Transformational Leadership and Employees' Information Security Performance: The Mediating Role of Motivation and Climate

Completed Research Paper

Benedikt Lebek
Leibniz Universität Hannover
Königsworther Platz 1,
30167 Hannover, Germany
lebek@iwi.uni-hannover.de

Nadine Guhr
Leibniz Universität Hannover
Königsworther Platz 1,
30167 Hannover, Germany
guhr@iwi.uni-hannover.de

Michael H. Breitner
Leibniz Universität Hannover
Königsworther Platz 1,
30167 Hannover, Germany
breitner@iwi.uni-hannover.de

Abstract

The importance of organizational information security is constantly increasing. Next to technical information security measures, research has incorporated multidisciplinary behavioral theories in order to explain employees' information security awareness and behavior. While focusing on employees as the weakest link in the information security chain, the role of leadership has been considered less. To address this gap, the purpose of this explorative study is to investigate how transformational leadership can influence employees' information security performance. A research model is developed that is empirically tested by means of structural equation modeling (SEM) with data collected from 208 employees across different industries. Our results indicate a significant influence of transformational leadership on employees' information security participation. Moreover, our study reveals that transformational leaders are able to form a positive organizational climate towards information security and thereby (indirectly) enhance employees' motivation. Drawing from our findings, implications for practitioners and future IS research are derived.

Keywords: Information security, employees' security behavior, transformational leadership, security motivation, security climate, structural equation modeling

Introduction

Information system (IS) security has received much attention in popular media and trade journals throughout the past decade (Boss et al. 2009), since information security breaches cause hundreds of billions US Dollars of annual worldwide economic damage (D'Arcy et al. 2009; D'Arcy and Hovav 2011). Consequently, ensuring information security has become critically important and is considered to be one of the top management priorities in many organizations (Kirsch and Boss 2007; Bulgurcu et al. 2010; D'Arcy and Herath 2011; Herath and Rao 2009). To mitigate threats to information security, organizations primarily focus on technology-based solutions (Boss et al. 2009; Bulgurcu et al. 2010). However, the majority of serious IS security breaches originates from inside organizations due to employees' failure to comply with basic security procedures (Siponen and Vance 2010; Karjalainen and Siponen 2011). Literature often refers to employees as the weakest link in IS security (e.g., Spears and Barki 2010; Siponen et al. 2006), forcing organizations to focus not only on technological tools for information security, but also "on other formal and informal control mechanisms, including policies, procedures, organizational culture, and the role individuals play in security" (Herath and Rao 2009b). Organizations commonly establish information security policies that provide employees with guidelines on how to ensure information security in the course of performing their jobs (Bulgurcu et al. 2010). However, the lack of employees' awareness of the importance of security practices or the lack of motivation to comply with the security policies, can render these efforts ineffective (Herath and Rao 2009b). A major challenge for organizations is to find an effective way to promote security policies to individual employees. In this context, not only the design of security policies, but also the motivation of individuals to follow those policies is of high importance (Boss et al. 2009).

Due the shift in focus toward individual perspectives, employees' information security awareness and behavior and the resulting (non-)compliance with information security policies is considered a key socio-organizational resource (Bulgurcu et al. 2010; Siponen and Vance 2010) that has garnered increasing academic attention over the last ten years. In this interdisciplinary research domain, theories from social psychology and criminology were adopted to IS literature (Mishra and Dhillon 2005) in order to explain and predict employees' security-related behavior and awareness. Studies show a significant influence of employees' subjective norms, perceived ability to cope with threats, perceived severity of threats, and perceived severity and certainty of sanctions in case of uncompliant behavior on their intention to comply with organizational information security policies (Lebek et al. 2013). In addition to focusing on employees' perspective within the context of information security, IS security researchers also considered the impact of differences in management (Uffen et al. 2012).

Introduced by Bass (1985), transformational leadership has been recognized by both scholars and practitioners as a way to positively influence employee attitudes, behavior, and performance (Walumbwa et al. 2008) and to encourage employees to perform beyond expectations (Rafferty and Griffin 2004). The purpose of this study is to investigate how transformational leaders influence employee performance in the context of information security. Employees' information security performance is defined as a bi-dimensional aspect comprising security compliance and security participation. The first term refers to employees' intention to meet minimum information security standards, and the second refers to behavior that actively supports information security, such as helping co-workers with information security related issues or promoting the necessity of security measures (Innes et al. 2010). Although transformational leadership has been proven to enhance organizational and IT effectiveness (e.g. Cho and Park 2007), the question arises whether these findings can be adopted to the information security field mainly due to two reasons. First, information security is not directly generating business value. Second, employees' often see information security as inconvenient and in contrast to work efficiency and productivity (Chan et al. 2005). This study investigates the following research question:

RQ: How does transformational leadership influence employees' information security performance?

The paper is structured as follows: In the first section we provide the theoretical basis and identify the targeted research gap. In this context, a research model is developed and hypotheses are deduced from academic literature. Subsequently, the research design and methodology are described. After presenting the data analysis procedure, we report the results. Following the discussion and implications for research and practice, we conclude by pointing out limitations and giving an outlook for future research.

Theoretical Background and Hypotheses

Behavioral Theories in Information Security Research

IS researchers have incorporated multidisciplinary theories from psychology, sociology, and criminology into behavioral information security success outcome models. The most frequently applied theories in the examined research field are the theory of reasoned action/theory of planned behavior, general deterrence theory, and protection motivation theory (Lebek et al. 2013).

Founded by Fishbein and Ajzen (1975), the theory of reasoned action postulates that a person's behavioral intention depends on his or her subjective norm and attitude towards a certain behavior. By adding the construct of perceived behavioral control, the theory of planned behavior (Ajzen 1985 & 1991) expands the theory of reasoned action in order to improve its predictive power. In the context of employee information security awareness and behavior, researchers emphasize the use of employees' behavioral intention to comply with organizational information security policies as a predictor of actual employee behavior (e.g., Limayem and Hirt 2003; Pahnila et al. 2007) due to certain difficulties with observing actual security compliant behavior (Vroom and von Solms 2004). Several studies show a significant relationship between perceived behavioral control (e.g. Bulgurcu et al. 2010; Dinev et al. 2009; Johnston and Warkentin 2010), subjective norms (e.g. Bulgurcu et al. 2010; Pahnila et al. 2007; Siponen et al. 2010) and attitude (e.g. Ifinedo 2012; Hu and Dinev 2007) and employees' intention to comply with information security policies.

Originating from health psychology, the protection motivation theory was introduced by Rogers (1975) and later revised by Rogers (1983) by emphasizing the cognitive process that mediates behavioral change. The theory aims to explain whether a person's attitudes and behaviors are influenced directly or indirectly by fear appeals. A significant relationship of the theory's core constructs to employees' intention towards information security was demonstrated by several studies (see Lebek et al. 2013). While Ifinedo (2012) investigated a significant relationship by separation of perceived severity and perceived vulnerability as threat appraisal constructs e.g. Pahnila et al. (2007) and Siponen et al. (2010) considered the whole construct. The authors show that threat appraisal is a predictor of employees' intention to comply with organization security policies. Response efficacy and self-efficacy have been proven to be significant for employees' compliance intention (e.g. Ifinedo 2012; Johnston and Warkentin 2010).

Adapted from criminal justice research, deterrence theory states that persons are deterred from committing criminal behavior if they perceive sanctions to be certain and severe. In addition, classic conceptualization of deterrence theory also includes celerity of sanctions as a third component. However, due to measurement difficulties and the lack of its theoretical importance, IS studies did not include the celerity construct (D'Arcy and Herath 2011). Employees' information security awareness and behavior mainly utilizes general deterrence theory, including formal sanctions. Employees' decisions regarding the intention to comply with information security policy compliance is the result of balancing the possible cost and benefits of different behavioral alternatives (Bulgurcu et al. 2010; D'Arcy et al. 2009). The constructs of perceived severity of sanctions and perceived certainty of sanctions were related to behavioral intention (D'Arcy et al. 2009; Herath and Rao 2009b; Hovav and D'Arcy 2012; Xue et al. 2011). Although deterrence theory was frequently used within the information security behavior research, it "has received mixed support in the IS security literature" (D'Arcy and Herath 2011).

Leadership in Information Security Research

In the area of information security research, the role of managers in the information security chain has received little attention, as studies mainly focus on the employee perspective (Uffen et al. 2013). With regard to management involvement in the context of information security, literature emphasizes the importance of CIOs and IT executives in developing and maintaining a culture of compliance in order to achieve information security effectiveness (Stewart and Thelander 2005). For example, Broadbent and Kitzis (2004) pointed out that the success of CIOs depends on their ability to go beyond pure management and lead by setting expectations and influencing others to change. The main challenges for IT leaders is to balance in terms of cutting costs and promote innovation, and to develop trust and relationships. Therefore interpersonal skills are critical factors for CIOs in order form alliances and partnerships, with the business leaders and other functional leaders (Stewart and Thelander 2005).

Not only does leadership play an important role on CIOs and IT executive level, it is also relevant on a corporate and business level. Beginning with senior management, organizations have to aim to establish a leadership style that perceives information security as an important issue and forms a security culture throughout the organizational levels (Dutta and McCrohan 2002). Focusing on small and medium enterprises, Dojkovski et al. (2007) identified several attributes of managerial leadership that influence organizational information security outcomes. Accordingly, leaders must act as role models with regard to information security and take initiative in order to be informed about information security topics and develop governance structures for maintaining adequate information security. Mishra and Dhillon (2005) emphasize that top management accountability is a crucial factor for effective information security. The authors split managerial information security responsibilities into formal and informal measures. Formal measures include, for example, the creation and implementation of security policies, the assessment of internal control mechanisms, the promotion of group behavior, and the development of a leadership style that promotes compliant behavior and carries out strong measures against non-compliant behavior. Research on leadership style has demonstrated that using punishment as a negative stimulus is an effective way of enhancing employee job performance and reducing undesirable behavior when a punishment expectancy has developed among employees (Xue et al. 2011). The informal side of managerial information security measures is about the creation of an organizational culture that recognizes the importance of information security by considering prevalent norms, individual believes, and personal values of employees (Mishra and Dhillon 2005).

Considering the behavioral theories previously mentioned in this section, it can be assumed that a laissez-faire style of leadership and management attitude with regard to employee security awareness and behavior is not effective. Laissez-faire leaders tend to avoid corrective actions (Bass et al. 1987) and wait until deviations and errors occur before taking actions (Stewart 2006). Studies demonstrate that this type of leadership style does not cause the guidelines to be followed properly due to a lack of employee motivation. (Siponen and Kajava 1998). To increase employees' intrinsic motivation and intention to comply with information security policies, certain leadership soft skills and a healthy organizational culture are imperative factors and a basic precondition (Siponen 2000). This is consistent with Collins (2001), who identified key strategies for successful leaders: "a focus on natural talent; passionate interest and well rewarded activity [and] a culture of discipline. People come first and their efforts good or bad are amplified" (Stewart and Thelander 2005). Considering the previous research in this area, it is clear that the relationship of leadership styles and employees' information security awareness and behavior needs further investigation.

Transformational Leadership

The concept of transformational leadership goes back to the theoretical ideas of Burns (1978) in the context of political leadership. Burns (1978) stated that two forms of leadership styles exist. Accordingly the leadership process can occur in a transactional way or a transformational way. Both kinds of leadership styles differ in the relationship between leaders and followers.

Transactional leadership aims to motivate followers by helping them to fulfill their own self-interests (Sadgehi 2012) as they use conventional reward (or punishment) in exchange for (not) achieving previously defined performance goals (Jung and Sosik 2002; Rafferty 2004; Yukl 2006). There are three dimensions of transactional leadership behavior: contingent reward (or punishment), management-by-exception and laissez-faire leadership (Avolio et al. 1999; Bono and Judge 2004; Stewart 2006). Transactional leadership is sufficient for maintaining the current situation in organizations (Geijsel 2003; Sadgehi 2012).

Whereas transactional leadership addresses followers' selfish concerns, transformational leadership addresses social values and encourages people to collaborate, rather than work as individuals (Burns 1978). They use charismatic methods to attract people to the leader and convey the value and importance of desired outcomes to their followers. They stimulate their followers to transcend their self-interest for the interest of their groups or organizations and thus facilitate a collective motivation (Jung and Sosik 2002). Four specific components of transformational leadership have been identified: (1) idealized influence, (2) inspirational motivation, (3) intellectual stimulation, and (4) individualized consideration (Geijsel 2002; Jung 2002; Bass 2003). *Idealized influence* refers to the degree to which a leader displays behavior that causes followers to identify with the leader. Leaders possess a clear set of values like high ethical and moral standards (Bono and Judge 2004) and considers the needs of their followers over their own (Bass 2003). *Inspirational motivation* deals with ways leaders motivate followers and generate optimism (Stewart 2006). Leaders with inspirational motivation challenge followers to uphold high standards, communicate an optimistic vision, and speak optimistically about the future. Leaders attract enthusiasm and energize their followers (Rafferty 2004; Liu 2010). Through *intellectual stimulation*, leaders encourage followers to question established methods and organizational norms and to get a new perspective on a problem (Bass et al. 1987; Avolio et al. 1999). Thereby leaders push followers to develop innovative strategies and to improve existing methods (Bono and Judge 2004). *Individualized consideration* refers to the degree of leaders' concern about their followers' needs and interests (Liu 2010). By establishing a supportive climate and providing coaching and mentoring, leaders help followers raise their personal abilities and potential (Stewart 2006; Geijsel 2002). Hence, transformational leaders not only recognize and satisfy followers' current needs, they also elevate those needs in order to personally develop followers (Bass et al. 1987).

Based on Burns' work, Bass (1985) introduced a model of transformational leadership that was later adopted into organizational psychology research. In contrast to Burns (1978), who considered transactional and transformational leadership to be at opposite ends of a continuum, Bass (1985) sees them as separate leadership dimensions that aim to achieve goals of leaders, followers, and organizations. Accordingly, leaders can be transactional and transformational at the same time. Transformational leadership is not a substitute for transactional leadership, but a special form of transactional leadership (Den Hartog et al. 1997). For example a leader can display all the qualities of a transformational leader in order to enhance employees' willingness to show greater commitment and work performance. However, that leader may still use the corrective actions of a transactional leader (i.e., punishment) if employees fail to meet performance goals (Avolio and Bass 2004).

Hypothesis Generation

Transformational leaders are capable of directing their organizations to effectiveness and productivity, and to produce greater effects than transactional leaders (Sadgehi and Lope 2012). Past research has demonstrated that transformational leadership is positively related to IS effectiveness, as this leadership style enhances employees' organizational commitment and performance (Cho and Park 2007). Effectiveness in the context of organizational information security has been widely discussed in previous studies. Hagen et al. (2008) defined effectiveness as the positive influence of a security measure on individual and organizational security awareness and behavior. In the context of this study, we refer to organizational information security policies as a fundamental security measure. Accordingly, we argue that it is essential to organizational information security effectiveness that employees' security behavior be compliant with the specifications of the security guidelines (Heikka 2008; Hearth and Rao 2009a). The general goal of employees' information security awareness and behavior research is to investigate employees' actual behavior (Mehri and Ahluwalia 2013). However, previous studies on behavioral theories in the research field at hand mostly assessed behavioral intentions rather than actual behavior due to difficulties in observing employees' actual security behavior, especially in organizational settings (Vroom and von Solms 2004; Hu et al. 2012). Since Fishbein and Ajzen (1975) stated that intentions are proximal cognitive antecedents of actions or behavior, we utilized employees' intentions as the key dependent variable. Consequently, the purpose of this study is to investigate the influence of transformational leadership on employees' behavioral intention towards information security.

Employees' information security compliance intention is defined as "behavior that protects the information and technology resources of the organization from potential security breaches" (Guo 2013). The author states further that employees can have non-malicious or even beneficial motives. Accordingly, we argue that employees' behavioral intentions occur in two dimensions, namely security compliance intention and security participation intention, which together form the construct of employee security performance. Based on definitions of task performance, *security compliance intention* refers to in-role behaviors. In-role behaviors are defined as "all the behaviors that were necessary for the completion of the responsible work" (Zhu 2013) and are described within employees' formal job requirements. In the information security context, these behaviors are non-malicious, as they are focused on adhering to information security policies in order to meet minimum information security standards at work (Inness et al. 2010). This is equivalent to the key dependent variable that was mostly used in employees' information security awareness and behavior research, as mentioned earlier. However, organizations that rely mainly on in-role behaviors are prone to develop an insubstantial social system (Zhu 2013). Consequently, in order to efficiently and sustainably enhance employees' information security behavior within organizations, it is not sufficient to focus on employees' intention to comply with security measures. Extending the effects of in-role behaviors, extra-role behaviors are capable of enhancing organizational effectiveness and operational efficiency (Zhu 2013). Representing extra-role behaviors or organizational citizenship behaviors (OCBs), *security participation intention* is utilized based on definitions of contextual performance (Rafferty 2004; Clarke and Ward 2006). In contrast to in-role behaviors, extra-role behaviors include a greater voluntary element and benefit the organizational information security in contrast to just adhering to minimum standards. These behaviors include, for example, helping co-workers with information security issues or attending security training, and are not specified in employees' formal job requirements. Extra-role behavior constitutes "individual behavior that is discretionary, not directly or explicitly recognized by the formal reward system" (Organ 1988) but promotes and contributes to an environment that supports effective organizational information security (Clarke and Ward 2006; Neal and Griffin 2006). According to Podsakoff et al. (1990), the most striking benefit of transformational leaders is their ability to stimulate employees to perform beyond expectations and on contextual levels. A meta-analysis of Podsakoff et al. (2000) shows that especially two sub-dimensions of transformational leadership, namely intellectual stimulation and contingent reward, are positively associated with extra-role behaviors. Thus, we propose the following hypotheses:

> **$H1_a$:** *Transformational leadership experienced by employees has a significant positive influence on employees' intentions to comply with information security policies.*
>
> **$H1_b$:** *Transformational leadership experienced by employees has a significant positive influence on employees' intentions to participate in information security activities.*

Research has identified variables that mediate the relationship between transformational leadership behaviors and followers' behaviors. These variables include intrinsic motivation and organizational climate. Although the concept of attitude is not adopted in this study, there is a need to distinguish between attitude and motivation for the sake of clarity. Originating from the technology acceptance model, employees' attitude towards information security has been examined in numerous studies (e.g., Dinev and Hu 2007; Bulgurcu et al. 2009; Herath and Rao 2009b). Attitude reflects employees' feelings towards engaging in a specified behavior (Pahnila et al., 2007). Whereas attitude is seen as being more static in nature because it refers to the quality of actions (i.e., the perception as to whether a behavior is positive or negative), motivation refers to activity levels (i.e., the perceived importance of performing a behavior) and is seen as being more dynamic (Siponen 2000). In the context of this study, we adopted the concept of intrinsic motivation. Intrinsic motivation is defined as a behavior that is personally rewarding and leads to inherent satisfaction because it does not depend on external rewards (Brown 2007). Accordingly, employees feel free to make their own decisions by "justifying their actions in terms of internal reasons such as their own aspirations" (Siponen 2000). Charbonneau et al. (2001) demonstrated that transformational leadership influences followers' performance indirectly through the mediating effects of intrinsic motivation. Accordingly, transformational leadership enhances intrinsic motivation since transformational leaders are capable of empowering followers and promoting their autonomy. Through this empowerment process, followers' self-efficacy and capacity for self-determination, an essential component of intrinsic motivation, is increased (Deci and Ryan 1985). Several studies underlined the importance of intrinsic motivation in the context of employees' information security policy compliance behavior (most notably: Siponen 2000; Herath and Rao 2009a; Son 2011). Consequently, we propose the second hypothesis:

> **H2:** *Transformational leadership experienced by employees has significant positive influence on employees' security motivation.*

Information security research frequently utilizes subjective norms in order to explain employees' information security policy adherence (e.g., Herath and Rao 2009b; Bulgurcu et al. 2010; Aurigemma and Panko 2012). Originating from the theory of planned behavior, subjective norms reflect employees' beliefs about expectations of other people that result in the perception of social pressure to perform a certain behavior (Zhang et al. 2009; Aurigemma and Pankow 2012). In the context of information security, employees' adhere to organizational information security policies if their peers (e.g., superiors, co-workers, and friends) would like them to follow the policies (Ifinedo 2012). Transformational leaders, however, do not have to resort to pressuring employees to complying with information security policies as they are capable of conveying the value and purpose of information security to their followers. Employees' perception of values within their work environment is referred to as organizational climate (James and James 1989). In contrast to subjective norms, organizational climate has "a strategic focus, i.e., to be for something" (Warner 2006). This construct encompasses a variety of factors, including management values, management and organizational practices, communication, and employee involvement (Neal et al. 2000). Security climate is a specific form of organizational climate that focuses on employees' perceived value of safety in their work environment. Drawing from workplace safety literature, Chan et al. (2005) introduced climate to the area of information security because the authors regarded information security as a form of organizational safety for several reasons: both safety and information security are crucial to business success, but they do not directly generate business value. Furthermore, effectiveness of safety or information security programs is achieved if incidents do not occur or are at least are reduced. Last, following safety and security guidelines is often seen by employees to be in direct conflict with work efficiency and productivity. In the context of this study, we define information security climate as employees' perceptions of management and organizational approaches to information security, which helps employees to make sense of the priority accorded to information security within the organization. We propose the following hypothesis:

> **H3:** *Transformational leadership experienced by employees has a significant positive influence on employees' perception of the information security climate.*

Griffin and Neal (2000) provided evidence that the influence of employees' perception of safety climate on their performance outcomes is mediated through employees' motivation. Employees are motivated to perform safely at work if they perceive a climate that supports safety in the workplace. Furthermore, a positive safety climate also implies that the supervisor is concerned about workplace safety and generates an implicit obligation for his or her followers to carry out safety activities. Drawing from expectancy-valence theory (Vroom 1964), it is assumed that employees who work in an environment with a positive safety climate are more motivated to perform safety activities since they believe that these behaviors will lead to valued outcomes (Neal and Griffin 2006). Adopting this assumption into the area of information security, we propose the following hypothesis:

> **H4:** *Employees' perception of organizational security climate has a significant positive influence on employees' security motivation.*

With regard to the theories of work performance, employees' perception of organizational climate is an antecedent of employees' behavior (Neal and Griffin 2006). In organizational safety research, various studies examined the relationship between employees' perceived security climate and employees' intention to comply with safety guidelines. Researchers were able to provide evidence for a positive relationship between perceptions of safety climate with self-reported safety behaviors (e.g., Griffin and Neal 2000; Probst and Brubaker 2001). It is argued that safety climate is reflected in the behavior and attitudes of individuals and thus reduces accidents in the workplace. Moreover, safety climate promotes safety participation through employees' perception of management's safety values (Clarke and Ward 2006). Transferred to the field of information security, this means that a high perception of management's commitment to information security causes employees to comply with organizational information security policies (Chan et al. 2005). Moreover, employees also voluntarily contribute to an environment that supports information security:

> **H5$_a$:** *Employees' perception of organizational security climate has significant positive influence on employees' intention to comply with security policies.*

> **H5$_b$:** *Employees' perception of organizational security climate has a significant positive influence on employees' intentions to participate in security activities.*

Vroom's (1964) expectancy valence theory posits that employees' performance is determined by his or her motivation to perform a certain behavior. Employees' willingness to perform a certain behavior depends on the perceived desirability (valence) of the expected outcomes. Accordingly, if employees' are rewarded for complying with organizational policies, the motivational force to perform those behaviors perceived by the employees is assumed to be high (Probst and Brubaker 2001). Herath and Rao (2009a) demonstrated the importance of intrinsic motivation in the context of employees' intention to comply with information security policy. Son (2011) showed that intrinsic motivation is a strong determinant of employees' information security policy compliance intention. Since employees' motivation to perform a certain behavior influences both, employees' task and contextual performance (Griffin 2000), we propose the following hypotheses:

> **H6$_a$:** *Employees' security motivation has a significant positive influence on employees' intention to comply with security policies.*
>
> **H6$_b$:** *Employees' security motivation has a significant positive influence on employees' intentions to participate in security activities.*

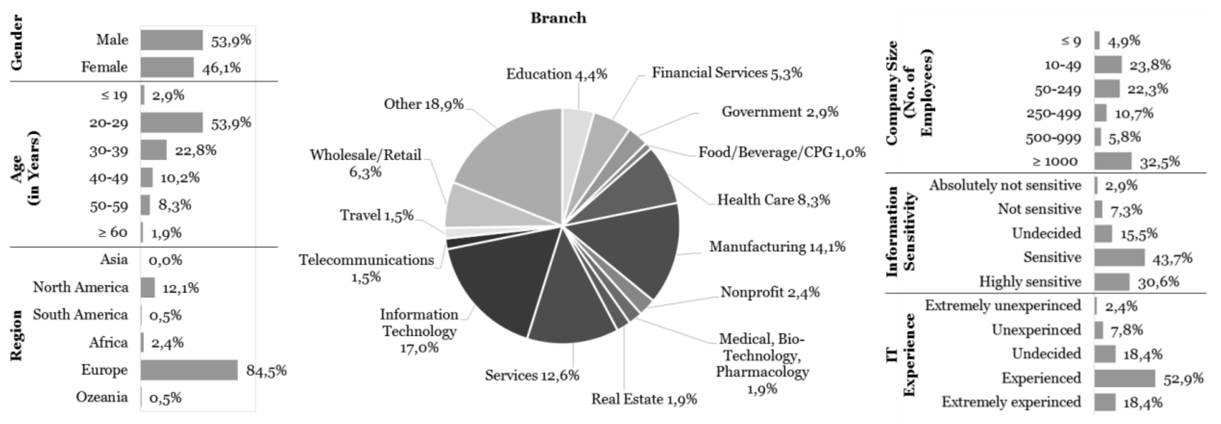
Research Design and Methodology

Explorative Data Collection Procedures

Acknowledging the challenges associated with gaining acceptable empirical data within the critical domain of transformational leadership in the context of employees' information security performance, we chose the survey methodology to collect empirical data and multivariate analysis methods to test the revised model statistically. To increase content validity and to assess the conciseness and clarity of the survey questions and instructions, and to evaluate the measurement models, the questionnaire was pre-tested. The initial set of items was reviewed by 12 information systems faculty members and doctoral students and has been modified slightly as a result of the feedback. Next, people of different age groups, as well as undergraduate and graduate students, were interviewed and asked for their feedback. Comments and opinions on the survey questions were collected and used to revise the final questionnaire and to modify several items, especially wording. Furthermore, as described by Johnston and Warkentin (2010), content validity for the instrument scales was established through a content validity expert panel comprised of 12 information systems faculty members and doctoral students, as mentioned above.

For the final study we used a simple random sample in order to provide unbiased random selection of employees. For this purpose, e-mail addresses and contact data were collected from international company websites and social media profiles (e.g., Xing, LinkedIn, Facebook) over a span of six months. Potential participants were contacted and an online survey was distributed. Additionally, a link to the online survey was posted in relevant groups within social media and online forums. The first question of the online survey eliminated participants who were unemployed. These restriction concerning the target group allowed the authors to accurately measure the proposed hypotheses. Participation was voluntary, but was motivated by sharing the results. Due to the critical information being shared in the survey, participants were assured that their responses would be treated with anonymity and confidentiality, because the survey was hosted using a university-based survey tool in a secure environment. In the final study a total of 440 employees participated, with 208 producing usable data for statistical analysis that demonstrates a response rate of 47.27 %. The response rate is acceptable given the nature of the study. A summary of the demographic characteristics of respondents is provided in Figure 1.

Figure 1. Demographic Profile of the Sample



In the first part of the survey, employees were asked to respond to the leadership items according to their subjective perception of their respective supervisors. In this context, the four dimensions of transformational leadership, namely idealized influence, individualized consideration, inspirational motivation, and intellectual stimulation were measured using a five-point rating scale ranging from "not at all" to "frequently, if not always". In the second part, employees were asked to indicate how strongly they agreed or disagreed with a number of statements relating to their perception of organizational security climate as well as their security motivation, security compliance intention, and security participation intention. These constructs were measured with multiple items using a five-point Likert scale, which ranged from "strongly disagree" to "strongly agree."

Operationalization of Variables and Measurement

All measurement items were adapted from prior studies, although some terms were changed to fit the specific research context (see Appendix, Table A1). To measure transformational leadership as perceived by the participants, Multifactor Leadership Questionnaire (MLQ) form 5X-Short was utilized. The MLQ is a well-established instrument and has been used in a broad range of sample population and variety of setting, e.g. marketing, organizations in different countries, industry, and military (Antonakis et al. 2003; Avolio and Bass 2004; Erkutlu 2008; Sadeghi and Lope Pihie 2012).Transformational leadership was conceptualized as being a function of idealized influence, individualized consideration, inspirational motivation, and intellectual stimulation. These sub-dimensions, which are viewed as defining characteristics of the focal construct, are measured using 16 items (MacKenzie et al. 2011). The constructs of security motivation, security climate, security participation intention, and security compliance intention were multi-item scales drawn from previous validated measures. The construct security motivation was measured using five items partly adapted from Neal and Griffin (2006), and Griffin and Neal (2000), while security climate was measured using five items based on research by Neal and Griffin (2006), and Chan et al. (2005). Furthermore, we adapted the five items measuring security participation intention from Neal and Griffin (2006) and Clarke et al. (2006) and the six items measuring security compliance intention from Bulgurcu et al. (2010), Herath and Rao (2009b) and Warkentin et al. (2011).

In the course of operationalization of the measurement model, which analyzes the relationship between the latent construct and their associated indicators, it is important to distinguish between reflective and formative measurement models, because constructs in SEMs, which are the basic element of a theory, are not inherently reflective or formative, which clearly differ with regard to their basic premises (MacKenzie et al. 2011). After examining the relationship between each indicator and the construct in the research model, we determined the overall security constructs to be reflective, because of the direction of the causality, the interchangeability of the indicators, the covariation among the indicators, and the nomological net of the constructs, which should not differ (Petter et al. 2007). Transformational leadership is modeled as a second-order latent construct with first-order subdimensions as formative indicators, namely: (1) Idealized Influence, which is divided into Idealized Influence (Behavior), and Idealized Influence (Attributed), (2) Individualized Consideration, (3) Inspirational Motivation, and (4) Intellectual Stimulation. Transformational leadership is conceptualized as having multiple behavioral sub-dimensions that together define what it means to be a transformational leader and determine a leader's level of transformational leadership (MacKenzie et al. 2011). Thus, even though this construct has consistently been modeled in the literature as having reflective indicators, transformational leadership construct should be modeled second-order formative construct (MacKenzie et al. 2005).

Data Analysis and Results

Empirical data was analyzed via partial least squares structural equation modeling (PLS-SEM). In general, SEM provides the flexibility to model a relationship among criterion variables and multiple predictors, such as model errors in measurements for observed variables, to design unobservable latent variables, and to statistically test a priori theoretical and measurement assumptions against empirical data (Chin 1998). As this research is an exploratory study in a new stream, it probes an area which is not well understood. Measurement validation and model testing were conducted using a two-step approach with SmartPLS version 2.0.M3. PLS-SEM does not impose a normality requirement on the data and it is advantageous when the research model has a variety of indicators, is relatively complex, and the measures are not well established (Sun 2012; Wetzels et al. 2009; Hair et al. 2011).

Initially, we examined the composite reliability, the item reliability and the convergent and discriminant validity. To ensure item reliability, we examined the loadings of each item to their respective underlying construct. Acceptable item loadings are recommended to be above at least 0.6 and ideally above the threshold of 0.707, indicating that at least 50 percent of the variance is shared with the respective construct (Chin 1998). We assessed item reliability and found that the loadings for all items exceeded 0.6 (0.625 to 0.945). The t-values ranged from 8.159 to 85.704, which shows significance for all item loadings at p<0.001. The composite reliability (also known as internal consistency reliability-ICR) is similar to Cronbach's alpha and measures its internal consistence, except that the latter presumes, a priori, that each indicator of a construct contributes equally (i.e,. the loadings are set to unity) (Chin 1998; Fornell and Larcker 1981). Fornell and Lacker (1981) argued that their measure is superior to Cronbach's alpha because it uses the actual item loadings obtained within the nomological network to calculate internal consistency reliability. ICR should be 0.70 or higher (Diamantopoulos et al. 2008). The value is above the threshold (ICR: 0.8559 – 0.9542). Convergent and discriminant validity was assessed by the average variance extracted (AVE). Discriminant validity is the degree to which measures of different constructs are distinct (Campbell and Fiske 1959). AVE represents the overall amount of variance in the indicators that was accounted for the latent construct. The reported values provide evidence of discriminant and convergent validity, since the AVE is well above the recommended level of 0.50 (Bhattacherjee and Premkumar 2004). The AVE values for all constructs in this model are higher than the recommended threshold value of 0.50 (AVE: 0.5676 – 0.8035), suggesting the convergent validity of the scale (Bhattacherjee and Premkumar 2004). The Fornell and Larcker criterion is met (Fornell and Larcker 1981). Another way to evaluate discriminant validity is to examine each indicator's factor loadings (Chin 1998). Indicators should load higher on the construct of interest than on any other variable. This condition is also met (see Table A6). The Kaiser-Meyer-Olkin (KMO) criterion should be at least 0.5 (Chin 1998; Fishbein and Ajzen 1975). Here the KMO criterion is higher than the recommended threshold for the whole reflective measurement models. Overall, the evidence of reliability, convergent validity, and discriminant validity indicates that the measurement model was appropriate for testing the structural model at a subsequent stage. The validity and reliability criteria are presented in Table A5.

Since formative indicators may move in different directions and can theoretically co-vary with other constructs, procedures for determining the validity of reflective measures do not apply to formative indicators (Lowry and Gaskin 2014; Petter et al. 2007). At the indicator level, it is obligatory to test for multicollinearity, which illustrates whether and to what degree the items are mutually linearly dependent. But in particular, the concept of reliability has no significant meaning when formative models are employed. Thus, the importance of reliability decreases, while the significance of assessing validity increases (Diamantopoulos 2011). The variance inflation factor (VIF) is equal to one and should not be greater than ten, as this might indicate the presence of harmful multicollinearity. To test for multicollinearity, we first created the latent variable scores in SmartPLS and tested for VIF in SPSS. The VIF values ranged from 2.491 to 4.138. Therefore all of the VIFs of the indicators were below 10, indicating sufficient construct validity for our formative constructs. Another important aspect is testing communality as validity criteria. The values for all constructs in this model are lower than the recommended threshold value of 0.9 (0.5987 – 0.7446). Thus, it can be said that the quality criteria of the formative constructs are met on all levels. With an adequate measurement model and an acceptable level of multicollinearity, the hypotheses proposed in this study were tested. The results of the analysis of the structural model are depicted via path coefficients and t-values in Figure 2. To receive valid results, a test of significance of all paths in the structural model was performed using the bootstrapping resampling procedure with a resampling of 500. With this procedure, the analysis produced estimates of both the explained variance and path coefficients. As shown by the PLS results of the analysis of the structural model, of the nine hypotheses ($H1_a$ – $H6_b$), all but three were found to be significant (see Figure 2).

We also tested for mediation effect of security motivation and security climate in the relationship between transformational leadership and security compliance intention, as well as security participation intention. The recommendations for testing the mediation effect can be categorized into different approaches (Mackinnon et al. 2002; Wood et al. 2008; Malhotra et al. 2014). As mentioned by Baron and Kenny (1986) the evidence for mediation is strongest when there is no direct effect, but rather an indirect effect. Baron and Kenny (1986) call this "full mediation." When there are both direct and indirect effects there is a "partial mediation" (Lowry and Gaskin 2014). The assessment of the significance of the reduction of the relationship between the independent and dependent variables cannot be assessed by a visual inspection of the path coefficients. Using the Sobel z-test, which is a traditional method of testing the significance of mediation effects, you can test whether a mediator variable carries the influence of an independent variable to a dependent variable (Soper 1982). However, since the Sobel test assumed normal distribution, we use bootstrapping, which is a nonparametric resampling procedure and a method that does not impose the assumption of normality of the sampling distribution (Preacher and Hayes 2010). Furthermore, the bootstrap method seems to be more appropriate for PLS-SEM than Sobel's (1982) large sample test to obtain the standard error for the indirect effect (Shrout and Bolger 2002; Wetzels et al. 2009). Our results provide support for the full mediation role both security climate and security motivation between transformational leadership and security compliance intention with a significant indirect effect at the 0.01 level ($p < 0.01$). A partial mediation role for both security motivation and security climate between transformational leadership and security participation intention could also be confirmed ($p < 0.01$) see Table A3. These results validated our model by providing strong evidence that security motivation and security climate act as a full/partial mediator and that predicting only a direct relationship between transformational leadership and security compliance intention and security participation intention is theoretically incorrect. This is also true for the mediation effect of security climate in the relationship between transformational leadership and security compliance intention.

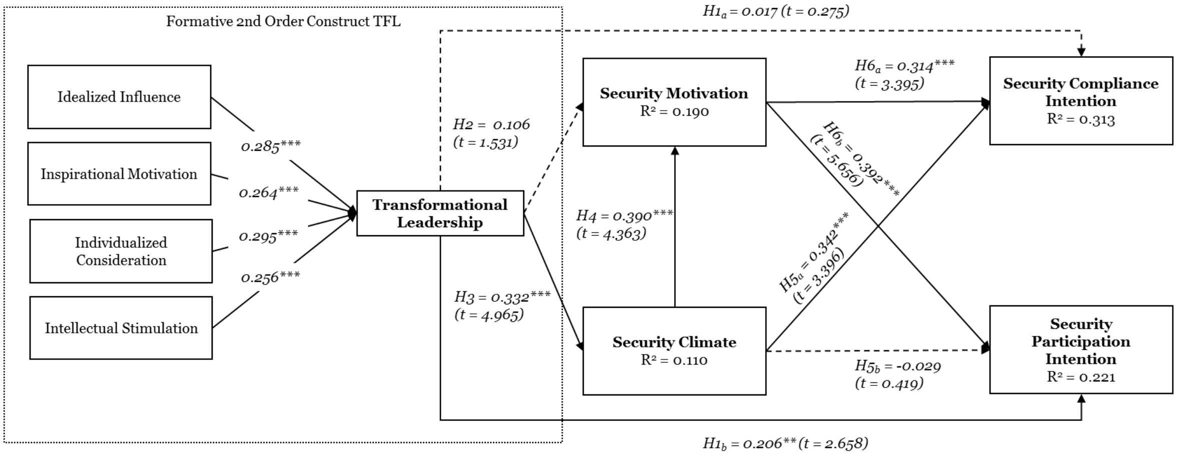
Effect size measures have been offered as indices of meaningfulness or practical significance (Olejnik and Algina 2000; Onwuegbuzie and Leech 2004). Effect sizes have the benefit that they are independent of the sample size and that the measurement of the effect size allows a direct comparison of different quantities measured, e.g., on different scales (Selya et al. 2012). In order to check for practical significance, the effect size as per Cohen (1988) is calculated. According to Cohen (1988), the difference in R^2 can assess the overall effect size f^2 at three different levels: 0.02-0.14 for small effects, 0.15-0.34 for medium effects, and above 0.35 for large effects. Besides the value or height of the path coefficients, the effect size f^2 is another measure of substantial effect of exogenous latent variables on the latent endogenous variable. f^2 provides information about the size of the effects, although it has to be noted that a low f^2 does not necessarily imply an insignificant effect (Chin et al. 2003). It can thus also be used to illustrate the practical relevance of statistical significant results. The effect sizes are shown in Table A4.

Furthermore, the potential for common method variance (CMV) should be addressed because the data was collected from a survey instrument (Chang et al. 2010; Liang et al. 2007; McElroy et al. 2007; Doty and Glick 1998; Podsakoff and Organ 1986) and in many empirical research papers CMV remains a critical methodological concern (Siemsen et al. 2010; Turel et al. 2011). We tried to minimize these methodological concerns ex ante in the research design stage and ex post in different ways: first, a number of procedural remedies were used when designing and administering the questionnaire to reduce the likelihood of CMV. The items for measuring the different constructs (independent and dependent variables) were mainly adapted from different previously validated studies (Chang et al. 2010, Degirmenci et al. 2013). Furthermore, counterbalancing the order of questions in relation to different constructs makes CMV less likely. This is due to the fact that the participant cannot easily combine related indicators to cognitively create the correlation needed to produce a CMV-biased pattern of responses (Murray et al. 2005; Uffen et al. 2012; Degirmenci et al. 2013). Therefore, we implemented the online survey questionnaire in such way as to prevent participants from backtracking to change their answers. To achieve this, the pages of the survey items were presented in a random manner to discourage participants from figuring out the relationship between the predictor and criterion variable that we were trying to establish. Second, the anonymity and confidentiality of the study were guaranteed (Chang et al. 2010). This would also mitigate self-serving answers and the probability that respondents provided answers they believe were expected (Uffen et al. 2012, Degirmenci et al. 2013). These remedies can ex ante reduce the likelihood of the consistency motive in participants' responses and theory-in-use biases (Chang et al. 2010; Podsackoff et al. 2003). Second, this study employed Harman's single-factor test (Podsackoff et al. 2003) to access the common method bias ex post. The results of the EFA shows that no single factor accounted for the covariance in the variables and no single factor emerged from the unrotated factor solution (Podsackoff et al. 2003).

Discussion and Implications for Research and Practice

The goal of the present study is to examine the relationship between generalized transformational leadership and employees' information security performance (i.e., security compliance and security participation intention). The results from structural model testing support the proposed model in great parts. Based on our empirical investigation, the major findings are discussed in the following.

Figure 2. Overview of the Findings


Formative 2nd Order Construct TFL
Idealized Influence
Inspirational Motivation
Individualized Consideration
Intellectual Stimulation
0.285***
0.264***
0.295***
0.256***
Transformational Leadership
H2 = 0.106 (t = 1.531)
H3 = 0.332*** (t = 4.965)
Security Motivation R² = 0.190
Security Climate R² = 0.110
H4 = 0.390*** (t = 4.363)
H1a = 0.017 (t = 0.275)
H6a = 0.314*** (t = 3.395)
H6b = 0.392*** (t = 5.656)
H5a = 0.342*** (t = 3.396)
H5b = -0.029 (t = 0.419)
Security Compliance Intention R² = 0.313
Security Participation Intention R² = 0.221
H1b = 0.206** (t = 2.658)

*p < 0.05, ** p < 0.01, *** p < 0.001
Note: Dashed lines represent unsupported paths.

As predicted, transformational leadership has a significant influence on employees' intention to participate in organizational information security ($H1_b$). This is consistent with the notion that transformational leaders are capable of motivating employees to perform beyond expectations on a contextual level (Avolio and Bass 2004). As we investigate generalized transformational leadership, this finding also suggests that transformational leaders must not necessarily possess a specific orientation towards information security in order to stimulate information security participation of employees. Generalized transformational leadership enables supervisors to achieve interpersonal and organizational goals. This also includes the motivation of employees to make extra effort in order to promote information security within the organization.

In contrast, the results of this study do not support the hypothesis that general transformational leadership also has a significant influence on employees' intention to comply with organizational information security policies ($H1_a$). Based on the assumption that transformational leadership results in high organizational commitment of employees, we expected that transformational leaders convey the value and importance information policy compliant behavior to their followers. Moreover, transformational leaders were supposed to stimulate employees to neglect their self-interest (i.e., avoidance of inconvenient security measures) in favor of the organizational group-interest. However, empirical evidence shows that the experience of generalized transformational leadership did not directly affect whether employees intend to comply with information security policies. This finding is consistent with a study from Innes et al. (2010) in the field of employees' safety behavior research. The authors presumed that "high levels of transformational leadership indirectly give employees greater latitude to use their discretion in deciding whether to comply with existing organizational policies." Extending this argument to include information security, we infer that employees' intention to comply with organizational information security policies is subject to variability, demanding further measures in order to achieve employees' policy compliance. Previous studies in the field of employees' information security behavior showed that sanctions like formal control measures are capable of inducing compliant behavior by employees (e.g., Herath and Rao 2009b; Siponen and Vance 2010; Hovav and D'Arcy 2012). The exertion of punishment and rewards is closely related to transactional leadership (Avolio and Bass 2004; Podsakoff et al. 2006). Since transformational leadership is an extension of transactional leadership, transformational leaders are also able to use contingent reward as a dimension of leadership style. However, the examination of full range leadership is necessary in order to explain employees' intention to meet (minimum) information security standards.

As hypothesized, empirical results revealed a significant positive influence of transformational leadership on employees' perception of information security climate ($H3$). This suggests that the conviction of transformational leaders regarding the value and importance of organizational information security policies, procedures, and practices directly translates into employees' individual evaluation of information security in their work environment. Chan et al. (2005) initially provided evidence of a relationship between direct leadership practices and security climate. We extend the findings of the latter study by introducing the concept of transformational leadership in the context of the subject matter in order to gain a better understanding of the influence of leadership practices.

Since the results of this study only partially confirmed a direct influence of transformational leadership on employees' information security performance, employees' perception of information security climate is of particular importance, as it positively influences employees' intention to comply with information security policies ($H5_a$). Accordingly, by forming a positive organizational climate towards information security, transformational leaders are capable of ensuring employees' adherence to information security procedures, rules, and regulations. However, a significant influence of employees' perception of information security climate on their intention to participate in organizational information security could not be confirmed by empirical evidence ($H5_b$). This finding contradicts studies from the field of employees' safety behavior that demonstrated an even stronger relationship between climate and employees' participation than between climate and employees' compliance (e.g., Neal and Griffin 2006; Clarke 2006). Clarke (2006) argues that positive safety climate "may represent an employer that is committed to safety and accident prevention, which is reciprocated by employees' willingness to engage in safety-related activities." This argument is valid, as accident prevention directly promotes employees' wellbeing in the workplace. However, this argument cannot be transferred to the context of information security as management commitment to information security does not primarily benefit employees' self-interests but organizational group-interest. This is in line with our finding that transformational leaders directly influence employees' information security participation intention as they are able to stimulate employees' willingness to make a stand for the group-interest.

The importance of employees' perception of information security climate is further underlined as results confirmed the direct influence on employees' information security motivation (*H4*). Through mediating effects, security motivation provides an individual process that links employees' perceived security climate to specific security performance outcomes. The results support the hypotheses that employees' security motivation mediates the impact of security climate on both dimensions of employees' information security performance, information security compliance ($H6_a$), and participation ($H6_b$) intention, which is consistent with Probst and Brubaker (2001). However, the authors focused on extrinsic motivation, such as rewards and punishments, whereas our study assessed intrinsic value that employees place on information security. Our findings thus question Neal and Griffin's (2006) assumption that "extrinsic motivators, such as rewards and punishment, may be more important determinants of changes in compliance than the intrinsic value that individuals place on safety." Current research in the field of employee information security behavior focused on extrinsic motivation by drawing from general deterrence theory, for example. Our findings, however, support the importance of intrinsic motivation in the context of information security behavior, since intrinsic motivation has not received much attention in literature despite its potential to explain employees' security-related behavior (Son 2011).

Our findings indicate that employees' security motivation influences employees' information security compliance intention to a lesser extent than employees' information security participation intention. This can be explained by Motowidlo Borman, and Schmit's (1997) argument, „that motivation is a stronger determinant of contextual performance than task performance, because contextual behaviors are more discretionary" (Neal and Griffin 2006). Neal and Griffin (2006) further provided empirical evidence for a reciprocal relationship between safety motivation and safety participation in the course of time. Accordingly, the participation in safety activities leads to a higher safety motivation, which is caused by positive reward and encouragement. The increased motivation in turn leads to participation in further activities. Extending this logic to the field of information security, this suggests that carrying out behaviors in favor of organizational information security has positive motivational consequences. Information security compliance is not supposed to entail motivational effects since receiving positive reward and encouragement is less likely for merely complying with (minimum) information security standards (Neal and Griffin 2006). To explore the described reciprocal effect in the context, long-term studies are necessary.

The hypothesis that transformational leadership directly influences employees' intrinsic motivation towards information security (*H2*) was not confirmed by empirical evidence. The absence of a positive relationship between transformational leadership and intrinsic motivation in the information security context contradicts studies on motivational effects of transformational leadership from other research fields (e.g., Masi and Cooke 2000; Charbonneau et al. 2001). As it is generally assumed within academic literature that the supportive character of transformational leadership increases followers' intrinsic motivation (Charbonneau et al. 2001), our findings provide an interesting aspect that requires further investigation. A considerable point in this context is the scale for measuring intrinsic motivation. For example, Herath and Rao (2009a) utilized employees' perceived effectiveness of their actions towards information security in order to measure intrinsic motivation. Son (2011) focused on employees' perception of value congruence and legitimacy of the information security policy as factors of intrinsic motivation. Drawing from safety behavior research (e.g., Neal and Griffin 2006), we measured intrinsic motivation by assessing the value that employees placed on information security. It may be appropriate to adopt scales from other research fields (e.g., Vallerand et al. 1992; Pelletier et al. 1995) in order to enhance the understanding of intrinsic motivation in the field of information security behavior.

Several practical implications arise in addition to the implications for research discussed above. Results of our study emphasize the role and importance of supervisors within the organizational information security chain. Accordingly, not only must information security training and awareness (SETA) programs address employees' knowledge and skills for coping with threats to information security, they must also enhance supervisors' awareness and abilities to promote and convey the value and necessity of information security among employees. Furthermore, with regard to the organizational strategy for protecting information assets, organizations have to promote transformational leadership in order to improve the security level. Previous studies stressed the meaning of security climate and intrinsic motivation for individual and organizational information security behavior. Transformational leadership provides a way for organizations to enhance both security climate and indirectly, motivation. Drawing from deterrence theory, external influences like punishment were seen to be an applicable measure to prevent employees' non-compliance to information security policies. By stimulating employees' intrinsic motivation, transformational leadership enables organizations to reduce controlling leadership measures (i.e., punishment). This is also necessary due the overjustification effect. This effect occurs when the addition of extrinsic reinforcement decreases employees' intrinsic motivation to perform a certain behavior as they perceive the behavior as overjustified (Griggs 2010).

Limitations

This study is subject to several limitations, some of which offer opportunities for future research. First of all, the aim of this study is to investigate the effects of leadership on security climate and security motivation and thus on employees' information security performance. Since literature showed that transformational leaders very well suited to enhance followers' perceived climate, motivation and performance, we focused on transformational leadership effects in this initial study in order to provide a basis for further research. The comparison of the effects of transformational leadership versus transactional leadership would be interesting and are part of an ongoing research process. Another key limitations of the current study is that employees' behavioral intentions is assessed rather than their actual behavior. However, due to the difficulties in observing employees' security behavior in a practical setting (Vroom and von Solms 2004), it is common in the field of security behavior research to measure behavioral intentions as proximal cognitive antecedents of actions or behavior (Lebek et al. 2013). Second, the fact that all data was collected using a single survey at a single point in time raises the possibility that our results are prone to common-method variance (CMV). Since respondents are a source of the exogenous variable and the endogenous variable at the same time, any defect in that source will contaminate both measures in the same fashion and in the same direction (Podsakoff and Organ 1986). In order to mitigate the likelihood of CMV occurrence, we applied several ex ante and ex post measures, as described in the methodology section. Moreover, there are limitations regarding the use of generic measures for information security compliance. Siponen and Vance (2014) advocate the use of specific measures in order to reduce bias "respondents need to use their memory and imagination" in order to answer generic questions. However, there are two reasons for choosing generic measures for this study: first, as the survey was not limited to any company, branch, or country, it was not possible to investigate a specific yet common and relevant issue. Second, we adopted the items from renowned and frequently cited sources in order to provide validity. A further limitation occurs with regard to the assumption that leaders influence employees' attitudes. However, it is possible that followers' attitudes influenced their ratings of their supervisors. In order to address this concern, there is a need to conduct longitudinal or experimental research where leadership ratings are collected prior to attitude measures. To assess transformational leadership, we used the standardized and validated Multifactor Leadership Questionnaire (MLQ), which represents a generally accepted measurement scale in behavioral research. Several further measurements exist, but most of them agree on core facets of transformational leadership. However, we cannot exclude that other measures would lead to different results. Moreover, we use a limited set of variables to predict performance. Additional variables such as self-efficacy may impact employees' security performance. Furthermore, cultural factors may limit the general applicability of our conclusions. The results of the study may include regional biases due to the data collection, which took place mainly in Europe and North America. Thus, the results have to be carefully interpreted with regard to other cultures.

Conclusion and Outlook

This study contributes to the field of employee information security behavior, as it aims to explain the relationship between leadership and employees' information security performance. Recent studies mentioned leadership in the context of information security; however, the role of managers and supervisors in the information security chain has received little attention in academic research. To address this gap, we introduced the concept of transformational leadership to the research field of employee information security behavior. Overall, this study contains potentially important implications for the role of transformational leadership in enhancing employees' information security performance. Results show that transformational leadership is strongly related to employees' information security participation. Moreover, it could be proven that employees' perception of security climate and employees' intrinsic motivation mediate the influence of transformational leaders on employees' security performance. Consequently, transformational leaders possess the ability to (indirectly) enhance employees' motivation and thereby complement or even supersede external influences like punishment. However, it must be taken into consideration that it is likely that confounding variables exist which affect the influence of transformational leadership on employees' information security performance. It is argued that national-, organizational- and group culture are critical variables for managerial processes that directly or indirectly influence IT (Leidner and Kayworth 2006). It can be assumed that different beliefs, basic assumptions or shared values within different cultural settings have a diverse impact on the effects of transformational leadership on employees' information security behavior. Future research could extend this study across different cultural settings, i.e., by investigating the degree of transformational leadership within different branches. In this context, the inclusion of other antecedents that influence climate and motivation for security might be useful. This includes, for example, the risk level of a particular organization or branch (i.e., severity and certainty of threats) or organizational characteristics such as size. Moreover, experimental and longitudinal studies are required to ascertain the causal nature of the proposed model and to investigate the influence of employees' attitudes on their ratings of leadership. Additionally, experimental studies allow the authors to control for associated confounding variables (i.e., cultural differences). Furthermore, this study focuses on transformational leadership. It would be interesting for future research to examine whether the full range of leadership, including transactional leadership, exerts different effects on employees' information security performance. Although we stated in the introduction why the effects transformational leadership in the context of information security may differ from other contexts, future research is needed for further investigation of those differences.

Appendix

Table A1. Survey Instrument – Questionnaire for the Security Constructs

Construct	Adopted Item	Source
Security Climate 1-5	Information security is given a high priority by management	Neal and Griffin (2006)
	The organization sets high standards for the protection of its information assets	Chan et al. (2005)
	Management is concerned with information security of the organization	Chan et al. (2005)
	My supervisor is concerned with information security of the organization	Chan et al. (2005)
	My coworkers are concerned with information security of the organization	Chan et al. (2005)

Table A1. Survey Instrument – Questionnaire for the Security Constructs (continued)

Security Motivation 1-4	I feel that it is important to maintain information security at all times	Neal and Griffin (2006)
	I believe that it is important to reduce the risks to information security in the workplace	Neal and Griffin (2006)
	I believe that information security at the workplace is an important issue	Neal and Griffin (2006)
	It is important to consistently use the correct security tools (e.g. Anti Virus Software, Data Encryption, Safe Passwords, etc.)	Griffin and Neal (2000)
Security Participation Intention 1-5	I promote the information security within the organization	Neal and Griffin (2006)
	I put in extra effort to improve information security at the workplace	Neal and Griffin (2006)
	I voluntarily carry out tasks or activities that help to improve information security	Neal and Griffin (2006)
	I am involved in discussing the effectiveness information security measures	Clarke et al. (2006)
	I don't think it is my responsibility to be involved in information security initiatives	Clarke et al. (2006)
Security Compliance Intention 1-6	I intend to comply with the requirements of the information security policy of my organization in the future	Bulgurcu et al. (2010)
	I intend to protect information and technology resources according to the requirements of the information security policy of my organization in the future	Bulgurcu et al. (2010)
	I intend to carry out my responsibilities prescribed in the information security policy of my organization when I use information and technology in the future	Bulgurcu et al. (2010)
	I am likely to follow organizational security policies	Herath and Rao (2009b)
Please note:	The items for assessing Transformational Leadership were adapted from the Multifactor LeadershipQuestionnaire (MLQ) Form 5X Short with permission of the publisher, MIND GARDEN, Inc., Redwood City, CA 94061 (www.mindgarden.com). Copyright © 1995, 2000, 2004 by Bernard Bass and Bruce Avolio. All rights reserved. Further reproduction is prohibited without the publisher's written consent	

Table A2. Latent Variable Correlations*

	IC	II	IM	IS	SCI	SPI	SC	SM
IC	1	0.6458	0.4363	0.6615	0.0430	0.0433	0.1174	0.0192
II	0.8036	1	0.5938	0.6979	0.0410	0.0924	0.0729	0.0515
IM	0.6605	0.7706	1	0.5148	0.0125	0.0681	0.0404	0.0595
IS	0.8133	0.8354	0.7175	1	0.0438	0.0759	0.1463	0.0578
SCI	0.2074	0.2026	0.1112	0.2092	1	0.0448	0.2312	0.2149
SPI	0.2082	0.3039	0.2609	0.2756	0.2118	1	0.0425	0.1834
SC	0.3426	0.2700	0.2009	0.3825	0.4808	0.2061	1	0.1804
SM	0.1386	0.2270	0.2439	0.2405	0.4636	0.4283	0.4247	1

* The squared factor correlations are shown above the main diagonal.
IC = Individualized Consideration; II = Idealized Influence; IM = Inspirational Motivation; IS = Intellectual Stimulation; SCI = Security Compliance Intention; SPI = Security Participation Intention; SC = Security Climate; SM = Security Motivation; TFL = Transformational Leadership

Table A3. Mediation Effects of Security Climate and Security Motivation

IV	M	DV	IV -> DV	IV -> M	IV -> DV	M -> DV	Results
TFL	SC	SCI	0.204*	0.332**	0.050	0.464**	Full
TFL	SM	SCI	0.204*	0.235**	0.101	0.440**	Full
TFL	SM	SPI	0.289**	0.235**	0.199**	0.381**	Partial
TFL	SC	SPI	0.289**	0.332**	0.248**	0.124	

Notes: * $p < 0.05$, ** $p < 0.01$

Table A4. Effect Size

Latent variable being explained (endogenous)	Explanatory latent variable (exogenous)	$R^2_{incl.}$ [a]	$R^2_{excl.}$ [b]	f^2
Security Motivation	Transformational Leadership	0.190	0.180	0.0124
	Security Climate	0.190	0.055	0.1667
Security Participation Intention	Transformational Leadership	0.221	0.184	0.0453
	Security Motivation	0.221	0.097	0.1592
	Security Climate	0.221	0.221	0.000
Security Compliance Intention	Transformational Leadership	0.313	0.313	0.000
	Security Motivation	0.313	0.233	0.1165
	Security Climate	0.313	0.224	0.1295

[a] → R^2 of the latent variable being explained (endogenous), together with the explanatory latent variable (exogenous).
[b] → R^2 of the latent variable being explained (endogenous), in the absence of the explanatory latent variable (exogenous).
Note: Cohen's f^2-statistics = $[R^2_{incl.} – R^2_{excl.}] / [1- R^2_{incl.}]$ (1988). $f^2 \geq 0.02$, 0.15, and 0.35 are termed small, medium, and large effect sizes. The rationale for these benchmarks (f^2) can be found in Cohen (1988) on the following pages: pp. 413-414.

Table A5. Validity and Reliability Criteria

Construct	Indicators	Std. Loading	t-value	Average Variance Extracted (AVE) AVE(ξi) ≥ 0.5	Composite Reliability (ICR) (ρ ≥ 0.7)
TFL	Ideal_Influen_Attri_1 Ideal_Influen_Attri_3 Ideal_Influen_Attri_4 Ideal_Influen_Behav_2 Indiv_Consider_1 Indiv_Consider_2 Indiv_Consider_3 Indiv_Consider_4 Intellect_Stimul_1 Intellect_Stimul_2 Intellect_Stimul_3 Intellect_Stimul_4 Inspir_Motiv_1 Inspir_Motiv_2 Inspir_Motiv_3 Inspir_Motiv_4	0.723 – 0.899	17.061 – 70.526	0.5676 (0.6987-0.7446)	0.9542 (0.8559-0.9208)
Sec_Climate	Sec_Climate_1 - 5	0.641 - 0.834	9.836 – 37.703	0.5874	0.8759
Sec_Com_Inten	Sec_Com_Inten 1 - 4	0.768 – 0.945	10.699 – 85.971	0.8035	0.9420
Sec_Part_Inten	Sec_Part_Inten 1 - 5	0.625 – 0.869	15.304 – 38.284	0.6206	0.8897
Sec_Motivation	Sec_Motivation 1,2,4,5	0.801– 0.904	14.404 – 59.280	0.7082	0.9064

Table A6. Factor Loadings and Cross-Loadings for the Final Indicators

	IIA	IC	IM	IS	SC	SCI	SM	SPI
II1	0.8635	0.7072	0.6524	0.6983	0.2391	0.1853	0.2271	0.2882
II2	0.8437	0.7225	0.5661	0.6986	0.2660	0.2232	0.2269	0.2813
II3	0.8728	0.6523	0.6838	0.6879	0.1481	0.1979	0.1717	0.1981
II4	0.7586	0.6007	0.6742	0.7088	0.2512	0.0657	0.1298	0.2479
IC1	0.7275	0.8992	0.5188	0.7274	0.3695	0.2010	0.1908	0.1437
IC2	0.5988	0.7885	0.5233	0.5902	0.1718	0.1659	0.0525	0.2022
IC3	0.6822	0.8773	0.6722	0.7289	0.3285	0.1785	0.1576	0.1222
IC4	0.7564	0.8822	0.5612	0.7492	0.2975	0.1703	0.0698	0.2543
IM1	0.6328	0.5201	0.8564	0.5506	0.1218	0.0358	0.1544	0.1602
IM2	0.5199	0.4376	0.8005	0.5227	0.2420	0.0981	0.3110	0.1683
IM3	0.7572	0.6380	0.8750	0.6914	0.0992	0.0946	0.1090	0.2791
IM4	0.6752	0.6174	0.8550	0.6468	0.2322	0.1448	0.2742	0.2603
IS1	0.5300	0.5494	0.4887	0.7231	0.3666	0.2592	0.2936	0.2440
IS2	0.6149	0.5408	0.5182	0.7176	0.2969	0.1017	0.1224	0.1904
IS3	0.6898	0.7303	0.5537	0.8248	0.2860	0.2045	0.1673	0.2393
IS4	0.7332	0.6775	0.6488	0.8228	0.2527	0.0945	0.1739	0.1854
SC1	0.2462	0.3071	0.1059	0.3506	0.8338	0.5162	0.3665	0.1394
SC2	0.1799	0.2104	0.0688	0.2643	0.7877	0.4362	0.2902	0.1492
SC3	0.1457	0.2821	0.1693	0.3128	0.8249	0.2905	0.2779	0.1070
SC4	0.2710	0.3126	0.3110	0.3308	0.7278	0.2384	0.3501	0.2352
SC5	0.1715	0.1874	0.1282	0.1881	0.6411	0.3094	0.3287	0.1570
SCI1	0.2188	0.2596	0.1270	0.2579	0.4657	0.9311	0.4881	0.2108
SCI2	0.1870	0.1684	0.1070	0.1953	0.4638	0.9452	0.4520	0.1639
SCI3	0.2005	0.1807	0.0672	0.1807	0.4584	0.9296	0.4263	0.2249
SCI4	0.0907	0.1090	0.1000	0.0770	0.3037	0.7678	0.2419	0.1540
SM1	0.2214	0.1638	0.2220	0.2302	0.3941	0.4239	0.9044	0.4108
SM2	0.1902	0.1369	0.2092	0.1946	0.3712	0.3562	0.8095	0.3020
SM4	0.1139	0.0046	0.1453	0.1599	0.3644	0.3216	0.8011	0.4282
SM5	0.2367	0.1577	0.2448	0.2226	0.2975	0.4565	0.8472	0.2923
SPI1	0.2858	0.2159	0.1778	0.2767	0.3274	0.3379	0.4029	0.8110
SPI2	0.2232	0.1156	0.2051	0.2238	0.1434	0.1468	0.4057	0.8645
SPI3	0.2349	0.1440	0.2384	0.2259	0.1019	0.1788	0.3305	0.8692
SPI4	0.2631	0.2080	0.2846	0.2089	0.1559	0.0921	0.3045	0.7425
SPI5	0.1759	0.1359	0.0986	0.1103	0.0035	-0.0120	0.1814	0.6254

References

Ajzen, I. 1985. "From intentions to actions: A theory of planned behavior," in *Action-control: From cognition to behavior*, J. Kuhl and J. Beckman (eds.), Heidelberg: Springer-Verlag, pp. 11-39.

Ajzen, I. 1991. "The theory of planned behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Antonakis, J., Avolio, B. J., and Sivasubramaniam, N. 2003. "Context and leadership: an examination of the nine-factor fullrange leadership theory using the Multifactor Leadership Questionnaire," *The Leadership Quarterly* (13), pp. 261-295.

Aurigemma, S., and Panko, R. 2012. "A Composite Framework for Behavioral Compliance with Information Security Policies," in *Proceedings of the 45th Hawaii International Conference on System Sciences*, Maui, HI, pp. 3248- 3257.

Avolio B. J., Bass B. M., and Jung D. I. 1999. "Re-examining the components of transformational and transactional leadership using the Multifactor Leadership Questionnaire," *Journal of Occupational and Organizational Psychology* (72:4), pp. 441-462.

Avolio B. J., and Bass B. M. 2004. *Multifactor Leadership Questionnaire: Manual and Sample Set.* California: Mindgarden.

Baron, R. M., and Kenny, D. A. 1986. "The moderator mediator variable distrinction in social-psychological-research – conceptual, strategic, and statistical considerations," *Journal of Personality and Social Psychology* (51:6), pp. 1173-1182.

Bass, B. 1985. *Leadership and Performance beyond Expectations*, New York, USA: The Free Press.

Bass, B. M., Waldman, D. A., Avolio B. J., and Bebb M. 1987. "Transformational Leadership and the Falling Dominoes Effect," *Group & Organization Management* (73:12), pp. 73-87.

Bhattacherjee, A., and Premkumar, G. 2004. "Understanding Changes in Belief and Attitude Toward Information Technology Usage: A Theoretical Model and Longitudinal Test," *MIS Quarterly* (28:2), pp. 229-254.

Bono J. E., and Judge T. A. 2004. "Personality and Transformational and Transactional Leadership: A Meta-Analysis," *Journal of Applied Psychology* (89:5), pp. 901–910.

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

Broadbent M., and Kitzis E. S. 2004. *The New CIO Leader: Setting the Agenda and Delivering Results*, Boston, USA: Harvard Business Press.

Brown, L. V. 2007. *Psychology of motivation*. New York: Nova Science Publishers.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I, 2009. "Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance," in *Proceedings of the 15th Americas Conference on Information System,* San Francisco, CA, Paper 419.

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.

Burns, J. M. 1978. *Leadership*. New York: Harper & Row.

Campbell, D. T., and Fiske, D. 1959. "Convergent and discriminant validation by the multitrait-multimethod matrix," *Psychological Bulletin* (56), pp. 81-105.

Chang, S.-J., van Witteloostuijn, A., and Eden, L. 2010. "From the Editors: Common method variance in international business research," *Journal of International Business Studies* (41:2), pp. 178-184.

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 & Security* (1:3), pp. 18-41.

Charbonneau, D., Barlign, J., and Kelloway, E. K. 2001. "Transformational Leadership and Sports Performance: The Mediating Role of Intrinsic Motivation," *Journal of Applied Social Psychology* (31:7), pp. 1521-1554.

Chin, W. W. 1998. "Issues and opinion on structural equation modeling," *MIS Quarterly* (29:3), pp. vii-xvi.

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

Cho, J., and Park, I. 2007. "Transformational Leadership and Information System Effectiveness," in *Proceedings of the 28th International Conference on Information Systems*, Montreal, Canada, Paper 85.

Clarke, S., and Ward, K. 2006. "The role of leader influence tactics and safety climate in engaging employees' safety participation," *Risk Analysis* (26:5), pp. 1175-1185.

Collins J., 2001. *Good To Great: Why Some Companies Make the Leap…and Others Don't*, New York: HarperCollins.

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.

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643-658.

Deci, E. L., and Ryan, R. M. 1985. *Intrinsic motivation and self-determination in human behavior*. New York, NY: Plenum.

Degirmenci, K., Guhr, N., and Breitner, M. H. 2013. "Mobile Applications and Access to Personal Information: A Discussion of users' Privacy Concerns," in *Proceedings of the 34th International Conference on Information Systems*, Milano, Italy.

Den Hartog, D. N., Van Muijen, J. J., & Koopman, P. L. 1997. "Transactional versus transformational leadership: an analysis of the MLQ," *Journal of Occupational and Organizational Psychology* (70), pp. 19-34.

Diamantopolous, A. 2011. "Incorporating formative measures into covariance-based structural equation models," *MIS Quarterly* (35:2), pp. 335-358.

Diamantopolous, A., Riefler, P., and Roth, K. P. 2008. "Advancing formative measurement models," *Journal of Business Research* (61), pp. 1203-1218.

Dinev, T., and Hu, Q., 2007. "The Centrality of Awareness in the Formation of User Behavioral Intention towards Protective Information Technologies," J*ournal of the Association for Information Systems* (8:7), pp. 386-408.

Dinev, T., Goo, J., Hu, Q., and Nam, K. 2009. "User Behavior toward Protective Technologies - Cultural Differences between the United States and South Korea," *Information Systems Journal* (19:4), pp. 391-412.

Dojkovski, S., Lichtenstein, S., and Warren, M. J. 2007. "Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia," in *Proceedings of the 15th European Conference on Information Systems*, St. Gallen, Switzerland, Paper 120.

Doty, D. H., and Glick, W. H. 1998. "Common methods bias: Does common methods variance really bias results?," *Organizational Research Methods* (1), pp. 374-406.

Erkutlu, H. 2008. "The impact of transformational leadership on organizational and leadership effectiveness the Turkish case," *Journal of Management Development* (27:7), pp. 708-726.

Fishbein, M., and Ajzen, I. 1975. *Belief, attitude, intention, and behavior: An introduction to theory and research. Reading*, MA: Addison-Wesley.

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

Geijsel, F., Sleegers, P., Leithwood, K., and Jantzi, D. 2003. "Transformational leadership effects on teachers' commitment and effort toward school reform," *Journal of Educational Administration* (41:3), pp.228-256.

Griffin, M. A., and Neal, A. 2000. "Perceptions of safety at work: a framework for linking safety climate to safety performance, knowledge, and motivation," *Journal of occupational health psychology* (5:3), pp. 347-358.

Guo, K. H. 2013. "Security-Related Behavior in Using Information Systems in the Workplace: A Review and Synthesis," *Computers & Security* (32:1), pp. 242–251.

Hagen, J. M., Albrechtsen, E., and Hovden, J. 2008. "Implementation and effectiveness of organizational information security measures," *Information Management & Computer Security* (*16*:4), pp. 377-397.

Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. "PLS-SEM: Indeed a Silver Bullet," *Journal of Marketing Theory and Practice* (19:2), pp. 139-151.

Heikka, J. 2008. "A Constructive Approach to Information Systems Security Training: An Action Research Experience," in *Proceedings of the 14th Americas Conference on Information Systems*, Toronto, ON, Canada, Paper 319.

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 Organizations," *European Journal on Information Systems* (18:2), pp. 106-125

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

Howell, J. M., and Avolio, B. J. 1993. "Transformational Leadership, Transactional Leadership, Locus for Control, and Support for Information: Key Predictors of Consolidated-Business-Unit Performance," *Journal of Applied Psychology* (78:6), pp. 891-902.

Hu, Q., and Dinev, T. 2007. "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *Journal of the Association for Information Systems* (8:7), pp. 386-408.

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 Journal* (43:4), 2012.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security*, (31:1), pp. 83-95.

Inness, M., Turner, N., Barling, J., and Stride, C. B. 2010. "Transformational Leadership and Employee Safety Performance: A Within-Person, Between-Jobs Design," *Journal of Occupational Health Psychology* (15:3), pp. 279-290.

James, L. A., and James, L. R. 1989. "Integrating work environment perceptions: Explorations into the measurement of meaning," *Journal of Applied Psychology* (74:5), pp. 739-751.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Jung, D. I., and Sosik J. J. 2002. "Transformational Leadership in Work Groups: The Role of Empowerment, Cohesiveness, and Collective-Efficacy on Perceived Group Performance," *Small Group Research* (33:3), pp. 313-136.

Karjalainen, M., and Siponen, M. T. 2011. "Toward a New Meta-Theory for Designing Information Systems (IS) Security," *Journal of the Association for Information Systems*, (12:8), pp. 518-555.

Kelloway, E. K., Mullen, J., and Francis, L. 2006. "Divergent effects of transformational and passive leadership on employee safety," *Journal of Occupational Health Psychology* (11:1), pp. 7686.

Kirsch, L., and Boss, S. R. 2007. "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines," in *Proceedings of the 28th International Conference on Information Systems*, Montreal, QC, Canada, Paper 103.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., and Breitner, M. H. 2013. "Employees' Information Security Awareness and Behavior: A Literature Review," in *Proceedings of the 46th Hawaii International Conference on System Sciences*, Maui, HI, USA, pp. 2978-2987.

Leidner, D. E., and Kayworth, T. 2006. "A review of culture in information systems research: toward a theory of information technology culture conflict," *MIS Quarterly*, (30:2), pp. 357-399.

Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management," *MIS Quarterly* (31:1), pp.59-87.

Limayem, M., and Hirt, S. G. 2003. "Force of Habit and Information Systems Usage: Theory and Initial Validation," *Journal of Association for Information Systems* (4:1), pp. 65-97.

Lowry, P. B., and Gaskin, J. 2014. "Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose and How to Use it," *IEEE Transactions on Professional Communication* (57:2), pp. 123-146.

MacKenzie, S. B., Podsakoff, P. M., and Jarvis, C. B. 2005. "The Problem of Measurement Model Misspecification in Behavioral and Organizational Research and Some Recommended Solutions," *Journal of Applied Science* (90:4), pp. 710-730.

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

MacKinnon, D. P., Lockwood, C. M., Hoffmann, J. M., West, S. G., and Sheets, V. 2002. "A comparison of methods to test mediation and other intervening variables effects," *Psychological Methods* (7), pp. 83-104.

Malhotra, M. K., Singhal, C., Shang, G., and Ployhart, R. E. (2014). "A critical evaluation of alternative methods and paradigms for conducting mediation analysis in operations management research," *Journal of Operations Management* (32), pp. 127-137.

McElroy, J. C., Hendrickson, A. R., Townsend, A. M., and DeMarie, S. M. 2007. "Dispositional factors in internet use: Personality versus cognitive styles," *MIS Quarterly* (31:4), pp. 809-820.

Mishra, S., and Dhillon, G. 2005. "Information Systems Security Governance Research: A Behavioral Perspective," in *Proceedings of the Symposium on Information Assurance*, Academic Track of 9th Annual NYS Cyber Security *Conference*, pp.18-26.

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.

Neal, A., and Griffin, M. A. 2006. "A study of the lagged relationships among safety climate, safety motivation, safety behavior, and accidents at the individual and group levels," *Journal of Applied Psychology* (91:4), pp. 946-953

Organ, D. W. 1988. *Organizational Citizenship behavior: The good soldier syndrome*, Lexington Books, Lexington, MA

Pahnila, S., Siponen, M. T., and Mahmood, A. 2007. "Employees' Behavior Towards IS Security Policy Compliance," in *Proceedings of the 40th Hawaii International Conference on System Sciences*, Big Island, Hawaii, USA, pp. 1-10.

Petter, S., Straub, D., and Rai, A. 2007. "Specifying formative constructs in information systems research," *MIS Quarterly* (31:4), pp. 623-656.

Podsakoff, P. M., and Organ, D. 1986. "Self-Reports in Organizational Research: Problems and Prospects," *Journal of Management* (12), pp. 531-544.

Podsakoff, P. M., MacKenzie, S. B., Moorman, R. H., & Fetter, R. 1990. "Transformational leader behaviors and their effects on followers' trust in leader, satisfaction, organizational citizenship behaviors," *The Leadership Quarterly* (1:2), pp 107-142.

Podsakoff, P. M., MacKenzie, S. B., Paine, J. B., & Bachrach, D. G. 2000. "Organizational citizenship behaviors: a critical review of the theoretical and empirical literature and suggestions for future research," *Journal of Management* (26:3), pp. 513-563.

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.

Preacher, K. J., and Hayes, A. F. 2010. "Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models," *Behavior Research Methods* (40:3), pp. 879-891.

Probst, T. M., and Brubaker, T. L. 2001. "The effects of job insecurity on employee safety outcomes: Cross-sectional and longitudinal explorations," *Journal of Occupational Health Psychology* (6:2), pp. 139-159.

Rafferty, A. E., and Griffin, M. A. 2004. "Dimensions of transformational leadership: Conceptual and empirical extensions," *The Leadership Quarterly* (15:3), pp. 329-354.

Rogers, R. W. 1975. "A protection motivation theory of fear appeals and attitude change," *Journal of Psychology* (91:1), pp. 93-114.

Rogers, R. W. 1983. "Cognitive and physiological processes in fear appeals and attitude change: A Revised theory of protection motivation," in *Social Psychophysiology,* J. Cacioppo and R. Petty (eds.), New York: Guilford Press.

Sadeghi, A., and Lope Pihie Z. A. 2012. "Transformational Leadership and Its Predictive Effects on Leadership Effectiveness," *International Journal of Business and Social Science* (3:7), pp. 168-197.

Sharma, R., and Yetton, P. 2003. "The Contingent Effects of Management Support and Task Interdependence on Successful Information Systems Implementation," *MIS Quarterly* (27:4), pp. 553-556.

Shrout, P. E., Bolger, N. 2002. "Mediation in Experimental and Nonexperimental Studies: New Procedures and Recommendations," *Psychological Methods* (7:4), pp. 422-455.

Siemsen, E., Roth, A., and Oliveira, P. 2010. "Common Method Bias in Regression Models With Linear, Quadratic, and Interaction Effects," *Organizational Research Methods* (13:3), pp. 456-476.

Siponen, M. T., and Kajava, J. 1998. "Ontology of Organizational IT Security Awareness - From Theoretical Foundations to Practical Framework," in *Seventh IEEE International Workshops on*

Enabling Technologies: Infrastructure for Collaborative Enterprises Proceedings, Stanford, CA, USA, pp. 327-331.

Siponen, M. T., 2000. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security* (8:1), pp.31-41.

Siponen, M. T., Phanila, S., and Mahmood, A. M. 2006. "A New Model for Understanding Users' IS Security Compliance," in *Proceedings of the 10th Pacific Asia Conference on Information Systems*, Kuala Lumpur, Malaysia, Paper 48.

Siponen, M. T., and Vance, A. 2010. "Neutralization: New Insight into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Siponen, M., 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* (23:3), pp. 289-305.

Sobel, M. E. 1982. "Asymptotic confidence intervals for indirect effects in structural equation models," *Social Methodology* (13), pp. 290-312.

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

Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp. 503-522.

Stewart, G., and Thelander, N. 2005. "Can IT Security be Improved with Better IT Leadership in the 21st Century University?," in *Proceedings of the 11th Americas Conference on Information Systems*, Omaha, NE, USA, pp. 2762-2766.

Stewart, J. 2006. "Transformational Leadership: An Evolving Concept Examined through the Works of Burns, Bass, Avolio, and Leithwood," *Canadian Journal of Educational Administration and Policy,* (54:1) pp. 1-29.

Sun, H. 2012. "Understanding User Revisions when Using Information System Features: Adaptive System Use and Triggers," *MIS Quarterly* (36:2), pp. 453-478.

Turel, O., Serenko, A., and Giles, P. 2011. "Integrating Technology Addiction and Use: An Empirical Investigation of Online Auction Users," *MIS Quarterly* (35:4), pp. 1043-1061.

Uffen, J., Guhr, N., and Breitner, M. H. 2012. "Personality Traits and Information Security Management: An Empirical Study of Information Security Executives," in *Proceedings of the 33rd International Conference on Information Systems,* Orlando, FL, USA.

Vroom, V. H., 1964. *Work and motivation*: Oxford, England: Wiley

Vroom, C., von Solms, R. 2004. "Towards Information Security Behavioral Compliance," *Computer & Security* (23:3), pp. 191-198.

Walumbwa, F. O., Avolio, B. J., and Zhu, W. 2008. "How transformational leadership weaves its influence on individual job performance: The role of identification and efficacy beliefs," *Personnel Psychology* (61:4), pp. 793-825.

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. "The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention," *European Journal on Information Systems* (20:3), pp. 267-284.

Warner, J. 2006. "Towards Understanding User Behavioral Intentions to Use IT Security: Examining the Impact of IT Security Psychological Climate and Individual Beliefs," in *Proceedings of the 12th Americas Conference on Information Systems*, Acapulco, Mexico, pp. 4536- 4540.

Wetzels, M., Odekerken-Schroder, G., and van Oppen, C. 2009. "Using PLS Path Modeling for Assessing Hierachical Construct Models: Guidlines and Empirical Illustration," *MIS Quarterly* (33:1), pp. 177-195.

Wood, R. E., Goodman, J. S., Beckmann, N., and Cook, A. 2008. "Mediation Testing in Management Research – A Review and Proposals," *Organizational Research Methods* (11:2), pp. 270-295.

Xue, Y., Liang, H., and Wu, L. 2011. "Punishment, Justice, and Compliance in Mandatory IT Settings," *Information Systems Research* (22:2), pp. 400-414.

Yukl, G. 2006. *Leadership in organizations*. Upper Saddle River, NJ: Pearson Education, Inc.

Zhang, J., Reithel, B. J., and Li, H. 2009. "Impact of perceived technical protection on security behaviors," *Information Management & Computer Security* (17:4), pp. 330-340.

Zhu, Y. 2013. "Individual Behavior: In-role and Extra-role," *International Journal of Business Administration* (4:1), pp. 23-27.