive low affective commitment, they tend to engage in deviant behavior because they experience less emotional attachment and have no sense of belonging to the organization (Neves and Story, 2015). However, not all individuals who perceive low affective commitment will conduct deviant behavior. The effect of affective commitment on employees' ISP violation intention might be determined by the information security climate.

Information security climate prescribes rules and standards for employees to judge the appropriateness of their security behaviors (Chan *et al.*, 2005; Goo *et al.*, 2014). Employees might learn from the information security climate about rewards or punishments for appropriate and acceptable or unacceptable behaviors in the organization. Individuals with low affective commitment might be likely to violate organizational ISP, but they might not violate it when they perceive a high organizational information security climate. Thus, we hypothesize that.

H5. Information security climate positively moderates the negative relationship between affective commitment and employees' ISP violation intention.

3. Methods

3.1 Sample and procedure

Data were collected by using a cross-sectional survey developed on Qualtrics and distributed to members of Amazon Mechanical Turk (MTurk), and participants took approximately 8–10 min to complete. The participants were selected based on several criteria. First, participants had to be full-time employees and at least 18 years old. Second, the Human

Intelligence Tasks (HITs) approval rate for participants must be greater than 90%, and the number of HITs approved must be greater than 100. This ensured a high-quality sample pool. Rigorous scale development procedures were followed, and university ethics board approval was obtained. Participants who agreed with the informed consent continued to fill out the questionnaire. Each respondent received USD 1.00 for completing the questionnaire.

A total of 401 participants completed the survey. However, we discarded incomplete responses and excluded participants who did not pass the attention check question. This resulted in 339 responses, which were used for final data analysis. Among the respondents, the proportion of female employees was 46%. A total of 160 of the respondents were between 25 and 34 years old (47.9%) and 179 of them held a four-year university degree (52.8%). The average time they spent in their current organization was 5.99 years, and 184 of them held a position of supervisor, manager or executive in their organization (54.2%).

3.2 Measures

The measurement scales of ethical leadership, affective commitment, information security climate and ISP violation intention were adapted from previous studies, which were previously validated and empirically tested by the prior studies.

Ethical leadership. The items of ethical leadership which were adopted from Brown *et al.* (2005) have been empirically tested by numerous studies in the management field (Bavik *et al.*, 2018; Mo and Shi, 2017; Resick *et al.*, 2013). Respondents were asked to evaluate their perception of ethical leadership of their immediate supervisor. An example item was: "My leader (immediate supervisor) disciplines employees who violate ethical standards." A five-point Likert scale (1 = "strongly agree" and 5 = "Strongly disagree") was used. The Cronbach's alpha was 0.90.

Affective commitment. The scale of affective commitment in Allen and Meyer (1990), which has been adopted by several IS security studies (Goo *et al.*, 2014; Sharma and Warkentin, 2019), was used. Respondents rated their perception of affective commitment to the organization using a 5-point Likert scale (1 = "strongly agree" and 5 = "Strongly disagree"). An example item was: "I enjoy discussing my organization with people outside it." The Cronbach's alpha was 0.893.

Information security climate. Based on the scale widely used in prior research (Chan *et al.*, 2005; Goo *et al.*, 2014; Johnston *et al.*, 2016), we adopted the following steps to adjust the items for the information security climate in this study. First, we developed an introduction to information security climate, using examples that enabled participants to imagine their organizational information security climate. These examples include "When thinking of the following items, please imagine: (for example) your organization's top management is confident that the compliance of information security is important" or "your direct supervisor considers information security compliance as a key factor in assessing employees" overall performance." Second, the respondents were asked to respond to five items, such as "My organization can protect its information assets well." A five-point Likert scale (1 = "strongly agree" and 5 = "Strongly disagree") was used. The Cronbach's alpha was 0.865.

ISP violation intention. In this research, we tested employees' behavioral intention instead of actual behavior. This approach is chosen is because the actual ISP violation is difficult to be observed by a researcher. Previous research suggests that there may be inconsistency between intention and behavior; however, a large number of studies have found a strong correlation between behavioral intention and actual behavior (Notani, 1998; Sutton, 1998). Therefore, the self-reported behavioral intention is used in this study. The scale for ISP violation intention was adapted from Johnston *et al.* (2016). Participants were randomly assigned to read one of the four scenarios that were borrowed from Johnston *et al.* (2016). Participants read the scenario and were asked to imagine the experience of the individual

whose situation was described in the scenario. Each vignette described a situation where a company employee, named Joe, wants to take company-owned sensitive customer data back home to continue his work, which will violate an organizational ISP. We asked participants to evaluate the likelihood that they would duplicate such behavior under a similar condition if they were the scenario character. This method, widely used in many security behavior studies, reduces social desirability bias, especially when measuring deviant behavioral intention. An example item was: "In this situation, I would do the same as Joe." We also used a five-point Likert Scale (1 = "strongly agree" and 5 = "Strongly disagree"). The Cronbach's alpha was 0.925. The scenarios have been presented in the appendix section.

In addition, we also tested the response consistency of ISP violation intention across four scenarios. To test the difference, we conducted a one-way analysis of variance (one-way ANOVA) by using SPSS V25. The result showed that the responses were not significantly different among scenarios ($p > 0.05$), which indicated a response consistency across scenarios.

Control variables. We control for age, gender and employees' position in this study. According to prior studies, age, gender and employees' position have been found to be associated with employees' security behaviors (D'Arcy *et al.*, 2009; Lee *et al.*, 2017; Guo *et al.*, 2011). The results showed age and employees' position significantly influence ISP violation intention, while gender has no significant effect.

4. Results

We used AMOS v.24 to test the measurement model and structural model. AMOS is used for covariance-based structural equation modeling, which can simultaneously test latent variables and path coefficients. As recommended by Gefen *et al.* (2000), we first used confirmatory factor analysis (CFA) to assess the measurement model. We used chi-square divided by degrees of freedom (x^2/df), the comparative fit index (CFI), the Tucker–Lewis index (TLI) and the root mean square error of approximation (RMSEA) to test the model fit. Then we tested the structural model and estimate the path coefficient using bootstrapping.

4.1 Test of the measurement model

The first step was to estimate the measurement model using AMOS. The measurement model fit data well (χ^2/df = 1.89; CFI = 0.96; TLI = 0.95; RMSEA = 0.05). χ^2/df < 2, CFI > 0.90, TLI > 0.90, and RMSEA <0.05 indicate a good model fit (Hu and Bentler, 1999). All factor loadings of items were statistically significant and between 0.66 and 0.92. We used composite reliability and Cronbach's alpha to assess the reliability. Table 1 shows that the composite reliability was between 0.86 and 0.93, and Cronbach's alpha was between 0.865 and 0.925, which indicates good reliability (Gliem and Gliem, 2003; Nunnally and Bernstein, 1994). Moreover, we assessed the convergent validity and discriminant validity. The validity was calculated based on the AVE and correlations among constructs. Table 2 showed that correlations among constructs were lower than the square root of AVE, which indicated a good discriminant validity (Fornell and Larcker, 1981). AVE values of all constructs are higher than 0.5, which indicate a good convergent validity in the measurement model.

We followed Podsakoff *et al.* (2003)' prescriptions to mitigate the influence of common method bias (CMB). First, we have conducted expert panel reviews to decrease the ambiguity of items and increase the content validity. Second, survey respondents were guaranteed anonymity and were informed that there is no correct or incorrect answer for the survey questions. In addition, questions were randomized to avoid clustering by construct. Further, we performed the unmeasured latent common method to detect CMB. A latent common method variable was included in the model to test for the effect of CMB. We conducted a CFA

Constructs	Standardized factor loading
Affective commitment (Allen and Meyer, 1990)	C.R. = 0.86
1. I would be very happy to spend the rest of my career with this organization	0.78 *
2. I enjoy discussing my organization with people outside it	0.70
3. I really feel as if this organization's problems are my own	0.70
4. I do not feel like "part of the family" at my organization	0.70
5. I do not feel "emotionally attached" to this organization	0.66
6. This organization has a great deal of personal meaning for me	0.86
7. I do not feel a strong sense of belonging to my organization	0.66
ISP violation intention (Johnston et al., 2016)	C.R. = 0.93
1. In this situation, I would do the same as Joe	0.92 *
2. If I were Joe, I would have also skipped the procedure	0.86
3. I think I would do what Joe did if this happened to me	0.92
Information security climate (adapted from Goo et al., 2014)	C.R. = 0.86
1. My organization can protect its information assets well	0.72 *
2. The information assets in our organization could be protected well	0.66
3. Protecting information assets is a critical concern in my organization	0.70
4. Information security is important to my organization	0.80
5. Information security protection in my organization has been well-developed	0.83
Ethical leadership (Brown et al., 2005)	C.R. = 0.92
My leader (immediate supervisor) ...	
1. listens to what employees have to say	0.80 *
2. conducts his/her personal life in an ethical manner	0.68
3. has the best interests of employees in mind	0.86
4. makes fair and balanced decisions	0.89
5. can be trusted	0.86
6. discusses business ethics or values with employees	0.69
7. defines success not just by results but also the way that they are obtained	0.70
8. when making decisions, asks "what is the right thing to do?"	0.74

Note(s): Model Fit Statistics (χ^2 = 450.96, DF = 239, CFI = 0.959, TLI = 0.953, RMSEA = 0.05); *Items constrained for identification purpose; CR = Composite Reliability

Table 1. Confirmatory factor and reliability analysis

	AVE	Mean	SD	Affective commitment	Ethical leadership	Information security climate (ISC)	ISP violation intention
Affective commitment	0.525	2.623	1.031	0.725			
Ethical leadership	0.577	2.005	0.879	0.605	0.759		
Information security climate	0.554	1.774	0.762	0.386	0.517	0.744	
ISP violation intention	0.806	3.936	1.171	0.134	−0.203	0.302	0.898

Note(s): The square root of AVE is loaded on diagonal

Table 2. Correlations, means and average variance Extracted (AVE)

to compare the model with and without the latent method variable. The results showed that the difference of chi-square was less than 3.84 before and after the latent method variable was included in the measurement model, which indicates that CMB is not of great concern in this study.

4.2 Test of the structural model

With an adequate measurement model, we next used AMOS to test the structural model and hypotheses. Results show that the structural model fits the data well ($p < 0.001$; $\chi^2/df = 1.90$; CFI = 0.96; IFI = 0.96; RMSEA = 0.05). Figure 2 shows the result of our research model testing. Hypotheses 1 and 3 proposed positive relationships between ethical leadership and information security climate, and affective commitment. The results showed that ethical leadership was positively associated with information security climate ($b = 0.523$, $p < 0.001$) and was also positively associated with affective commitment ($b = 0.609$, $p < 0.001$). Thus, hypotheses 1 and 3 were supported. Table 3 shows the summary of hypotheses testing.

To test the mediation effects of information security climate and affective commitment, we conducted the mediation test by following Zhao *et al.* (2010), which assessed the indirect effect by examining the product of A path and B path while controlling the direct effect of C path. Consistent with hypothesis 2, the results showed that the indirect effect of ethical leadership on ISP violation intention through information security climate was significant ($B = -0.198$, $p < 0.05$) and the confidence interval is between −0.320 and −0.107. There was no remaining significant direct effect between ethical leadership and ISP violation intention ($B = -0.095$, $p > 0.05$). The result indicated that the relationship between the ethical leadership and ISP violation intention is fully mediated by the information security climate. Hypothesis 4 proposes the indirect effect of affective commitment. However, the results indicated that the indirect effect of ethical leadership on ISP violation intention through affective commitment

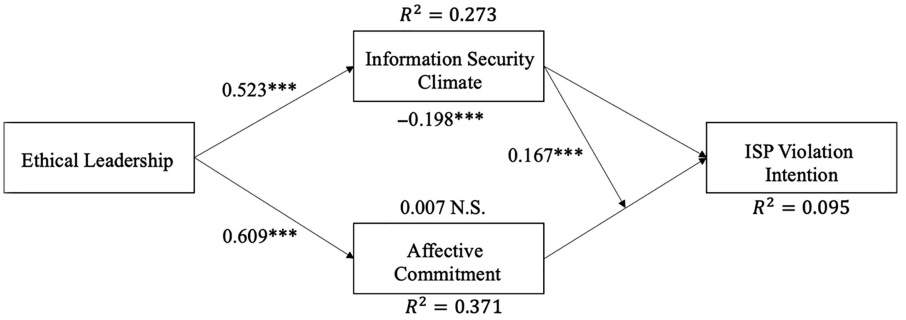

Figure 2.
Results of model testing

Note(s): ***$P < 0.01$

Hypotheses	Supported?	Path coefficient	p-value
Hypothesis 1: Ethical leadership → information security climate	Yes	0.523	$p < 0.01$
Hypothesis 2: Ethical leadership → information security climate → ISP violation intention	Yes	−0.198	$p < 0.01$
Hypothesis 3: Ethical leadership → affective commitment	Yes	0.609	$p < 0.01$
Hypothesis 4: Ethical leadership → affective commitment → ISP violation intention	No	0.007	$p > 0.05$
Hypothesis 5: Information security climate * affective commitment → ISP violation intention	Yes	0.167	$p < 0.01$
Gender → ISP violation intention	_	−0.029	$p > 0.05$
Age → ISP violation intention	_	−0.183	$p < 0.01$
Position → ISP violation intention	_	0.374	$p < 0.01$

Table 3.
Results of hypotheses testing

was insignificant ($B = 0.007$, $p > 0.05$), and the confidence interval was between −0.110 and 0.126.

Hypothesis 5 proposed the moderation effect of ISC on the influence of affective commitment on ISP violation. The results showed that the information security climate significantly and positively moderated the relationship between affective commitment and ISP violation intention ($B = 0.167$, $p < 0.05$). The results in Figure 3 indicated that the negative influence of affective commitment on ISP violation intention was enhanced when the information security climate was at a high level. Hence, hypothesis 5 was supported.

5. Discussion

This research identifies the role of ethical leadership under information security context and estimated the effect of ethical leadership on employees' ISP violation intention. We investigated the role of ethical leadership from two distinct perspectives. Based on social learning theory and social exchange theory, this research identified two different mediators: affective commitment and information security climate. We argue that, as a moral person, ethical leadership influences employees' ISP violation intention through affective commitment. As a moral manager, ethical leadership influences employees' ISP violation intention through information security climate.

In particular, we found that ethical leadership has a positive influence on information security climate and affective commitment. In addition, the effect of ethical leadership on employees' ISP violation intention was fully mediated by the information security climate. We also demonstrated the interactive effect of information security climate and affective commitment on ISP violation intention. That is, information security climate enhances the negative influence of affective commitment on ISP violation intention. These findings have engendered several important theoretical and practical implications.

5.1 Theoretical implications

Our findings provide contributions to ethical leadership and information security research in the following ways. First, our results supported the hypothesis that ethical leadership negatively influences employees' ISP violation intention. Although previous research has demonstrated the effects of ethical leadership on employees' deviant behavior (Demirtas and Akdogan, 2015; Kim and Brymer, 2011; Stouten *et al.*, 2013), the influence of ethical leadership on employees' information security behavior has not been thoroughly investigated. In this research, we contribute to a specific research context of information security, and we investigate how ethical leadership influences employees' ISP violation intention. We believe this is also the first study to shed light on such relationships; hence, our research opens a new

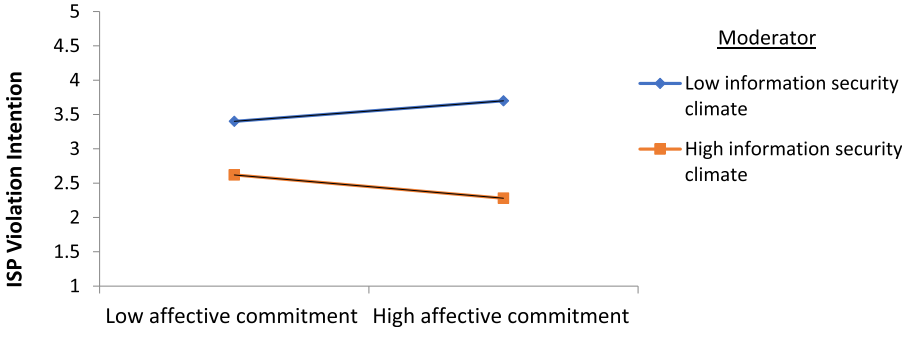

Figure 3.
Moderation effect of information security climate on the relationship between affective commitment and ISP violation intention

pathway for future research to investigate how different leadership styles can influence employees' ISP violation intention and illustrates how ethical leadership differs from other leadership styles in the context of information security.

Second, while previous studies have investigated the effects of ethical leadership on employees' workplace behavior (Lu and Lin, 2014; Mayer *et al.*, 2010; Mo and Shi, 2017; Stouten *et al.*, 2013; Toor and Ofori, 2009), there has been a dearth of research into the effects of ethical leadership from both moral person and moral manager perspectives. In the context of information security, we tested those two paths separately and found that ethical leadership influences employees' ISP violation intention through information security climate rather than affective commitment. As a moral manager, the ethical leader plays a critical role in generating organizational climate and norms to influence employees' security behaviors. Our results found that moral managers may be more important in the context of information security.

Finally, our findings highlight the importance of the interactive effects of information security climate and affective commitment. Although the moral manager and the moral person are regarded as distinct pathways for explaining the role of ethical leadership (Brown *et al.*, 2005; Ruiz *et al.*, 2011; Treviño *et al.*, 2000), the interactive effects have not been investigated. We found that information security climate positively moderates the effect of affective commitment on employees' ISP violation intention. Employees who perceive a high level of information security climate pay more attention to the rules and norms governing organizational security requirements. In a high information security environment, employees with low affective commitment may not intend to violate ISP.

5.2 Practical implications

In practical terms, information security protection is a critical agenda item for organizations. Our findings provide recommendations for improving information security in organizations. We found that the organization should create high ethical standards for managers. Managers are important model examples to inspire subordinates to reduce unethical behaviors. A manager with higher ethical and moral standards can help employees learn how to behave morally in the organization and reduce deviant behaviors, including ISP violations. Therefore, it is important to raise leaders' and top management's ethical standards. For example, organizations should require managers to comply with the ISP and set a good example for employees. Also, managers are expected to provide feedback mechanisms for employees to express and share their security concerns or suggestions since it is important for ethical leaders to obtain employee feedback.

Second, our study indicates a critical role of information security climate in reducing organizational security-related deviant behaviors. Therefore, organizations could make greater efforts to improve their organizational information security climate. For example, the organization should encourage employees to participate in security training and education programs to improve employees' understanding of organizational information security protection. Furthermore, more resources could be investigated and allocated to information security climate-related areas to highlight the importance of information security in organizations, thereby raising employees' perceptions of information security climate and intention of ISP compliance.

Third, our findings indicate that information security climate (from the perspective of moral manager) does not significantly influence ISP violation intention but significantly moderates the effect of affective commitment (from the perspective of moral person) on employees' ISP violation intention. This result implies that simply improving employees' affective commitment may not be useful in influencing employees' security behaviors; instead, the organization should consider the interactive effects of factors from a moral

manager and a moral person. For example, top executives of the organization should demonstrate themselves not only as moral administrators but also as moral people to influence subordinates' information security behaviors. Using authorized power ethically and properly in organizations will help leaders increase followers' organizational commitment and other positive outcomes while decreasing employees' information security violation behavioral intentions.

5.3 Limitation and future research

This research contributes to information security and ethical leadership literature; however, it has several inevitable limitations. First, this research used a cross-sectional survey to collect data. Although we found no evidence of common method bias, we cannot completely mitigate it. A longitudinal study or a method with multiple stages is recommended for future research.

Second, this research relied on self-reported intention rather than actual security behavior. The use of self-reported intention may have the social desirability effect, especially for violations of security policy. In addition, previous research has cautioned about the use of intentions as a proxy for actual behavior (Alec Cram *et al.*, 2019; Siponen and Vance, 2014; Crossler *et al.*, 2013; Warkentin *et al.*, 2012). Future research could collect data on employees' actual security behavior and estimate the effect of ethical leadership on actual security behavior.

In light of findings that information security climate plays a complete mediating role in the relationship between ethical leadership and ISP violation intention. Future researchers should explore other important mediators, such as psychological capital. In addition, our research found that affective commitment has no mediation effect. However, previous research has identified the importance of affective commitment (Goo *et al.*, 2014). The role of affective commitment should be paid more attention in further study. In addition, other factors, such as leadership member exchange, should be considered in future research.

Our research shows the moderating effect of information security climate on the influence of affective commitment on employees' ISP violation intention. Future research could look into the moderating effects of different psychological variables from the perspective of a moral manager and a moral person such as moral identity and perceived interpersonal justice. The interactive effects could play an important role in improving the understanding of the role of ethical leadership.

This research investigates the role of ethical leadership in explaining employees' ISP violation intention. Future research can explore the relationship between ethical leadership and other types of security behaviors, especially extra-role security behavior, such as voice and helping behavior. There has been no research into the impact of ethical leadership on ethical security behaviors.

6. Conclusion

This study extended academic work on ethical leadership to the field of information security and investigated the role of ethical leadership in influencing employees' ISP violation intention through a dual-mediation effect. Data collected from 339 employees demonstrated the influences of ethical leadership on employees' ISP violation intention by increasing perception of information security climate and affective commitment. Moreover, this study found the moderating effect of information security climate on the influence of affective commitment on ISP violation intention. The findings provided a management guide for organizational top management from both theoretical and practical lenses and highlighted the importance of ethical leadership within the information security context.

References

Alec Cram, W., D'Arcy, J. and Proudfoot, J.G. (2019), "Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance", *MIS Quarterly*, Vol. 43 No. 2, pp. 525-554.

Allen, N.J. and Meyer, J.P. (1990), "The measurement and antecedents of affective, continuance and normative commitment to the organization", *Journal of Occupational Psychology*, Vol. 63, pp. 1-18.

Aryee, S., Budhwar, P.S. and Chen, Z.X. (2002), "Trust as a mediator of the relationship between organizational justice and work outcomes: test of a social exchange model", *Journal of Organizational Behavior*, Vol. 23 No. 3, pp. 267-285.

Bandura, A. (1977), *Social Learning Theory*, Prentice Hall, Englewood Cliffs, New Jerssey, NJ.

Bavik, Y.L., Tang, P.M., Shao, R. and Lam, L.W. (2018), "Ethical leadership and employee knowledge sharing: Exploring dual-mediation paths", *Leadership Quarterly*, Vol. 29 No. 2, pp. 322-332.

Brown, M.E. and Treviño, L.K. (2006), "Ethical leadership: a review and future directions", *Leadership Quarterly*, Vol. 17 No. 6, pp. 595-616.

Brown, M.E., Treviño, L.K. and Harrison, D.A. (2005), "Ethical leadership: a social learning perspective for construct development and testing", *Organizational Behavior and Human Decision Processes*, Vol. 97 No. 2, pp. 117-134.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Chan, M., Woon, I. and Kankanhalli, A. (2005), "Perceptions of information security at the workplace: linking information security climate to compliant behavior", *Journal of Information Privacy and Security*, Vol. 1 No. 3, pp. 18-41.

Chen, Y., Geletta, D.F., Lowry, P.B., Luo, X., Moody, G.D. and Wilison, R. (2021), "Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model", *Information Systems Research*, forthcoming, pp. 1-23, doi: 10.1287/isre.2021.1014.

Cheng, L., Li, Y., Li, W., Holm, E. and 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*, Vol. 39, pp. 447-459.

Cheng, J., Bai, H. and Yang, X. (2019), "Ethical leadership and internal whistleblowing: a mediated moderation model", *Journal of Business Ethics*, Vol. 155 No. 1, pp. 115-130.

Chu, A.M.Y., Chau, P.Y.K. and So, M.K.P. (2015), "Explaining the misuse of information systems resources in the workplace: a dual-process approach", *Journal of Business Ethics*, Vol. 131 No. 1, pp. 209-225.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013), "Future directions for behavioral information security research", *Computers and Security*, Vol. 32, pp. 90-101.

D'Arcy, J., Herath, T. and Shoss, M.K. (2014), "Understanding employee responses to stressful information security requirements: a coping perspective", *Journal of Management Information Systems*, Vol. 31 No. 2, pp. 285-318.

Demirtas, O. and Akdogan, A.A. (2015), "The effect of ethical leadership behavior on ethical climate, turnover intention, and affective commitment", *Journal of Business Ethics*, Vol. 130 No. 1, pp. 59-67.

D'Arcy, J., Hovav, A. and Galletta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 79-98.

Eisenberger, R., Huntington, R., Hutchison, S. and Sowa, D. (1986), "Perceived organizational support", *Journal of Applied Psychology*, Vol. 71 No. 3, pp. 500-507.

Feng, G., Zhu, J., Wang, N. and Liang, H. (2019), "How paternalistic leadership influences it security policy compliance: the mediating role of the social bond", *Journal of the Association for Information Systems*, Vol. 20 No. 11, pp. 1650-1691.

Fornell, C. and Larcker, D.F. (1981), "SEM with unobservable variables and measurement error: algebra and statistics", *Journal of Marketing Research*, Vol. 18, pp. 382-388.

Gefen, D., Straub, D.W. and Boudreau, M.C. (2000), "Structural equation modeling and regression: guidelines for research practice", *Communications of the Association for Information Systems*, Vol. 4 No. 7.

Gerpott, F.H., Van Quaquebeke, N., Schlamp, S. and Voelpel, S.C. (2019), "An identity perspective on ethical leadership to explain organizational citizenship behavior: the interplay of follower moral identity and leader group prototypicality", *Journal of Business Ethics*, Vol. 156 No. 4, pp. 1063-1078.

Gliem, J. and Gliem, R. (2003), "Calculating, interpreting, and reporting cronbach's alpha reliability coefficient for likert-type scales", *2003 Midwest Research to Practice Conference in Adult, Continuing, and Community Education Calculating*, pp. 82-88.

Goo, J., Yim, M.S. and Kim, D.J. (2014), "A path to successful management of employee security compliance: an empirical study of information security climate", *IEEE Transactions on Professional Communication*, Vol. 57 No. 4, pp. 286-308.

Guhr, N., Lebek, B. and Breitner, M.H. (2019), "The impact of leadership on employees' intended information security behaviour: an examination of the full-range leadership theory", *Information Systems Journal*, Vol. 29 No. 2, pp. 340-362.

Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011), "Understanding nonmalicious security violations in the workplace: a composite behavior model", *Journal of Management Information Systems*, Vol. 28 No. 2, pp. 203-236.

Herath, T. and Rao, H.R. (2009), "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165.

Ho, S.M. and Warkentin, M. (2017), "Leader's dilemma game: an experimental design for cyber insider threat research", *Information Systems Frontiers*, Vol. 19 No. 2, pp. 377-396.

Hu, L.T. and Bentler, P.M. (1999), "Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives", *Structural Equation Modeling*, Vol. 6 No. 1, pp. 1-55.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing employee compliance with information security policies: the critical role of top management and organizational culture", *Decision Sciences*, Vol. 43 No. 4, pp. 615-660.

Huang, L. and Paterson, T.A. (2017), "Group ethical voice: influence of ethical leadership and impact on ethical performance", *Journal of Management*, Vol. 43 No. 4, pp. 1157-1184.

Johnston, A.C. and Warkentin, M. (2010), "Fear appeals and information security behaviors: an empirical study", *MIS Quarterly*, Vol. 34 No. 3, pp. 549-566.

Johnston, A.C., Warkentin, M. and Siponen, M. (2015), "An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric", *MIS Quarterly*, Vol. 39 No. 1, pp. 113-134.

Johnston, A.C., Warkentin, M., McBride, M. and Carter, L. (2016), "Dispositional and situational factors: influences on information security policy violations", *European Journal of Information Systems*, Vol. 25 No. 3, pp. 231-251.

Kacmar, K.M., Bachrach, D.G., Harris, K.J. and Zivnuska, S. (2011), "Fostering good citizenship through ethical leadership: Exploring the moderating role of gender and organizational politics", *Journal of Applied Psychology*, Vol. 96 No. 3, pp. 633-642.

Kim, W.G. and Brymer, R.A. (2011), "The effects of ethical leadership on manager job satisfaction, commitment, behavioral outcomes, and firm performance", *International Journal of Hospitality Management*, Vol. 30 No. 4, pp. 1020-1026.

Lebek, B., Guhr, N. and Breitner, M. (2014), "Transformational leadership and employees' information security performance: the mediating role of motivation and climate", *Proceedings of the Thirty Fifth International Conference on Information Systems, Auckland*.

Lee, J. Jr, Warkentin, M., Crossler, R.E. and Otondo, R.F. (2017), "Implications of monitoring mechanisms on bring your own device adoption", *Journal of Computer Information Systems*, Vol. 57 No. 4, pp. 309-318.

Li, H., Sarathy, R., Zhang, J. and Luo, X. (2014), "Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance", *Information Systems Journal*, Vol. 24 No. 6, pp. 479-502.

Li, J.J., Wong, I.K.A. and Kim, W.G. (2016), "Effects of psychological contract breach on attitudes and performance: the moderating role of competitive climate", *International Journal of Hospitality Management*, Vol. 55, pp. 1-10.

Li, H., Luo, X. and Chen, Y. (2021), "Understanding information security policy violation from a situational action perspective", *Journal of the Association for Information Systems*, Vol. 22 No. 3, pp. 739-772, doi: 10.17705/1jais.00678.

Lin, C. and Luo, X. (2021), "Toward a unified view of dynamic information security behaviors: insights from organizational culture and sensemaking", *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, Vol. 52 No. 1, pp. 65-90.

Lu, C.S. and Lin, C.C. (2014), "The effects of ethical leadership and ethical climate on employee ethical behavior in the international port context", *Journal of Business Ethics*, Vol. 124 No. 2, pp. 209-223.

Luo, X.R., Li, H., Hu, Q. and Xu, H. (2020), "Why individual employees commit Malicious computer abuse: a routine activity theory perspective", *Journal of the Association for Information Systems*, Vol. 21 No. 6, pp. 1552-1593.

Manz, C.C. and Sims, H.P. Jr (1981), "Vicarious learning: the influence of modeling on organizational behavior", *Academy of Management Review*, Vol. 6 No. 1, pp. 105-113.

Mayer, D.M., Kuenzi, M. and Greenbaum, R.L. (2010), "Examining the link between ethical leadership and employee misconduct: the mediating role of ethical climate", *Journal of Business Ethics*, Vol. 95 No. 1, pp. 7-16.

Mo, S. and Shi, J. (2017), "Linking ethical leadership to employees' organizational citizenship behavior: testing the multilevel mediation role of organizational concern", *Journal of Business Ethics*, Vol. 141 No. 1, pp. 151-162.

Moody, G.D., Siponen, M. and Pahnila, S. (2018), "Toward a unified model of information security policy compliance", *MIS Quarterly*, Vol. 42 No. 1, pp. 285-311.

Moore, C., Mayer, D.M., Chiang, F.F.T., Crossley, C., Karlesky, M.J. and Birtch, T.A. (2019), "Leaders matter morally: the role of ethical leadership in shaping employee moral cognition and misconduct", *Journal of Applied Psychology*, Vol. 104 No. 1, pp. 123-145.

Mutchler, L.A. and Warkentin, M. (2020), "Experience matters: the role of vicarious experience in secure actions", *Journal of Database Management*, Vol. 31 No. 2, pp. 1-20.

Neubert, M.J., Carlson, D.S., Kacmar, K.M., Roberts, J.A. and Chonko, L.B. (2009), "The virtuous influence of ethical leadership behavior: evidence from the field", *Journal of Business Ethics*, Vol. 90 No. 2, pp. 157-170.

Neves, P. and Story, J. (2015), "Ethical leadership and reputation: combined indirect effects on organizational deviance", *Journal of Business Ethics*, Vol. 127 No. 1, pp. 165-176.

Newman, A., Kiazad, K., Miao, Q. and Cooper, B. (2014), "Examining the cognitive and affective trust-based mechanisms underlying the relationship between ethical leadership and organisational

citizenship: a case of the head leading the heart?", *Journal of Business Ethics*, Vol. 123 No. 1, pp. 113-123.

Notani, A. (1998), "Moderators of perceived be- havioral control's predictiveness in the theory of planned behavior: a meta-analysis", *Journal of Consumer Psychology*, Vol. 7 No. 3, pp. 247-271.

Nunnally, J.C. and Bernstein, I.H. (1994), *Psychometric Theory*, McGraw-Hill, New York, NY.

Ormond, D., Warkentin, M. and Crossler, R.E. (2019), "Integrating cognition with an affective lens to better understand information security policy compliance", *Journal of the Association for Information Systems*, Vol. 20 No. 12, pp. 1794-1843.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y. and Podsakoff, N.P. (2003), "Common method biases in behavioral research: a critical review of the literature and recommended remedies", *Journal of Applied Psychology*, Vol. 88 No. 5, pp. 879-903.

Posey, C., Roberts, T.L. and Lowry, P.B. (2015), "The impact of organizational commitment on insiders motivation to protect organizational information assets", *Journal of Management Information Systems*, Vol. 32 No. 4, pp. 179-214.

PWC (2018), "The Global State of Information Security® Survey 2018", available at: https://www.idg.com/tools-for-marketers/2018-global-state-information-security-survey/ (accessed 25 July 2021).

Resick, C.J., Hargis, M.B., Shao, P. and Dust, S.B. (2013), "Ethical leadership, moral equity judgments, and discretionary workplace behavior", *Human Relations*, Vol. 66 No. 7, pp. 951-972.

Ruiz, P., Ruiz, C. and Martínez, R. (2011), "Improving the 'leader-follower' relationship: top manager or supervisor? The ethical leadership trickle-down effect on follower job response", *Journal of Business Ethics*, Vol. 99 No. 4, pp. 587-608.

Schaubroeck, J.M., Hannah, S.T., Avolio, B.J., Kozlowski, S.W., Lord, R.G., Treviño, L.K., Dimotakis, N. and Peng, A.C. (2012), "Embedding ethical leadership within and across organization levels", *Academy of Management Journal*, Vol. 55 No. 5, pp. 1053-1078.

Sharma, S. and Warkentin, M. (2019), "Do I really belong?: impact of employment status on information security policy compliance", *Computers and Security*, Vol. 87, p. 101397.

Siponen, M.T. and Vance, A. (2010), "Neutralization: new insights into the problem of employee information systems security policy violations", *MIS Quarterly*, Vol. 34 No. 3, pp. 487-502.

Siponen, M.T. and Vance, A. (2014), "Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations", *European Journal of Information Systems*, Vol. 23 No. 3, pp. 289-305.

Siponen, M., Vance, A. and Willison, R. (2012), "New insights into the problem of software piracy: the effects of neutralization, shame, and moral beliefs", *Information and Management*, Vol. 49 Nos 7-8, pp. 334-341.

Sparrowe, R.T. and Liden, R.C. (1997), "Process and structure in leader–member exchange", *Academy of Management Review*, Vol. 22 No. 2, pp. 522-552.

Stouten, J., van Dijke, M., Mayer, D.M., De Cremer, D. and Euwema, M.C. (2013), "Can a leader be seen as too ethical? The curvilinear effects of ethical leadership", *Leadership Quarterly*, Vol. 24 No. 5, pp. 680-695.

Sutton, S. (1998), "Predicting and explaining inten- tions and behavior: how well are we doing?", *Journal of Applied Social Psychology*, Vol. 28, pp. 1317-1338.

Tepper, B.J., Henle, C.A., Lambert, L.S., Giacalone, R.A. and Duffy, M.K. (2008), "Abusive supervision and subordinates' organization deviance", *Journal of Applied Psychology*, Vol. 93 No. 4, pp. 721-732.

Toor, S.R. and Ofori, G. (2009), "Ethical leadership: examining the relationships with full range leadership model, employee outcomes, and organizational culture", *Journal of Business Ethics*, Vol. 90 No. 4, pp. 533-547.

Treviño, L.K., Hartman, L.P. and Brown, M. (2000), "Moral person and moral manager: how executives develop a reputation for ethical leadership", *California Management Review*, Vol. 42 No. 4, pp. 128-142.

Trinkle, B.S., Warkentin, M., Malimage, K. and Raddatz, N. (2021), "High-risk deviant decisions: does neutralization still play a role?", *Journal of the Association for Information Systems*, Vol. 22 No. 3, pp. 797-826.

van Gils, S., Van Quaquebeke, N., van Knippenberg, D., van Dijke, M. and De Cremer, D. (2015), "Ethical leadership and follower organizational deviance: the moderating role of follower moral attentiveness", *Leadership Quarterly*, Vol. 26 No. 2, pp. 190-203.

Vance, A., Siponen, M.T. and Straub, D.W. (2020), "Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures", *Information and Management*, Vol. 57 No. 4, pp. 1-9.

Wall, J.D. and Warkentin, M. (2019), "Perceived argument quality's effect on threat and coping appraisals in fear appeals: an experiment and exploration of realism check heuristics", *Information and Management*, Vol. 56 No. 8, pp. 1-13.

Walumbwa, F.O., Hartnell, C.A. and Misati, E. (2017), "Does ethical leadership enhance group learning behavior? Examining the mediating influence of group ethical conduct, justice climate, and peer justice", *Journal of Business Research*, Vol. 72, pp. 14-23.

Wang, Y.D. and Sung, W.C. (2016), "Predictors of organizational citizenship behavior: ethical leadership and workplace jealousy", *Journal of Business Ethics*, Vol. 135 No. 1, pp. 117-128.

Warkentin, M. and Willison, R. (2009), "Behavioral and policy issues in information systems security: the insider threat", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 101-105.

Warkentin, M., Straub, D. and Malimage, K. (2012), "Featured talk: measuring secure behavior: a research commentary", *Annual Symposium of Information Assurance and Secure Knowledge Management*, Albany, New York, NY.

Willison, R., Warkentin, M. and Johnston, A.C. (2018), "Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives", *Information Systems Journal*, Vol. 28 No. 2, pp. 266-293.

Wimbush, J.C., Shepard, J.M. and Jon, M. (1994), "Toward an understanding climate: behavior of ethical behavior and supervisory influence", *Journal of Business Ethics*, Vol. 13 No. 8, pp. 637-647.

Xu, F., Wang, X. and Xue, B. (2019), "The differential effects of interpersonal justice and injustice on computer abuse: a regulatory focus theory perspective", *Journal of Database Management*, Vol. 30 No. 3, pp. 1-17.

Zhao, X., Lynch, J.G. and Chen, Q. (2010), "Reconsidering Baron and Kenny: Myths and truths about mediation analysis", *Journal of Consumer Research*, Vol. 37 No. 2, pp. 197-206.

Zhu, W., May, D.R. and Avolio, B.J. (2004), "The impact of ethical leadership behavior on employee outcomes: the roles of psychological empowerment and authenticity", *Journal of Leadership and Organizational Studies*, Vol. 11 No. 1, pp. 16-26.

Appendix

Violation scenarios (adopted from Johnston *et al.*, 2016)

Scenario 1: Joe has just collected sensitive customer data for his company, and he wants to take that data home to continue his work. He knows his company requires that he request a password to be issued and applied to all data before taking it out of the office on a USB drive so that it cannot be accessed by an unauthorized individual. Regardless, the password procedure takes several minutes, and he needs to leave now, so he skips the procedure. Joe believes his chances of being caught are low, but if caught, the punishment would be minimal.

Scenario 2: Joe has just collected sensitive customer data for his company, and he wants to take that data home to continue his work. He knows his company requires that he request a password to be issued

and applied to all data before taking it out of the office on a USB drive so that it cannot be accessed by an unauthorized individual. Regardless, the password procedure takes several minutes, and he needs to leave now, so he skips the procedure. Joe believes his chances of being caught are low, but if caught, the punishment would be severe.

Scenario 3: Joe has just collected sensitive customer data for his company, and he wants to take that data home to continue his work. He knows his company requires that he request a password to be issued and applied to all data before taking it out of the office on a USB drive so that it cannot be accessed by an unauthorized individual. Regardless, the password procedure takes several minutes, and he needs to leave now, so he skips the procedure. Joe believes his chances of being caught are high, but if caught, the punishment would be minimal.

Scenario 4: Joe has just collected sensitive customer data for his company, and he wants to take that data home to continue his work. He knows his company requires that he request a password to be issued and applied to all data before taking it out of the office on a USB drive so that it cannot be accessed by an unauthorized individual. Regardless, the password procedure takes several minutes, and he needs to leave now, so he skips the procedure. Joe believes his chances of being caught are high, but if caught, the punishment would be severe.

About the authors

Botong Xue is a Ph.D. Candidate of Business Information Systems in the College of Business at the Mississippi State University. He received his master's degree in MS&ISA from the University of New Mexico. He has published research papers in *The DATA BASE for Advances in Information Systems* and *Journal of Database Management*, and several conference papers. His research focuses on areas including individual information security behavior, cross-cultural information system study, organizational culture, and organizational leadership.

Feng Xu is a Ph.D. Candidate of Business Information Systems in the College of Business at the Mississippi State University. He has been a visiting Ph.D. student at Anderson School of Management of the University of New Mexico. He received his Ph.D. degree in management science from Xi'an Jiaotong University, China. His research interests center around behavioral information security and information security investment. He has published research papers in *Information & Management, Journal of Computer Information Systems, The DATA BASE for Advances in Information Systems, Information Systems Frontiers, Journal of Database Management*, and *Journal of Electronic Commerce Research*.

Xin Luo is Endowed Regent's Professor and Full Professor of MIS at the University of New Mexico. He received Ph.D. in MIS from Mississipi State University. He has published in leading IS journals, including *Information Systems Research, Journal of the Association for Information Systems, European Journal of Information Systems, Information Systems Journal, Journal of Strategic Information Systems, Decision Sciences, Decision Support Systems, Information & Management*, and *IEEE Transactions on Engineering Management*. He is an Associate Editor for *Journal of the Association for Information Systems, Decision Sciences, Information & Management, Electronic Commerce Research*, and *Journal of Electronic Commerce Research*. Xin Luo is the corresponding author and can be contacted at: xinluo@unm.edu

Merrill Warkentin is the James J. Rouse Endowed Professor of Information Systems in the College of Business and a William L. Giles Distinguished Professor at Mississippi State University. His research, primarily on the impacts of organizational, contextual, and dispositional influences on individual behaviors in the context of information security and privacy and in social media, has appeared in *MIS Quarterly, Journal of MIS, Journal of the AIS, European Journal of Information Systems, Information Systems Journal, Decision Sciences,* among others. He is the author or editor of seven books, and has authored or co-authored over 300 published manuscripts.