How Paternalistic Leaders Motivate Employees' Information Security Policy Compliance? Building Climate or Applying Sanctions

Completed Research Paper

Jiawen Zhu **Gengzhong Feng**

Huigang Liang

Abstract

This paper studies the influencing mechanisms of Paternalistic Leadership in motivating employees' Information Security Polices Compliance. We proposed that Sanctions and Information Security Climate can mediate the impact of different PL dimensions. Based on survey data from 760 participants, we found that, for different PL dimension, their influencing mechanism are different. The impact of AL dimension is partially mediated by employees' perception of the Sanction, while the impact of BL dimension and ML dimension are partially mediated by employees' perception of the Information Security Climate. Our research extends the existing literature by introducing the impact of specific leadership styles on employees' ISP Compliance and discovering the mediating role of Sanction and Information Security Climate. New knowledge is also found about how each PL dimension affects employees' Compliance in the information security context.

Keywords: Paternalistic Leadership, ISP Compliance, Sanction, Information Security Climate

Introduction

In the past two decades, investigating employees' Compliance to the organizational ISP has been one of the key focus of the IS scholars (Moody et al. 2018). So far, researchers have examined the impact of employees' cognitions about the situation, security counter measures and organizational factors on their ISP Compliance (Moody et al. 2018). Among these motivators, we contend that leadership is one of the most essential factors in shaping employees' ISP Compliance behaviors. This is because that nearly every aspect in the information security management is under the influence of leaders, such as deciding the overall information security strategy and polices, carrying out control mechanisms, organizing training and education programs and so on (Veiga and Eloff 2007). Leaders' sponsorship and commitment play a determinant role of the success of organizational information security campaign (Knapp et al. 2006; Veiga and Eloff 2007).

Several ISP Compliance studies have already investigated some leadership-related concepts, such as the top management support (Humaidi and Balakrishnan 2018; Knapp et al. 2006), participation (Hu

et al. 2012) and practice (Chan et al. 2005). These researches assumed that all leaders function on employees' ISP Compliance via same paradigms and affect employees in the same degree with same among of involvement. However, we contend that this assumption is questionable. Firstly, the influencing process of different leaders can be different. Leaders of different leadership style have different ways of implementing plans and motivating people (Westwood 1992). They may adopt different control measures when they support and participate in information security practices. Even the same control measures are adopted, leaders may have different ways to implement the control measures, which will result in different employees' perceptions of the control measures. For example, in compiling and executing information security policies, some leaders may prefer strict control while some may prefer a benign approach (Truss et al. 1997). Some leaders may prefer using articulated prescriptions to regulate their employees' behavior while some may prefer relying on social power and self-regulation (Ouchi and Maguire 1975). Secondly, not all the approaches adopted by leaders are effective. Griffin and Hu (2013) have proved that leaders' supervision is effective in improving the employees' security behavior while encouragement of learning and presenting the organizational vision of security make no significant impact. Thus, leaders of different leadership style, due to their different preferences for approaches, may lead to different impact on their employees. This suggests that we should separately examine the impact of different leadership styles and investigate how they function via corresponding mediating mechanisms.

Paternalistic Leadership (PL) describes a father-like leadership style (Farh et al. 2000). Authoritarianism, benevolence and morality are three dimensions of PL. PL researchers have suggested the effect of PL on employees' Compliance. They argued that employees are willing to comply due to fear of leaders' authority, reciprocation to leaders' benevolence and identification with leaders' morality (Aycan 2006; Aycan et al. 2000; Cheng et al. 2004; Farh 2006; Pellegrini and Scandura 2006). However, existing discussion about the PL-Compliance relationship is not enough to explain employees' ISP Compliance. Firstly, general Compliance does not mean that employees will comply every time or in every context. How PL affects employees' ISP Compliance needs to be discussed combining the context of information security. Secondly, the mediating process has not been explored. In fact, the three PL dimensions represent three different influencing strategies that leaders can use to affect employees' Compliance (Farh and Cheng 2000; Farh et al. 2000). Therefore, leaders of different PL dimension may adopt different control measures to achieve their goal, which will result in different indirect impact on employees' Compliance. In the current research, we adopt employees' perception of Sanction and Information Security Climate as the mediators to examine the impact of different PL dimensions. We focus on these two control mechanisms because they align with the management styles of PL dimensions and can reflect the difference of PL dimensions in adopting control mechanisms. By exploring the different control mechanisms adopted by AL, BL and ML, we intend to reveal that how will the three PL dimensions take effect and are they functioning through the same mechanism or in their own way, which will provide a clearer picture about how PL affect employees' Compliance in the information security context.

Overall, our research makes three major contributions to the existing literature. First, we proved that leadership style matters in the information security management. We found that all PL dimensions have positive effect on employees' ISP Compliance. The extent to which leaders apply AL, BL and ML will affect their effectiveness in motivating employees' Compliance to ISP. Second, we found that the impact of AL on ISP Compliance is mediated by employees' perception of Sanction while the impact of BL and ML are mediated by employees' perception of the Information Security Climate. In general, these findings suggest that leaders affect employees' ISP Compliance by carrying out information security control mechanisms. However, for the three PL dimensions, their mediating control mechanisms are different. Third, this research contributes to the PL literature. We studied the impact of PL on Compliance in the information security context and considered information security control mechanisms as the mediators. In the context of information security, we discovered new knowledge about how each PL dimension affect employees' Compliance.

Theoretical Framework

Paternalistic Leadership

Paternalism was introduced into the management field because leaders resemble the parental figures when they exercise power and authority to lead subordinates for improving both their personal and professional lives (Weber 1968). In return, employees behave as compliant children and their behavior become more controllable (Zhang et al. 2015). Such a father-like leadership style is named as Paternalistic Leadership (PL) (Westwood 1992). Summarizing the previous researches, Farh and Cheng (2000) defined PL as a leadership which combines strong discipline and authority, fatherly benevolence and moral integrity. They proposed a triad model of PL comprising three dimensions, Authoritarian Leadership, Benevolent Leadership and Moral Leadership (Farh et al. 2000). This triad model of PL is widely adopted in the PL studies (Pellegrini and Scandura 2008).

Existing literatures have mentioned that PL can influence employees' general Compliance (Aycan 2006; Aycan et al. 2000; Cheng et al. 2004; Farh 2006; Pellegrini and Scandura 2006). However, findings in existing researches are neither enough nor accurate to explain how PL affects employees' Compliance in the information security context. Firstly, the relationship between PL and employees' Compliance is not adequately addressed and that the findings are not conclusive. Studies that have investigated the impact of PL on general Compliance are scant with only a few exceptions (Cheng et al. 2004; Farh 2006; Niu et al. 2009). In these studies, Compliance is often mentioned as a result of the AL. Though some researchers tested the impact of all PL dimensions on employees' Compliance, the theoretical argumentation about BL and ML is missing (Cheng et al. 2004; Niu et al. 2009). Meanwhile, the findings of these existing studies are inconsistent. Cheng et al. (2004) found that AL and ML had significant influences on Compliance while BL didn't have significant impact. In the work of Niu et al. (2009), AL showed no significant influence on employees' Compliance while the impact of BL and ML are significant. Secondly, conclusions found in general Compliance have limited implication for Compliance in the information security context. First, the measurement of general Compliance can be problematic. For example, when asked to report their general Compliance, employees may think of different policies or requirements or have different standards to rate their general Compliance. Thus, the findings from the general Compliance may be inaccurate. Second, findings in the general Compliance studies may be unable to explain the Compliance in some specific contexts. A high general Compliance score doesn't mean high Compliance in ISP. Employees who are non-compliant with ISP but comply with most of the policies will still report high score in general Compliance. Third, in different Compliance contexts, employees may have different considerations. The influencing factors of employees' Compliance decisions may also be different. Hence, the impact of PL dimensions may be contingent on the context. Discussion regarding the features of the information security context needs to be made to offer in-depth explanation about the impact of PL on employees' ISP Compliance. Therefore, we develop the current research to investigate how PL functions on Compliance in a specific context.

Information Security Control Mechanisms

Sanction Perceptions

Sanctions, also called punishment and penalties, is suggested as a primary formal control mechanism to reduce employees' IT misuse (Straub 1990). Sanction perceptions includes the perceptions about Sanction Severity and Sanction Certainty. Sanction Severity refers to the individual's belief that deviant behaviors will be harshly punished. Sanction Certainty refers to the individual's belief of the probability that deviant behaviors will be punished. According to the General Deterrence Theory (GDT) (Gibbs 1975), when one perceives that the Sanction Severity and Certainty are high, the unacceptable behavior decreases. GDT is based on the notion that people make rational choice for their behavior, when the fear and anxiety brought by Sanctions towards misconduct overweight the potential benefit, people would modify their behavior to be proper. Straub (1990) argued that stressing the Sanctions for ISP non-Compliance can help reduce employees' violation to ISP. Numerous later researches also proved the effectiveness of Sanctions in motivating employees' ISP Compliance (Chen

et al. 2012; D'Arcy et al. 2009; Herath and Rao 2009a; Herath and Rao 2009b; Hovav and D'Arcy 2012; Johnston et al. 2015). Researchers have also showed that organizations can utilize other measures, such as procedural countermeasures (security polices and SETA program) and technical countermeasures (monitoring and auditing), to increase employees' perceptions of Sanction Severity and Certainty which could further deter ISP violation (D'Arcy et al. 2009; Hovav and D'Arcy 2012)..

Leadership styles can greatly affect the adoption and implementation of the Sanction mechanism, which makes Sanction perception a promising mediator for our research. We argue that leaders influence employees' perceptions about Sanctions in the following aspects. First, leaders may hold different preferences for adopting Sanctions (Kelman and Hong 2016). As describe by Truss et al. (1997), there are two major managerial control approaches in HRM, hard approach and soft approach. Leaders who adopt the hard approach prefer to utilizing tight control strategies to pressure employees to behave properly, such as monitoring and punishment. While for leaders who adopt the soft approach, they prefer not to compel their employees by their superior authority but to influence employees by nurturing their commitment to work (Kelman and Hong 2016; Truss et al. 1997). Second, leaders' activeness in management style affect the monitoring and detection of unexpected behavior. According to Hinkin and Schriesheim (2008), active leaders will closely observe their subordinate and interfere timely when employees' perform deviant behavior while passive leader will not take action until the problems are apparent. For example, transactional leadership tend to monitor employees proactively and take quick action to correct misconduct (Bass et al. 2003). While leaders of laissez-fair leadership usually show no response to the performance of employees (Hinkin and Schriesheim 2008). Leaders of this type would neither adopt punishment or reward as incentives to influence employees' behavior nor spend energy monitoring employees' behavior. Besides, active leaders may frequently use email, newsletters and briefings to disseminate the information about Sanction mechanisms as the fear appeal for non-Compliance (D'Arcy et al. 2009; Johnston et al. 2015). Without these efforts, employees may be less informed about the Sanction they may face for their non-Compliance to ISP. Third, leaders' behavioral consistency may greatly affect the effectiveness of Sanctions. According to the study of Podsakoff et al. (2006), whether leaders implement punishment consistently for every deviant behavior and every deviant employees and whether all leaders within the organization behave consistently in punishment for the same deviant behavior may greatly affect the Sanction perceptions of employees.

Information Security Climate Perceptions

Information Security Climate perception refers to individual perception of the value of information security from the organizational policies, procedures and practices in their work environments (Chan et al. 2005; Flin et al. 2000; Goo et al. 2014; Zohar 1980). This concept was firstly proposed by Chan et al. (2005) based on the literature of safety climate (Zohar 1980), which has been shown to be a strong predictor of safety outcomes (Clarke 2006), such as employees' safety Compliance behavior (Clarke 2006; Neal et al. 2000) and lower accident rates (Clarke 2006; Zohar 2002a; Zohar and Luria 2004). Inspired by the literature of safety climate, IS researchers also have examined the role of Information Security Climate in ISP Compliance (Chan et al. 2005; Dang-Pham et al. 2015; Dang-Pham et al. 2016; Goo et al. 2014; Shih and Liou 2015). In information security context, where information security practices often conflict with other operational demands, such as productivity (Herath and Rao 2009b), employees' perception regarding the priority of information security in their organization is even more important (Zohar 2010).

leadership plays a vital role in the formation of Information Security Climate perceptions. A great amount of supporting evidences can be found in the safety climate literature. Firstly, leadership have been recognized as the key elements in the safety climate formation. The significance of leadership can be seen from the definitions of climate perceptions, in which safety climate is described as the perceived attributes of supervisory actions (Zohar 2002a), perceived management value (Neal et al. 2000), perceived management support (Flin et al. 2000) and perceived commitment and attitude of management (Zohar 1980) in emphasizing the importance of safety over other competing work demands (Clarke 2010). Secondly, other safety climate determinants, such as job challenge and autonomy, role stress and harmony and group characteristics, are also under the influence of

leadership (Clarke 2010). For example, leaders' granting work autonomy to employees, clearly expressing role expectation and priority, designing cooperative work environment, frequently communicating with employees regarding the underlying organizational values have been proved to contribute to employees' perception of the safety climate of their organization (Clarke 2010; Kuenzi and Schminke 2009). Additionally, for leaders of different leadership style, their influence on these determinants are different. For example, they may have different preferences for how much autonomy should be granted to employees or way of communication, which will result in different level of safety climate perceptions. Thirdly, past literatures have also investigated the impact of specific leadership styles on safety outcomes via the mediation of safety climate, such as transformational leadership, constructive leadership, corrective leadership and laissez-faire leadership (Zohar 2002a; Zohar and Luria 2004). In the existing Information Security Climate literature, there are also researches that proposed leadership-related concepts as the determinants of Information Security Climate, such as leadership (Dang-Pham et al. 2015), management practice, supervisory practice (Chan et al. 2005; Dang-Pham et al. 2016) and management attention (Goo et al. 2014; Shih and Liou 2015). But they haven't tested the effect of specific leadership style on Information Security Climate.

In the current research, we contend that different leaders may prefer different control mechanisms. Sanction mechanisms are likely to be adopted by authoritarian leaders who stressed unquestioned obedience of their employees (Kelman and Hong 2016). Only by closely monitoring their subordinates and employing harsh punishment for deviant behavior can they strictly control the behaviors of their employees (Cheng et al. 2004). Climate is considered as softer and slower than the Sanction mechanisms, which cannot ensure the absolute Compliance of employees. However, for benevolent leaders and moral leaders, who value the warfare of their employees and demonstrate altruism, using Sanctions or compulsory demand disobeys their management philosophy. They may choose to express expectations through the organizational climate and guide their employees to understand it and voluntarily comply. Hence, we propose to adopt Sanction and Information Security Climate to study the different influencing process of the three PL dimensions.

Hypothesis

Based on the above theoretical analysis, we develop a research model and hypotheses (Figure 1). Authoritarian Leadership describes leaders who stress the power of the authority and control over subordinates. Such leaders require the unquestioned obedience from subordinates (Farh and Cheng 2000; Farh et al. 2000). Firstly, we argue that, employees' Compliance to ISP can be just like their Compliance to all the other policies proposed by authoritarian leaders. This is because that absolute obedience and perfect completion of instructions are strongly emphasized by the commanding authoritarian leaders. Secondly, information security practices, such as the requirement of ISP Compliance, often conflict with or bring impediment to other operational demands, such as productivity (Zohar 2010). ISP are often ignored to give way to more profiting organizational objectives (Herath and Rao 2009b). On the one hand, authoritarian leaders' insistence on high-performance and intolerance to low performance push their employees to exert themselves to accomplish every assigned tasks (Niu et al. 2009). On the other hand, the strict requirement and control initiated by Authoritarian Leadership signal the significance and mandatories of complying to ISP, which reduces employees' hesitation and reluctance due to costs of time or effort in ISP Compliance. Therefore, we propose that,

Hypothesis 1a: Authoritarian Leadership positively influences employees' ISP Compliance intention.

Benevolent Leadership describes leaders who show a holistic concern to employees' well-being both in work and in their personal life (Farh and Cheng 2000; Farh et al. 2000). Therefore, the main reason for employees' Compliance is that they feel gratitude and want to reciprocate the kindness of benevolent leaders (Cheng et al. 2004). Besides, both in work and after work, benevolent leaders. Thus, employees show agreements to their leaders' decisions, support their policies and comply as expected. Fulfill their responsibility and obligation to take good care of their subordinates, which helps them gain identification and respect from subordinates (Chan et al. 2013). In the current context, information security Compliance is also driven by employees' willingness to act for the organizational

interests (Herath and Rao 2009b). Chan et al. (2013) and Mussolino and Calabro (2014) mentioned that, under the care of benevolent leaders, employees feel that they are the in-group members and closer to their organization. Thus, benevolent leaders can influence employees to turn from self-interested goals to the goals of the collective (Wu and Tsai 2012). Therefore, employees are willing to comply to ISP for protecting the organizational interests. Hence, we propose that,

Hypothesis 1b: Benevolent Leadership positively influences employees' ISP Compliance intention.

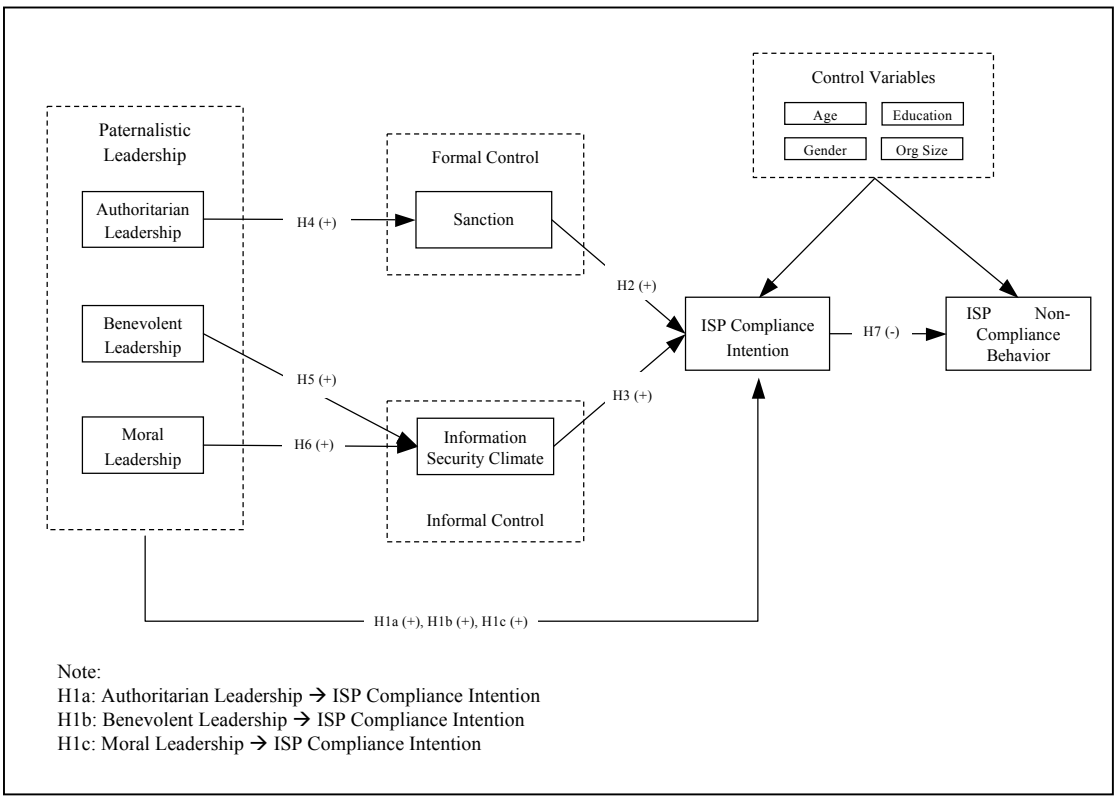

Figure 1. Research Model

Moral leaders align their behavior with moral standards and demonstrate integrity and self-discipline (Farh and Cheng 2000). Employees' responses to moral leaders include regarding them as role models, internalizing their values and imitating their behaviors (Cheng et al. 2004). Since moral leaders would comply to ISP for organizational information security, employees will learn from their moral leaders and comply in the same way (Cheng et al. 2004). Moral leaders work unselfishly to serve their organization, which cultivates an ethical work climate encouraging employee to pursuit the collectives' interests and help establish their sense of duty and normative commitment to their organization (Erben and Guneser 2008). Thus, employees may voluntarily comply to ISP because they feel morally obligated to protect their organizational interests. Moral leaders initiate respectful interactions with employees (Zhang et al. 2015). Employees feel the virtuous intention of their moral leaders and tend to support the judgement and policies of their leaders (Chan 2014). Therefore, employees are confident about their moral leaders' judgement on information security issues and show their support by complying to ISP. Hence, we propose that,

Hypothesis 1c: Moral Leadership positively influences employees' ISP Compliance intention.

According to the General Deterrence Theory (Gibbs 1975), perceived severity and certain of Sanction can deter undesired behavior. The more an individual perceived the severity and certain of Sanction, the less likely for them to conduct deviant behavior. This theory has been widely adopted to predict criminal, anti-social and deviant behavior in work place (D'Arcy et al. 2009). In the IT management context, Straub (1990) noted that the deterrence measures proposed by GDT are primary and useful strategies to deter computer abuse. Peace et al. (2003) found that the deterrence measures can

influence employees' intention of illicit software copy. Based on these works, information security researchers have also proved that Sanction perceptions positively related to employees' ISP Compliance (D'Arcy et al. 2009; Herath and Rao 2009b). In the context of information security, we argue that when employees perceived that the severity of punishment for non-Compliance is high, such as being charged, loss of job, heavy fine or other serious consequences, they will be more likely to comply to avoid the punishment (Herath and Rao 2009a). Therefore, employees' willingness to violate the ISP will decrease. Therefore, we propose that,

Hypothesis 2: employees' perceptions of Sanction positively influence their ISP Compliance.

According to the definition of James and Jones (1974), climate is considered as a perceptual media through which the objective characteristics of the working environment are translated into employees' behavior. Such definitions of climate actually imply the potential impact of climate on shaping employees' behavior. Information Security Climate originates from the safety climate literatures, which have proved as a strong predictor for safety behavior and safety accidents rate (e.g. Zohar 1980; Zohar 2002a). Especially, researchers proved that safety climate positively related safety Compliance (Clarke 2006; Kuenzi and Schminke 2009). This is because that safety climate reflects how much safety is valued by the organization and thus informs employees what behavior will be expected and rewarded, especially when formal procedures cannot be applied (e.g. Zohar 1980; Zohar 2002a). Under strong safety climate, to maintain their identity and gain supervisory approval, employees tend to conduct more safety behaviors (Zohar 2002b). Besides, Clarke (2006) argued that safe climate can help raise employees' awareness of safety knowledges, such as rules and significance of safety and reduce their skepticism about the importance and efficacy of safety measures. Employees with higher score in safety climate perceptions are more likely to work safely . Based on these evidences, IS researchers proposed and also verified the impact of Information Security Climate in employees' ISP Compliance (e.g. Chan et al. 2005; Dang-Pham et al. 2016). Therefore, we propose that,

Hypothesis 3: employees' perceptions of Information Security Climate positively influence their ISP Compliance intention.

Authoritarian leaders are very controlling and rigorous. Punishment and monitoring are often adopted by authoritarian leaders as effective mechanisms of control to ensure employees' obedience (Chan 2014; Pellegrini and Scandura 2008). According to Pellegrini and Scandura (2008), authoritarian leaders support the Theory X proposed by) which argues that employees inherently dislike work and they had to be controlled otherwise they would not work properly. Therefore, authoritarian leaders tend to adopt the hard control strategies, such as directly implementing the reward and punishment, to ensure employees' Compliance (Kelman and Hong 2016). Authoritarian leaders mostly concern about doing things in the right way and ignore the perceptions of their subordinates (Wu and Tsai 2012). Hence, authoritarian leaders may employ harsh punishment to achieve their goals regardless of the negative feelings of employees (Farh 2006; Zhang et al. 2015). Meanwhile, knowing the major concern of their authoritarian leaders, employees will tent to believe that the punishment will be very likely to happen. Hence, we propose that,

Hypothesis 4: Authoritarian Leadership positively influences employees' perception of Sanction.

Benevolent leaders show great concern to the well-being of their subordinates and are willing to exert effort to best secure their interests (Cheng et al. 2004). Therefore, benevolent leaders may tend to initiate and support a series of information security practices and nurture the corresponding climate to protect the organizational IT assets. This is because that If the organization encounters severe information security accidents, such as data breach or hacker attack, the interests of individual employee may also be threatened (Bulgurcu et al. 2010). Climate perceptions manifest the implicit values and beliefs of organizations (Ouchi 1977). However, when there are multiple competing work objectives, sometimes it is not easy for employees clearly understand the values and expectations of their organization and behavior properly (Zohar 1980). Benevolent leaders are sensitive to employees' needs and avoid putting their employees in embarrassment or dilemma (Zhang et al. 2015). Therefore, benevolent leaders would initiate a series of measures, such as training and education program,

courses, and give a special talk, to emphasize the organizational value and clearly express their expectation to employees. Hence, we propose that,

Hypothesis 5: Benevolent Leadership positively influences employees' perception of Information Security Climate.

Moral leaders feel responsible for organizational and employees' interests (Wu and Tsai 2012). Since information breach or IT attacks may cause severe loss to the organization (Chen et al. 2012), moral leaders feel it as their obligation to protect the information assets in their organization from these threats. Therefore, moral leaders take information security issues seriously and promote such value among their employees. According to Erben and Guneser (2008) , moral leaders promote their values via two-way communication and decision-makings. On the one hand, moral leaders directly explain to employees about the benefit and importance of information security to their organization. On the other hand, moral leaders may initiate a series of information security policies, procedure and practices to protect their organization. These policies and procedures inform employees which behavior will be rewarded or supported. From these behavior-outcome contingencies, employees can sense the priority of information security in their organization (Zohar 2002a). Meanwhile, this devoted effort of moral leaders also signals to employees that information security is valued in their organization. Hence, we propose that,

Hypothesis 6: Moral Leadership positively influences employees' perception of Information Security Climate.

According to Crossler and Bélanger (2014), measuring the actual security behavior is important since the ultimate goal of information security research is the behavior change. Therefore, we also include employees' actual behavior in our study. According to the Theory of Planned Behavior (Ajzen 1991), intention describes one's willingness to exert effort to perform a behavior and therefore it is a strong predictor of one's future behavior. Though most of the ISP Compliance researches only adopted intention as the indicator of actual behavior, there are also researchers who measured both the Compliance intention and actual behavior (e.g. Crossler and Bélanger 2014). These researches suggested the positive relationship between ISP Compliance intention and actual Compliance behavior. In the current research, we measured employees' non-Compliance behavior and propose that employees with high ISP Compliance intention will be less likely to conduct non-Compliance behavior.

Hypothesis 7: employees' Compliance intention negatively influences their non-Compliance behavior.

Method

A survey was conducted to collect data. All the constructs are measured by mature scales adopted from existing literature. Each item is measured by 7-point Likert scale. Minor revisions were made on the wording to make the items consistent with our research context.

To measure Paternalistic Leadership (PL), we adopted the scale from Cheng et al. (2004) and Farh et al. (2000), which measures PL from its three dimensions, Authoritarian Leadership (AL), Benevolent Leadership (BL) and Moral Leadership (ML). The scale of perceived Information Security Climate (ISC) is adopted from Chan et al. (2005). The scale of perceived Sanction (SANC) is adopted from Peace et al. (2003), which has been widely adopted in the IT security literature (e.g. D'Arcy et al. 2009; Herath and Rao 2009a). The scale of ISP Compliance Intention (CI) is adopted from Bulgurcu et al. (2010). We also asked respondents to report the frequency of their ISP violation to measure the actual Non-Compliance Behavior (NCB). To control the common method bias, we also measured employees' Social Desirability (SD) (Reynolds 1982).

In all, 760 valid questionnaires were collected. 548 questionnaires were from companies and government agencies while 222 questionnaires were from MBA and EDP classes. Since our data was collected in China, we translated the scales into Chinese using the back-translation method . A group

of IS PhD candidates were invited to help check the translation accuracy and language expressions of our questionnaire.

Results

Measurement model

We examined the Reliability and Validity of all the measured constructs in our model. All the Composite Reliability coefficients are above 0.7. The AVE of each construct is at least 0.525 (above 0.5). This means that all the constructs can explain more than half of the variances of their items. Table 1 below shows that, for each construct, its squared root of AVE is larger than its correlation with other constructs. This suggests good discriminate validity. We also conducted CFA using AMOS. The CFA model shows good model fit (CMIN/DF= 2.683, GFI=0.919, CFI=0.969, TLI=0.963, RMSEA=0.047, SRMR=0.0464) and good factor loadings of each construct. Therefore, our measurement model is valid and reliable.

Table 1. Correlations Among Major Constructs

	AL	BL	ML	ISC	SANC	CI	NCB	SD
AL	**0.724**							
BL	-0.271	**0.824**						
ML	-0.278	0.590	**0.890**					
ISC	-0.069	0.323	0.278	**0.907**				
SANC	-0.078	0.334	0.311	0.705	**0.829**			
CI	-0.042	0.304	0.333	0.426	0.482	**0.943**		
NCB	0.205	-0.095	-0.165	-0.191	-0.289	-0.544	**0.912**	
SD	0.319	-0.220	-0.319	-0.224	-0.282	-0.431	0.547	**0.730**

Note: The squared root of AVEs are bold.
ISC= Information Security Climate; SANC= Sanction;
CI= ISP Compliance Intention; NCB=Non-Compliance Behavior; SD= Social Desirability

Hypothesis testing

Our model is tested by Structural Equation Modeling using AMOS 22.0. Overall, our research model shows good model fit (CMIN/DF=2.761, GFI=0.931, CFI=0.959, TLI=0.951, RMSEA=0.048, SRMR=0.0831). The hypothesis test results are showed in Figure 2.

As shown in Figure 2, AL shows significant and positive influence on ISP Compliance Intention (β=0.278, $p<0.001$) supporting H1a. BL shows significant and positive influence on ISP Compliance Intention (β=0.193, $p<0.001$) supporting H1b. Comparing to AL and BL, ML shows weaker positive influence on ISP Compliance Intention but the path is also significant (β=0.107, $p<0.05$). Hence, H1c is supported. H2, which proposed the positive relationship between perceived Sanction and ISP Compliance Intention, is supported (β=0.158, $p<0.001$); H3, which stated that Information Security Climate positively affects ISP Compliance Intention, is also supported (β=0.161, $p<0.001$). We found that AL has positively impact on perceived Sanction (β=0.114, $p<0.01$). Therefore, H4 is supported. BL is found to have positive relationships with perceived Information Security Climate (β=0.163, $p<0.001$), which supports H5. ML shows significant relationships with perceived Information Security Climate (β=0.111, $p<0.05$), which supports H6. H7, which proposed the negative relationship between ISP Compliance Intention and ISP Non-Compliance Behavior, is also supported (β=-0.352, $p<0.001$).

For mediation effect, we performed Bootstrap to calculate the indirect effects. For AL, we found that the indirect effect from AL to CI through SANC are significant (β=0.012, $p<0.05$). For BL, we found the indirect effect of BL on CI through ISC is significant (β=0.022, $p<0.05$). For ML, the indirect effect of ML on CI through ISC is significant (β=0.008, $p<0.05$). Therefore, we conclude that the impact of AL on CI can be partially mediated by SANC, the impact of BL and ML can be partially mediated by ISC.

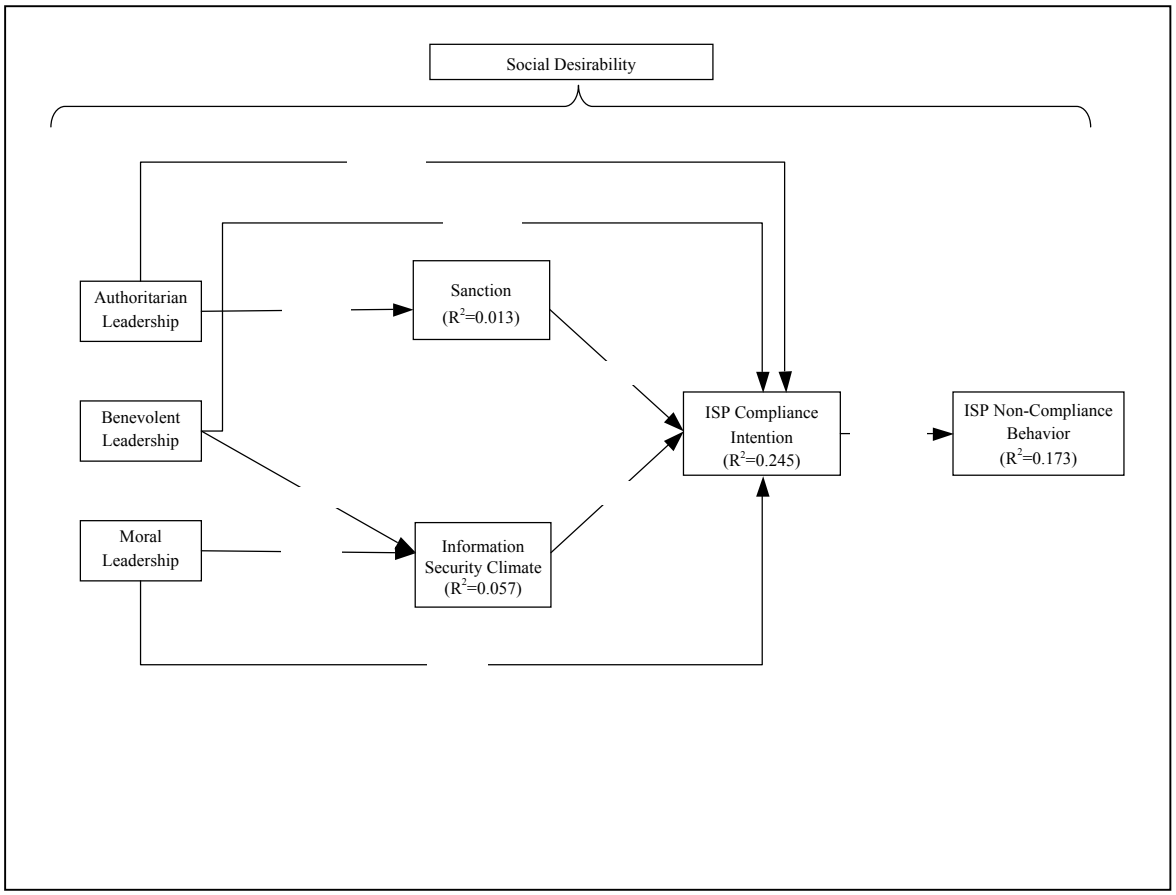

Figure 2. Model Test Results

Discussion

This research aims to further explore the role of leaders in ISP Compliance management by investigating the impact of a specific leadership style, Paternalistic Leadership, in ISP Compliance. We propose that PL can influence employees' perceptions about the information security control mechanisms in their organizational, such as employees' perceptions of Sanction and Information Security Climate, and then further affect employees' decisions in ISP Compliance. The findings of our research show that employees' perceptions of Sanction and Information Security Climate have significant and positive relationship with their ISP Compliance intention, which is consistent with previous literature (e.g. Chan et al. 2005; D'Arcy et al. 2009; Herath and Rao 2009a). More importantly, we proved that different PL dimensions affect employees' ISP Compliance through different information security control mechanism. The impact of AL can be partially mediated by employees' perception of the Sanction mechanism while the impact of BL and ML can be partially mediated by employees' perception of the Information Security Climate. This finding suggests that different leadership style functions through different control mode or control mechanisms to influence employees' ISP Compliance.

Theoretical Contribution

Our research contributes to the literature in the following aspects. Firstly, for the information security literature, we introduced in the leadership style perspective and proved the necessity to study employees' ISP Compliance from this perspective. Our findings show that all the PL dimensions, AL, BL and ML, have significant positive influence on employees' ISP Compliance intention. This suggests that leaders who score high in these leadership styles will have stronger effect on employees' ISP Compliance. This finding offers a possible explanation about why some leaders are more effective than others in motivating employees' ISP Compliance. Previous literature mostly stressed the more leaders involved in information security management, the better they can motivate employees' ISP

Compliance (Chan et al. 2005; Hu et al. 2012). While our study shows that leadership style also matters. We found that the extent to which leaders demonstrate the features of certain leadership styles, such as PL or its sub-dimension leadership styles, will affect their influence on employees' ISP Compliance intention. This is a new perspective to understand the impact of leaders on employees' ISP Compliance. By focusing on leadership style, i.e., the behavioral features of leaders, we can provide more implications to leaders about how to effectively behave when they participate, support and initiate practices in information security management.

Secondly, our research proves that leadership styles influence employees' ISP Compliance via the mediation of employees' perceptions of the control mechanisms. This finding has two implications. First, the control mechanisms offer us a new perspective to understand the process of how leaders motivate employees' ISP Compliance. As our findings show, the impact of AL can be mediated by employees' perception of the Sanction mechanism and the impact of BL and ML can be mediated by employees' perception of the Information Security Climate. Despite the specific mediators from AL, BL and ML to ISP Compliance are not totally the same, their underlying influencing mechanism are the same. All these paths suggest that leaders can affect employees' ISP Compliance by carrying out or affecting the implementation of the information security control mechanisms, which expands our knowledge about the influencing process of leaders on ISP Compliance. Therefore, not only for PL, when studying the impact of different leadership styles on ISP Compliance, researchers may try firstly looking at how the leaders adopt and implement the information security control mechanisms. Previous information security researchers rarely took the control mechanisms perspective to examine the impact of leaders. They mostly adopted employees' cognitive factors about ISP Compliance, such as attitude, subjective norm, perceived behavioral control, self-efficacy etc., as the influencing mechanisms to study how leaders affect employees' ISP Compliance (Hu et al. 2012; Humaidi and Balakrishnan 2018). Though Chan et al. (2005) have considered one control mechanism, the Information Security Climate, as the mediator to examine the impact of leaders practices in ISP Compliance, the difference in leaders was not discussed.

Second, the information security control mechanisms perspective also helps to explain how different leadership styles functions to motivate employees' ISP Compliance. Our research shows that the specific mediating control mechanisms between PL dimensions and employees' ISP Compliance are not the same. AL influences employees' ISP Compliance via the Sanctions mechanism while BL and ML function through the Information Security Climate. This may be due to that different leadership styles have different preferences in the adoption of control mechanisms. Or that, while implementing certain control mechanisms, the behavioral styles of leaders affect employees' perception of the real existence and intensity of the control mechanisms. In previous literature where the difference of leaders is ignored, all leaders were assumed to function in the same process to influence employees' ISP Compliance (Chan et al. 2005; Hu et al. 2012). While our research proves that leaders with different leadership style, they may function through different control mechanisms.

Managerial Implication

Our research also has implications to the information security management practices. Firstly, our research shows that leadership style matters in the information security management. Which leadership style is adopted and to what extend the leaders perform the leadership style will affect employees' information security behavior? Our research proves that the three dimensions of Paternalistic Leadership, Authoritarian Leadership, Benevolent Leadership and Moral Leadership, all have significant and positive influence on employees' ISP Compliance. Hence, PL combined by AL, BL and ML, and its single dimension, are beneficial for the information security management in organizations. Organizations can design training programs to arouse leaders' attention to their leadership styles and help them develop and apply proper leadership styles in information security management.

Secondly, our research shows that AL facilitates employees' perception of the Sanction mechanism. Therefore, leaders can treat their employees in the authoritarian way to increase employees' perception of the Sanction for ISP violation. For example, leaders can require unquestioned obedience of employees, rigorously monitor their employees' behavior, execute punishment once violation is

caught, express that they want everything to be done in the best way they see and show no tolerance to deviant behaviors, etc. All these efforts will make employees perceive that ISP violation will be easily caught and will face severe consequences once caught.

Thirdly, we also found that Information Security Climate can be increased by BL and ML. This suggests that there are two ways for leaders to cultivate the Information Security Climate in their organization. For example, leaders can nurture the climate by offering supporting programs, such as the security education, training and awareness program, and an open communication working environment, to assist employees to make sense of how information security is valued by their organization. In addition, leaders can deliver the value of information security by showing their good virtue and morality (Cheng et al. 2004). Employees who regard their moral leaders as role models will learn from their leaders to concern about the collective interests and develop the sense of duty to their organization (Erben and Guneser 2008), which will motivate them to make sense of the promoted values and priorities of their organization and protect their organizational information assets.

Conclusion

Our study examined the impact of Paternalistic Leadership on employees' ISP Compliance. We propose that, besides the direct impact, PL dimensions can influence ISP Compliance by carrying out information security control mechanisms, such as Sanction and Information Security Climate. Our research model is tested by survey data from 760 employees. We found that all PL dimensions have positive direct impact on employees' ISP Compliance. For different PL dimension, their mediating control mechanisms are not all the same. The impact of AL is mediated by employees' perception of the Sanction mechanism while the impact of BL and ML are mediated by employees' perception of the Information Security Climate.

Reference

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational behavior and human decision processes* (50:2), pp. 179-211.

Aycan, Z. 2006. "Paternalism," in *Indigenous and Cultural Psychology*. Springer, pp. 445-466.

Aycan, Z., Kanungo, R., Mendonca, M., Yu, K., Deller, J., Stahl, G., and Kurshid, A. 2000. "Impact of Culture on Human Resource Management Practices: A 10-Country Comparison," *Applied Psychology* (49:1), pp. 192-221.

Bass, B. M., Avolio, B. J., Jung, D. I., and Berson, Y. 2003. "Predicting Unit Performance by Assessing Transformational and Transactional Leadership," *Journal of applied psychology* (88:2), p. 207.

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* (34:3), pp. 523-548.

Chan, M., Woon, I., and Kankanhalli, A. 2005. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of information privacy and security* (1:3), pp. 18-41.

Chan, S. C., Huang, X., Snape, E., and Lam, C. K. 2013. "The Janus Face of Paternalistic Leaders: Authoritarianism, Benevolence, Subordinates' Organization-Based Self-Esteem, and Performance," *Journal of Organizational Behavior* (34:1), pp. 108-128.

Chan, S. C. H. 2014. "Paternalistic Leadership and Employee Voice: Does Information Sharing Matter?," *Human Relations* (67:6), pp. 667-693.

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

Cheng, B. S., Chou, L. F., Wu, T. Y., Huang, M. P., and Farh, J. L. 2004. "Paternalistic Leadership and Subordinate Responses: Establishing a Leadership Model in Chinese Organizations," *Asian Journal of Social Psychology* (7:1), pp. 89-117.

Clarke, S. 2006. "The Relationship between Safety Climate and Safety Performance: A Meta-Analytic Review," *Journal of Occupational Health Psychology* (11:3), pp. 315-327.

Clarke, S. 2010. "An Integrative Model of Safety Climate: Linking Psychological Climate and Work Attitudes to Individual Safety Outcomes Using Meta-Analysis," *Journal of Occupational and Organizational Psychology* (83:3), pp. 553-578.

Crossler, R., and Bélanger, F. 2014. "An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (Usp) Instrument," *ACM SIGMIS Database* (45:4), pp. 51-71.

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* (20:1), pp. 79-98.

Dang-Pham, D., Pittayachawan, S., and Bruno, V. 2015. "Investigating the Formation of Information Security Climate Perceptions with Social Network Analysis: A Research Proposal," *PACIS*.

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

Erben, G. S., and Guneser, A. B. 2008. "The Relationship between Paternalistic Leadership and Organizational Commitment: Investigating the Role of Climate Regarding Ethics," *Journal of Business Ethics* (82:4), pp. 955-968.

Farh, J.-L., and Cheng, B.-S. 2000. "A Cultural Analysis of Paternalistic Leadership in Chinese Organizations," in *Management and Organizations in the Chinese Context*. Springer, pp. 84-127.

Farh, J. L., Cheng, B. S., Chou, L. F., & Chu, X. P. 2006. "Authority and Benevolence: Employees' Responses to Paternalistic Leadership in China," in *China's Domestic Private Firms: Multidisciplinary Perspectives on Management and Performance. New York: Me Sharpe,* Y.B. A. S. Tsui, & L. Cheng (ed.). New York: Sharpe, pp. 230-260.

Farh, L. J., Cheng, B., and Chou, L. 2000. "A Triad Model of Paternalistic Leadership: Constructs and Measurement," *Indigenous psychological research in Chinese societies* (14), p. 3.

Flin, R., Mearns, K., O'Connor, P., and Bryden, R. 2000. "Measuring Safety Climate: Identifying the Common Features," *Safety science* (34:1), pp. 177-192.

Gibbs, J. P. 1975. *Crime, Punishment, and Deterrence*. Elsevier New York.

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* (57:4), pp. 286-308.

Griffin, M. A., and Hu, X. 2013. "How Leaders Differentially Motivate Safety Compliance and Safety Participation: The Role of Monitoring, Inspiring, and Learning," *Safety science* (60), pp. 196-202.

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

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

Hinkin, T. R., and Schriesheim, C. A. 2008. "An Examination of" Nonleadership": From Laissez-Faire Leadership to Leader Reward Omission and Punishment Omission," *Journal of Applied Psychology* (93:6), p. 1234.

Hovav, A., and D'Arcy, J. 2012. "Applying an Extended Model of Deterrence across Cultures: An Investigation of Information Systems Misuse in the Us and South Korea," *Information & Management* (49:2), pp. 99-110.

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* (43:4), pp. 615-660.

Humaidi, N., and Balakrishnan, V. 2018. "Indirect Effect of Management Support on Users' Compliance Behaviour Towards Information Security Policies," *Health Information Management Journal* (47:1), pp. 17-27.

James, L. R., and Jones, A. P. 1974. "Organizational Climate: A Review of Theory and Research," *Psychological bulletin* (81:12), p. 1096.

Johnston, A. C., Warkentin, M., and Siponen, M. T. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.

Kelman, S., and Hong, S. 2016. ""Hard,""Soft," or "Tough Love" Management: What Promotes Successful Performance in a Cross-Organizational Collaboration?," *International Public Management Journal* (19:2), pp. 141-170.

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., and Nelson Ford, F. 2006. "Information Security: Management's Effect on Culture and Policy," *Information Management & Computer Security* (14:1), pp. 24-36.

Kuenzi, M., and Schminke, M. 2009. "Assembling Fragments into a Lens: A Review, Critique, and Proposed Research Agenda for the Organizational Work Climate Literature," *Journal of management* (35:3), pp. 634-717.

Moody, G. D., Siponen, M., and Pahnila, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *Mis Quarterly* (42:1), pp. 285-+.

Mussolino, D., and Calabro, A. 2014. "Paternalistic Leadership in Family Firms: Types and Implications for Intergenerational Succession," *Journal of Family Business Strategy* (5:2), pp. 197-210.
Neal, A., Griffin, M. A., and Hart, P. M. 2000. "The Impact of Organizational Climate on Safety Climate and Individual Behavior," *Safety science* (34:1), pp. 99-109.
Niu, C. P., Wang, A. C., and Cheng, B. S. 2009. "Effectiveness of a Moral and Benevolent Leader: Probing the Interactions of the Dimensions of Paternalistic Leadership," *Asian Journal of Social Psychology* (12:1), pp. 32-39.
Ouchi, W. G. 1977. "The Relationship between Organizational Structure and Organizational Control," *Administrative science quarterly*), pp. 95-113.
Ouchi, W. G., and Maguire, M. A. 1975. "Organizational Control: Two Functions," *Administrative Science Quarterly* (20:4), pp. 559-569.
Peace, A. G., Galletta, D. F., and Thong, J. Y. 2003. "Software Piracy in the Workplace: A Model and Empirical Test," *Journal of Management Information Systems* (20:1), pp. 153-177.
Pellegrini, E. K., and Scandura, T. A. 2006. "Leader–Member Exchange (Lmx), Paternalism, and Delegation in the Turkish Business Culture: An Empirical Investigation," *Journal of international business studies* (37:2), pp. 264-279.
Pellegrini, E. K., and Scandura, T. A. 2008. "Paternalistic Leadership: A Review and Agenda for Future Research," *Journal of Management* (34:3), pp. 566-593.
Podsakoff, P. M., Bommer, W. H., Podsakoff, N. P., and MacKenzie, S. B. 2006. "Relationships between Leader Reward and Punishment Behavior and Subordinate Attitudes, Perceptions, and Behaviors: A Meta-Analytic Review of Existing and New Research," *Organizational Behavior and Human Decision Processes* (99:2), pp. 113-142.
Reynolds, W. M. 1982. "Development of Reliable and Valid Short Forms of the Marlowe-Crowne Social Desirability Scale," *Journal of Clinical Psychology* (38:1), pp. 119-125.
Shih, S.-P., and Liou, J.-Y. 2015. "Investigate the Effects of Information Security Climate and Psychological Ownership on Information Security Policy Compliance," *PACIS*, p. 28.
Straub, D. W. 1990. "Effective Is Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.
Truss, C., Gratton, L., Hope-Hailey, V., McGovern, P., and Stiles, P. 1997. "Soft and Hard Models of Human Resource Management: A Reappraisal," *Journal of Management Studies* (34:1), pp. 53-73.
Veiga, A. D., and Eloff, J. H. 2007. "An Information Security Governance Framework," *Information Systems Management* (24:4), pp. 361-372.
Weber, M. 1968. "The Types of Legitimate Domination," in *Economy and Society,* G.R.C. Wittich (ed.). New York: Bedminster, pp. 212-216.
Westwood, R. I. 1992. "Headship and Leadership," in *Organisational Behaviour: Southeast Asian Perspectives,* R.I. Westwood (ed.). Hong Kong : Longman: pp. 118-143.
Wu, Y. C., and Tsai, P. J. 2012. "Multidimensional Relationships between Paternalistic Leadership and Perceptions of Organizational Ethical Climates," *Psychological Reports* (111:2), pp. 509-527.
Zhang, Y., Huai, M. Y., and Xie, Y. H. 2015. "Paternalistic Leadership and Employee Voice in China: A Dual Process Model," *Leadership Quarterly* (26:1), pp. 25-36.
Zohar, D. 1980. "Safety Climate in Industrial Organizations: Theoretical and Applied Implications," *Journal of applied psychology* (65:1), p. 96.
Zohar, D. 2002a. "The Effects of Leadership Dimensions, Safety Climate, and Assigned Priorities on Minor Injuries in Work Groups," *Journal of Organizational Behavior* (23:1), pp. 75-92.
Zohar, D. 2002b. "Modifying Supervisory Practices to Improve Subunit Safety: A Leadership-Based Intervention Model," *Journal of Applied psychology* (87:1), p. 156.
Zohar, D. 2010. "Thirty Years of Safety Climate Research: Reflections and Future Directions," *Accident Analysis & Prevention* (42:5), pp. 1517-1522.
Zohar, D., and Luria, G. 2004. "Climate as a Social-Cognitive Construction of Supervisory Safety Practices: Scripts as Proxy of Behavior Patterns," *Journal of applied psychology* (89:2), p. 322.