Journal of the Association for Information Systems (2020) **21**(1), 152-174
doi: 10.17705/1jais.00595

RESEARCH ARTICLE

ISSN 1536-9323

The Mediating Role of Psychological Empowerment in Information Security Compliance Intentions

Gurpreet Dhillon[1], Yurita Yakimini Abdul Talib[2], Winnie Ng Picoto[3]

[1]University of North Carolina Greensboro, USA, gdhillon@uncg.edu
[2]Universiti Utara Malaysia, Malaysia, yurita@uum.edu.my
[3]University of Lisbon, Portugal, w.picoto@iseg.ulisboa.pt

Abstract

The issue of employee noncompliance with information security policies is universal. Noncompliance increases the possibility of invasive information security threats, which can result in compromised organizational assets. Although research has empirically revealed a relationship between structural empowerment and employee intention to comply with information security policies, the mediating role of psychological empowerment in the relationship has received limited attention. This study conceptualizes the role of psychological empowerment as a mediator between structural empowerment and the intention to comply with information security policy. It suggests that empowerment work structures, which include information security education, training, and awareness (SETA), access to information security strategic goals, and participation in information security decision-making all increase employees' feelings of being psychologically empowered, which consequently leads to positive intentions to comply with information security policy.

Keywords: Information Security, ISP Compliance Intention, Structural Empowerment, Psychological Empowerment

France Bélanger was the accepting senior editor. This research article was submitted on October 1, 2016, and underwent three revisions.

1 Introduction

Over the past few years, information security threats have been on the rise. Whether caused by ransomware attacks, which are growing at a rate of 2500% per year (Borkhataria, 2017), or just simple human error, these information security concerns are real and constitute a cause for concern. While several factors can be attributed to the increased number of security incidents, the lack of compliance with information security policies is often singled out as the primary cause. Security breaches are typically classified into intentional versus unintentional compliance categories (see Jouini et al., 2014). However, irrespective of the classification, humans play a significant role in violations (see Boulton, 2017; Mann, 2017). A study by CompTIA (2015) found that the leading cause of information security breaches was "end user failure to follow policies and procedures" (42%). They also found that 54% of respondents indicated that their company offered some form of security training. Since a significant proportion of information security lapses are attributed to humans (including employees), understanding the factors that motivate individuals to comply with information security policies (ISPs) would help improve information security overall.

Organizations and researchers alike are focusing on control and punitive regimens intended to "force" employees to comply with ISPs. However, this may be counterproductive, as individuals who feel controlled or oppressed by external forces may resist such control via poor performance on ISP-related tasks. A metaanalysis conducted by Deci, Koesntner, & Ryan (1999) found that “expected tangible rewards made contingent upon doing, completing, or excelling at an interesting activity undermine intrinsic motivation for that activity” (p. 632). In contrast, fully empowered employees may perform tasks more skillfully (Thomas & Velthouse, 1990; Spreitzer, 2008) and may also assume more task-related decision-making responsibility. Research has also found that empowerment enhances employee perceptions of meaningfulness, autonomy, and performance impact (see Spreitzer, 1996; Hon & Rensvold, 2006; Logan & Ganster, 2007; Seibert, Wang, & Courtright, 2011). Although control and punitive approaches are heavily researched and recommended strategies (Padayachee, 2012), employees who are not sufficiently motivated to take ownership of ISP compliance processes may fail to fully devote themselves to behavioral changes, thus potentially diminishing the long-term success of ISP compliance initiatives (Siponen & Vance, 2010; Guo et al., 2011; Guo & Yuan, 2012).

In spite of multiple calls to investigate the intrinsic factors influencing ISP compliance (Herath & Rao, 2009a; Son, 2011; Padayachee, 2012), little progress has been made. In our study, we deepen the understanding of the role that intrinsic motivation plays in ISP compliance intention. This is accomplished by conceptualizing compliance intention in terms of structural and physiological empowerment. Therefore, our work enhances the understanding of employee empowerment, particularly in terms of how it helps promote successful information security practices such as ISP compliance.

This research thus addresses the following questions:

1. What is the relationship between structural empowerment and ISP compliance intentions?
2. Does psychological empowerment play a mediating role between structural empowerment and ISP compliance intentions?

To answer these questions, we develop a theoretical model to explain how empowerment structures and psychological empowerment influence ISP compliance intentions. It is proposed that structural empowerment leads to employee ISP compliance, which then helps organizations protect their assets. However, the benefits provided by structural empowerment likely require a mediating mechanism in order to impact ISP compliance intentions. We propose that psychological empowerment (the feeling of competence, meaning, impact, and choice in what one does, i.e., the intrinsic value of the task) can act as such a mediator and offer a model that explains this mechanism of mediation. We tested this model using a survey of 290 employees from various organizations in the USA and analyzed the data using structural equation modeling.

2 Theoretical Background

This section draws upon three bodies of research that form the basis for a theoretical understanding of the intention to comply with information security policies: namely, ISP compliance, structural empowerment, and psychological empowerment.

2.1 ISP Compliance

ISP compliance is the act or process of conforming to official requirements and includes the disposition to yield to others (Herath & Rao, 2009a; Bulgurcu, Cavusoglu, & Benbasat, 2010). ISP compliance intentions reflect a person’s intention to perform security tasks and activities as prescribed in an organization’s ISP. Information systems researchers have studied the intention to comply with an ISP by focusing either on the extrinsic or the intrinsic motivation of individuals (e.g., see Chen et al., 2012). Research on extrinsic factors has highlighted the importance of sanctions, rewards, monitoring, and social pressures, while research focusing on intrinsic factors for ISP compliance has pointed out the significance of perceived effectiveness, perceived self-efficacy, perceived value congruence, and perceived ownership (see Table 1 for details).

Bulgurcu et al. (2010) argue that the security tasks mandated by an ISP typically require an employee to make an extra effort to accomplish the task. Because of the associated inconvenience, many employees choose not to complete the required security tasks (Albrechtsen, 2007). Herath & Rao (2009a) also note that employees tend to prioritize other tasks over tasks related to security policy compliance. Hence, ensuring compliance with information security policies is a constant struggle.

While there have been extensive studies on ISP compliance, the focus has mainly been on the value of extrinsic rewards for employees. However, as noted by Herath & Rao (2009a), both intrinsic and extrinsic rewards are important. Intrinsic motivational factors, such as self-efficacy, psychological ownership, commitment, perceived effectiveness, and perceived value congruence, can all serve to influence an employee’s decision to comply with an ISP (Herath & Rao, 2009b, Rhee, Kim, & Ryu, 2009; Workman, Bommer, & Straub, 2008; Son, 2011; Anderson & Agarwal, 2010; Aurigemma & Leonard, 2015). Furthermore, Son (2011) found that the intrinsic factors may be superior to extrinsic factors for explaining the variance in ISP compliance. This suggests that the factors associated with the intrinsic motivation to comply with ISPs should be carefully considered. Table 1 summarizes the extrinsic and intrinsic factors affecting ISP compliance.

Table 1. Summary of Factors Affecting ISP Compliance

Motivation	Factors	Description	Theory used	Seminal papers
EXTRINSIC	Sanctions	I comply with security policies to avoid penalties.	General deterrence theory (GDT); Agency theory	Bulgurcu et al. (2010); Pahnila et al. (2007); Straub (1990)
	Monitoring	I comply with security policies because I know my activities are being monitored.	Control Theory	Boss et al. (2009); Stanton & Weiss (2000); D'Arcy, Hovav, & Galletta (2009); Straub (1990)
	Rewards	I comply with security policies to attain rewards.	Rational choice theory; theory of planned behavior	Boss et al. (2009); Bulgurcu et al. (2010); Stanton & Weiss (2005)
	Normative beliefs	I comply with security policies because I believe that others (supervisors, IT management, and peers in ID departments) expect me to comply.	Protection motivation theory	Bulgurcu et al. (2010); Herath & Rao (2009a); Pahnila et al. (2007)
	Social climate/ observations	I comply with security policies because I observe that my management, supervisors, and colleagues place great importance on prescribed security procedures.	Protection motivation theory	Chan, Woon, & Kankanhalli (2005); Herath & Rao (2009a); Leach (2003)
INTRINSIC	Perceived effectiveness	I comply with security policies because I perceive that my security actions will help improve my organization.	None	Herath & Rao (2009b)
	Perceived self-efficacy	I comply with security policies because I perceive that I have the skills or competence to perform security tasks.	Self-efficacy Theory	Chan et al. (2005); Rhee et al. (2009); Workman et al. (2008)
	Perceived value congruence	I comply with security policies because I perceive that the security values/goals are in congruence with my values.	None	Son (2011)
	Perceived ownership	I comply with security policies because I perceive that I own the assets (computer, Internet)	None	Anderson & Agarwal (2010)

2.2 Structural Empowerment

Kanter (1977) introduces the concept of empowerment in her seminal book, *Men and Women of the Corporation*. In this book, she argues that power is derived from the structural conditions within an organization and is not inherent to personality traits or the effects of socialization. Additionally, she states that work environments that provide access to information, resources, support, and opportunities to learn and develop facilitate employees' feelings of empowerment. Empowered employees are more likely to be satisfied with their tasks, and satisfaction with tasks influences the quality of task performance. Empowerment in the workplace is also affected by the degree of power sharing among employees. With a certain amount of power, employees are able to think for themselves about the requirements of their task or job and are therefore less likely to blindly do what they are told to do (Thorlakson & Murray, 1996). Empowerment also enables employees to take appropriate action when facing work challenges (Kanter, 1977, 1983; Quinn & Spreitzer, 1997). Building on Kanter (1977), empowerment in the context of information security is related to power sharing among employees, which can enable employees to make the best possible choices for their organizations. Endowed with such power, employees will thus be more likely to perform security tasks as prescribed by the ISP since they are able to think for themselves about the importance of ISP compliance in a context of minimal monitoring and control.

The concept of employee perceptions of working conditions is central to Kanter's (1977) theory. Kanter discusses several practices that indicate structural empowerment, including: (1) access to opportunity; (2) access to information, and (3) participation in decision-making. *Access to opportunity* relates to job or task conditions that provide individuals with opportunities for growth and development within the organization, as well as opportunities to develop their skills, abilities, and knowledge. Access to opportunity allows an individual to learn about skills and the economies pertinent to the larger organization (Lawler, 1986). Laschinger (1996) defines access to opportunity as being opportunities for growth and movement within an organization, as well as opportunities to enhance and develop one's knowledge and skills, which could be achieved through training and education programs.

Another important part of social-structural empowerment is *access to information*. Kanter (1977) posits that access to information refers to the ability to obtain the knowledge and information necessary to carry out a task and understand what is going on in the larger organization. In his discussion of emerging information technologies, Hoffman (2001), states that, "to support worker empowerment throughout [the] enterprise we will be prepared to provide every worker with all information relevant to that worker's job, regardless of its effect on the company as a whole (Hoffman, 2001, p. 55)." Laschinger (1996) refers to access to information as possessing information regarding organizational goals and policy changes. Other researchers (Conger & Kanungo, 1988; Liao et al., 2009) have also identified information regarding the mission and future direction of the organization as important elements of access to information. Access to information about organizational goals helps employees perceive that their tasks are meaningful and important. Information about strategies or operational goals allows employees to view their work as meaningful because they understand how it fits into organizational goals and strategies (Seibert et al., 2011). In other words, access to information about strategy and goals allows an individual to see the "big picture" and hence helps employees understand how their work can contribute to larger organizational goals (Bowen & Lawler, 1992).

Finally, Kanter's (1977) theory also postulates that empowerment can occur through *participation in the decision-making process*. This means that employees are able to provide input and exercise influence over decisions. Inputs in this context consist of strategic and day-to-day operational decisions related to one's job or task. Knoop (1995) notes that participation is the act of sharing decision-making with others to achieve organizational goals. When employees work at the operational level, they are better able to understand how specific actions related to their jobs or tasks affect the organization. Such employees are also more likely to offer valuable ideas on how operations can be improved and their suggestions are more likely to be accepted and adopted.

2.3 Psychological Empowerment

The literature characterizes psychological empowerment as a multifaceted concept that is generally related to "job incumbent activities" (Knoop, 1995). Following Spreitzer (1995a) and in the context of ISP compliance intention, we equate such job-incumbent activities with intrinsic motivation factors. Based on Thomas and Velthouse (1990), we then define intrinsic motivation as, "positively valued experiences that the individual derives directly from the task" (p. 668). These positive experiences are related to the individual conditions pertaining to a task, which may then result in employee satisfaction and motivation. Intrinsic motivation exists within individuals; as such, the motivation to act emerges from intrinsic regulation, or from the self and the task itself, rather than from others, or from extrinsic factors (Thomas & Velthouse, 1990). Various theories have documented this need for drivers or antecedents to enhance the intrinsic motivation related to one's task or job (Deci et al., 1999; Hackman & Oldham, 1980; Deci & Ryan, 1985).

Several previous studies (Thomas & Velthouse, 1990; Spreitzer et al., 1997; Wat & Shaffer, 2005; Ke & Zhang, 2011; Campbell et al., 1993) have found that intrinsic motivation yields various performance-related outcomes. Such outcomes include individual task performance, increased work effort, effectiveness, and organizational citizenship behavior. With respect to intrinsic motivation, the intrapersonal or psychological empowerment role as mediator between social structural context and behavioral outcomes has previously been studied in the literature (Chen & Klimoski, 2003). Psychological empowerment is formed based on individual assessment or judgments of a task in terms of four cognitions: competence, meaning, impact, and choice (Spreitzer, 1995a). Empowerment refers to a set of cognitions reflecting personal perceptions about a task and one's ability to control, shape, or influence that task (Thomas & Velthouse, 1990; Spreitzer, 1995b). This contrasts with structural empowerment, which focuses on managerial practices that share power with employees (Spreitzer, 1995a). Thus, at the core of such models is the identification of cognitions known as task assessments. In other words, individuals are intrinsically motivated whenever they experience the following four cognitions in relation to a task: competence, meaning, impact, and choice.

Work structures that empower employees tend to increase individuals' overall sense of empowerment (Thomas & Velthouse, 1990). Additionally, work structures that provide access to opportunity in the form of educational opportunities contribute to individuals' intrinsic motivation by increasing their beliefs in their capability to perform task activities skillfully (Spreitzer, 2008; Thomas & Velthouse, 1990). Similarly, access to information may help employees perceive a job or task to be meaningful and important because it allows them to understand how their tasks contribute to the organization's goals (Liao et al., 2009; Spreitzer, 1995b). Autonomy and decision-making opportunities allow employees to contribute to and influence decisions, which thus makes them more likely to experience a greater sense of self-determination and meaning about what they do at work (Spreitzer, 2008).

Although empowerment structures may influence various performance-related outcomes, we postulate that the effect is likely to be indirect and argue that psychological empowerment serves as a mediator. The idea of psychological empowerment serving as a mediator between structural empowerment and performance-related outcomes has been supported in numerous studies (Spreitzer, 2008; Maynard et al., 2012), albeit not in the context of ISP compliance intentions. Changing the organizational structural context is not sufficient for changing individual behavior, as ultimately an individual sense of empowerment is necessary to influence such behaviors. For example, Spreitzer (1995b) found support for the claim that psychological empowerment partially mediates the relationship between social structures and innovative behavior. In addition, Liao et al. (2009) found that cognitions of empowerment fully mediate the relationships between high-performance work systems and service performance. Furthermore, Laschinger et al. (2001) found that psychological empowerment mediates the relationship between structural empowerment and individual satisfaction. In these studies, both structural and psychological empowerments were measured as composite constructs. Our study extends these studies by focusing specifically on an important form of performance-related outcomes—namely, ISP compliance behavior intentions.

3 Research Model and Hypotheses

This study focuses on three categories of structural empowerment in information security that have theoretical links to psychological empowerment: (1) security education, training and awareness (SETA); (2) access to an organization's information security strategy and goals; and (3) participation in information security decision-making. Based on these categories of structural empowerment, this work draws upon the seminal work of Spreitzer (1995b) to propose that psychological empowerment plays a mediator role between empowerment structures and ISP compliance intentions. We present the initial research model in Figure 1.

In their consideration of independent dimensions of psychological empowerment, Gist & Mitchell (1992) found that self-efficacy could mediate the effects of training on individual performance. In a medical context, Bonias et al. (2010) tested for a mediating effect of all dimensions of psychological empowerment and found that feelings of competence, meaning, and autonomy fully mediate the relationship between high-performance work systems and quality of patient care. Our paper draws on studies such as these to investigate the mediating role of psychological empowerment on the relationship between elements of structural empowerment and the intention to comply with information security policies (i.e., individual performance-related outcomes).

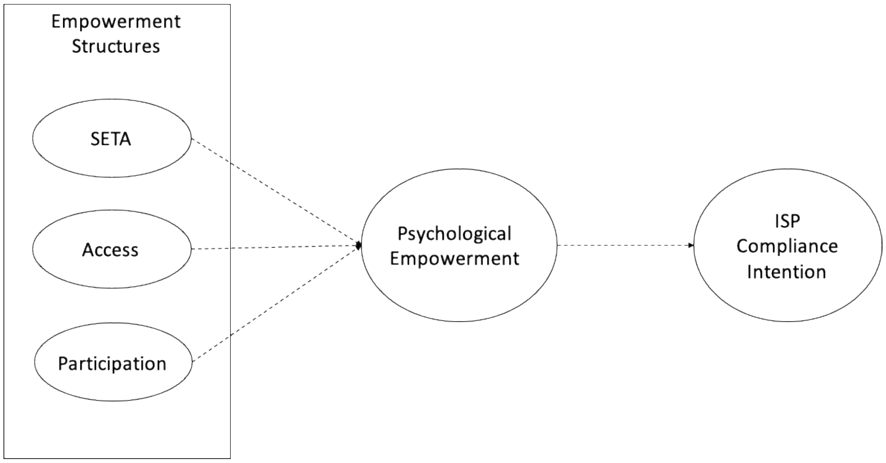


Figure 1. Research Model: Mediating Role of Psychological Empowerment

3.1 SETA and Employees' Intention to Comply

Security education, training, and awareness (SETA) programs focus on providing users with a general knowledge of the information security environment along with the skills necessary to perform the required information security tasks (D'Arcy et al., 2009). Through SETA, individuals are educated in information security and have an opportunity to discuss the successes and failures associated with different information security behaviors. As such, this information can serve a guideline for employees against which they can compare their own self-efficacy (Bandura, 1977).

In addition, verbal persuasion is a regular feature of SETA programs. Individuals receive suggestions from instructors that encourage and support their information security skills and foster responsible development. Thus, we anticipate that psychological empowerment (i.e., competence) regarding information security tasks may be developed through the ongoing acquisition of knowledge related to information security, including information about the consequences, coping strategies and action paths associated with information security issues. Since employees who feel empowered are more likely to believe they can competently perform information security tasks as prescribed in the ISP, they are more likely to have positive feelings toward performing information security tasks. These positive feelings, in turn, may increase their motivation to carry out the actions necessary to perform the information security tasks. In other words, we believe that SETA programs likely have positive impacts on ISP compliance intention by psychologically empowering (competence) individuals. Some empirical studies have examined the influence of perceived competence on information security behaviors (e.g., Chan et al., 2005; Workman et al., 2008; Herath & Rao, 2009b; Rhee et al., 2009). For instance, Chan et al. (2005) found that employees' beliefs in their information security efficacy influence their decision to perform activities related to information security, particularly those prescribed by the organization's ISP. Rhee et al. (2009) demonstrate that self-efficacy in information security influences individuals' intentions to strengthen their security compliance efforts and also encourages their use of security protection software and compliance behavior. This leads to the following hypothesis:

H1: Psychological empowerment mediates the relationship between SETA and employees' intentions to comply with an ISP.

3.2 Access to Information and Employees' Intention to Comply

Access to an organization's information security strategy and goals denotes the extent to which the work structure provides opportunities for employees to obtain and understand their organization's information security strategic objectives and goals. This can be accomplished through the communication of an ISP that comprises the goals related to information security (Straub, 1990; Boss et al., 2009). Access to information regarding security strategies and goals helps individuals feel informed about where an organization is headed in the context of information security. When employees have sufficient information about security, they tend to be more aware of how performing their own information security tasks can contribute to achieving the organization's stated information security goals (Spreitzer, 1995a). In other words, access to information helps employees acquire a greater sense that the information security tasks they are charged with are meaningful and serve a purpose, which in turn enhances their ability to make choices aligned with an organization's information security goals.

Accordingly, employees' access to an organization's information security strategies and goals increases the meaning of their information security tasks, thus affecting the employees' ISP behavioral intentions. Empowered employees who believe that information security tasks, as prescribed in the ISP, are meaningful are thus more likely to engage in ISP-compliant behaviors. Thomas & Velthouse (1990) suggest that individuals who are more likely to engage put more energy into tasks if the task activities are meaningful, serve an important purpose, and are also in accordance with their own values and goals. Individuals who believe that assigned tasks are meaningful are more likely to be motivated to invest in accomplishing the goal related to the task because, by doing so, they are also able to reach their own goals. This leads to the following hypothesis:

H2: Psychological empowerment mediates the relationship between access to information and employees' intentions to comply with an ISP.

3.3 Participation in Decision-Making and Employees' Intentions to Comply

Participation in decision-making means that employees at all levels are able to contribute to and influence decisions related to a specific task or job (Cotton et al., 1988). In the context of information security, participation relates to an individual's involvement in the information security decision-making process. Spears & Barki (2010) define participation in security risk management as a set of activities assigned to individuals during the risk assessment, design, and implementation of information security controls. Participation in information security decision-making allows individuals to contribute to their organization's information security goals by, for example, expressing thoughts and opinions regarding information security. Fostering participation in decision-making, in turn, strengthens the motivation of employees to engage in behaviors related to information security by providing them with opportunities to gain intrinsic rewards from their work, including a greater experience of self-determination, meaningfulness, and impact (Scandura Graen, & Novak, 1986; Manz & Sims Jr, 1987; Spreitzer, 1996). Employee involvement in decision-making processes related to information security tasks can help further the goals of the ISP. As such, participation gives employees the sense that they have a certain degree of freedom and independence in making information security task-related decisions. Participation is an influential source of self-determination in that it provides evidence of the inputs, thoughts, contribution, and activities related to one's job (Lawler, 1992; Spreitzer, 1996). In a case study setting in information security, Dhillon, Silva, and Backhouse (2004) found that most employees do not feel a sense of freedom at work because they were left out of all major decision-making and they had no say about the latest developments related to information security in the organization.

Greater participation may also serve as an impetus to enhance individual feelings of impact (Seibert et al., 2011). When employees participate in decision-making processes related to their information security task, they have the opportunity to make decisions jointly with their superiors. This likely influences the extent to which employees feel that they can impact their work environment. Spreitzer (1996) provided empirical evidence of the relationship between participation in decision-making and perceived impact. Spreitzer concluded that participation signals to employees that they are important to the organization and that they can impact or make a significant difference to the organization. Furthermore, when employees are allowed to participate in the decision-making process related to their information security task, they have the opportunity to offer input that is consistent with their own values or needs, which then shape the information security task. Therefore, they are more likely to perceive the information security task to be meaningful and important. Hon and Rensvold (2006) provide evidence indicating that participation is strongly related to the perceived meaning of a task. We would thus expect that if employees are involved in decision-making processes related to information security tasks, and if they have opportunities to offer their input in furthering information security objectives, this would affect the work environment, which leads to the following hypothesis:

H3: Psychological empowerment mediates the relationship between participation in decision-making and employees' intentions to comply with an ISP

4 Research Method

4.1 Sample Selection and Data Collection

The sample for this study was composed of employees at both management and non-management levels. As the primary thrust of this study is to investigate the relationship between individuals' perceptions of structural empowerment related to their information security task and ISP compliance behavior intentions in the workplace, we surveyed employees in different jobs and at different levels. Respondents were drawn from MBA, Executive MBA and Executive MIS students enrolled at two public US universities. We distributed a self-administered survey instrument and a cover letter explaining the purpose of the study, as well as information about willingness, confidentiality, and anonymity, to 410 respondents. Of the 410 surveys distributed, 326 complete responses (79.5%) were returned and 36 of these met the exclusion criteria for the questions (i.e., the respondents were not employed, did not know whether their organization had an ISP, or were not aware of the ISP requirements) and were thus excluded from the study. This resulted in a final sample size of 290 responses with potentially useable data. An additional assessment for missing data identified one case that was excluded to an excessive number of missing values (40%).

4.2 Operationalization of the Constructs

The constructs in this study were measured using multi-item scales adapted from previously validated studies (see Appendix 1). All measures used 7-point Likert-type scales with anchors ranging from 1 (*strongly disagree*) to 7 (*strongly agree*). The survey instrument was pretested with eight management and information systems academics to assess the clarity of the questions and the structure of the questionnaire. No changes resulted from the pretest.

We used three items from Bulgurcu et al. (2010) to measure ISP-compliant behavior intentions. For example, respondents were asked how much they agreed or disagreed with statements such as: "I intend to comply with the requirements of the information security policy of my organization," and "I intend to protect information and technology resources according to the requirements of the information security policy of my organization." This measure demonstrated an acceptable level of reliability (α = 0.75).

Three constructs served to define structural empowerment: SETA, access to information security, and participation in information security decision-making. SETA was measured using five items from D'Arcy et al. (2009), such as: "I receive training to help me improve my awareness of computer and security issues" and "I am briefed on the consequences of modifying computerized data in an unauthorized way." The scale had an acceptable level of reliability (α = 0.88). We adapted three items from Spreitzer (1995a) to measuring access to information security strategies and goals, including: "I have access to the strategic information that I need to do my job of securing information and information systems well." This scale demonstrated an acceptable level of internal consistency (α = 0.76). Two items to measure participation in information security decision-making were adapted from Spears and Barki (2010). For instance, respondents were asked to specify the extent to which they agreed or disagreed with statements such as: "I actively participate in defining, reviewing, or approving information security controls related to protecting the organization's information." This scale also had an acceptable level of reliability (α = 0.78).

Psychological empowerment is a second-order construct (Spreitzer 1995a) comprised of competence, meaning, impact and choice. In order to assess the appropriateness of representing the individual dimensions instead of a single, global psychological empowerment construct, we performed confirmatory factor analyses (CFAs). The CFAs show that the hypothesized four-factor model χ^2 (48, N = 289) = 91.45, $p < 0.05$; RMSEA = 0.056; SRMR = 0.047; CFI = 0.98; NFI = 0.96) fits the model better than a model with one construct χ^2 (50, N = 289) = 111.85, $p < 0.05$; RMSEA = 0.066; SRMR = 0.075; CFI = 0.97; NFI = 0.95). These results are consistent with previous research showing that the four dimensions of psychological empowerment are distinct (e.g., Spreitzer, 1995a; Kraimer, Seibert, & Liden, 1999). Consistent with this, we adapted separate scales from Spreitzer (1995a) that measured each dimension of psychological empowerment.

We used three items to measure perceived competence. First, respondents were asked to what extent they agree or disagree with statements such as: "I am confident about my ability to do my job of securing information and information systems." The scale demonstrated a high level of reliability (α = 0.89). Perception of meaning was measured using three items. These items included: "My work of securing information and information systems is very important to me" and "My work of securing information and information systems is meaningful to me." This scale was also highly reliable (α = 0.91). Next, we measured perceived impact from the employees' perspective by using three items, including: "My impact on what happens in my department related to information security is large." This scale revealed a high level of reliability (α = 0.90). Finally, perceived choice was measured using three items, which included: "I have significant autonomy in determining how I do my job of securing information and information systems." The reliability of this scale was acceptable (α = .78).

5 Results

Table 2 provides the demographic characterization of our final sample. We analyzed the collected data using the covariance approach to structural equation modeling (SEM) with AMOS Version 18. SEM, a multivariate statistical technique, is a powerful quantitative data analysis tool that enables researchers to observe the structural element (path model) and measurement element (factor model) simultaneously (Gefen, Straub, & Boudreau, 2000). Nunnally (1978) suggests that in SEM estimation, there should be at least ten times as many subjects as indicators. In the tested model, 25 indicators were present, implying that a minimum sample size of 250 was needed. Therefore, our sample size of 290 was adequate for modeling. We used Anderson and Gerbing's (1988) two-step approach, which assessed and improved the measurement model prior to testing the structural model.

5.1 Measurement Model

The measurement model estimates the relationships between the measured variables (scale items) and the latent constructs they represent. This involves the estimation and evaluation of construct reliability (individual item and composite reliabilities), validity (convergent and discriminant validities) of the measurement model, and overall measurement model fit.

By examining the factor loading of each item to its related construct, the individual item reliability was assessed. At a minimum, all the factor loadings must be statistically significant ($p < 0.05$). As a general rule, the standardized loading estimates should be 0.5 or higher (Hair et al., 2010). In the measurement model, all items loaded significantly ($p < 0.05$, two-tailed) to the respective constructs (Table 3). Nunnally (1978) suggests that composite reliability should be 0.7 or higher for a construct to demonstrate adequate reliability. As shown in Table 3, the Cronbach's alphas were between 0.75 and 0.91 and the composite reliability for all the constructs in our model ranged from 0.76 to 0.91, which thus indicates adequate composite reliability.

Table 4 shows the convergent and discriminant validities. Convergent validity measures the extent to which items for each construct are related to each other, assessed by average variance extracted (AVE).

An AVE measure of 0.5 or higher demonstrates adequate convergent validity (Hair et al., 2010). The AVEs for all the constructs in the model were above the cut-off value, indicating adequate convergent validity. Finally, to confirm the discriminant validity of the constructs, the square root of every AVE value belonging to each construct was tested to ensure that it was larger than the correlation among any pair of latent constructs (Fornell & Larcker, 1981). The square roots of the AVEs for all constructs, reported in the diagonal of the correlation matrix, were larger than the corresponding off-diagonal correlations, which provides evidence of adequate discriminant validity. The above analyses and evaluations indicate that the measurement model is suitably reliable and valid.

We also assessed the overall measurement model fit. Table 5 presents the values of the fit indices for the measurement model of this study. The overall measurement model fit was χ^2 (261, N = 289) = 618.87, $p < 0.001$; SRMR = 0.077, RMSEA = 0.069 with CI90: (0.062, 0.076), and CFI = 0.91. The results indicate that the values of SRMR and RMSEA were less than the selected cut-off values of 0.08 (Hu & Bentler, 1999; Byrne, 2016; Kline, 2011) and thus demonstrate "acceptable" fit (McDonald & Ho, 2002). Furthermore, the value of CFI was marginally lower than the cut-off of 0.95 (Hu & Bentley, 1999). However, many researchers use a cut-off value of 0.90 as an acceptable fit (McDonald & Ho, 2002). Overall then, the results confirm a reasonably good fit for the measurement model.

Table 2. Respondent Profile

Demographic features	**Frequency (*N*=290)**	**Percentages**
Gender		
Male	202	68.7
Female	86	29.7
Missing	2	0.7
Level of education		
High school degree	5	1.7
College degree	45	15.5
Undergraduate degree	118	40.7
Graduate degree	118	40.7
Other	1	0.3
Missing	3	1
Age		
20-25	72	33.4
26-35	147	50.7
36-45	49	16.2
46-55	18	14.8
56-65	1	27.9
Missing	3	1.7
Years working in current organization		
Less than 5 years	203	70
More than 5 years	87	30
Position in current organization		
Owner of the firm	8	2.8
Managing director/director	24	8.3
Chief executive officer	2	7
General manager/manager	47	16.2
Executive/leader/officer	28	9.7
Nonmanagement	155	53.4
Missing	26	9
	Mean	***SD***
Hours of computer usage at work per day	7.7	2.5

Table 3. Measurement Model Quality Criteria

Latent Variable	Mean	Variance	Loadings
ISP compliance intentions (α=0.75, CR=0.76)			
ISPC1	6.24	1.13	0.61
ISPC2	5.71	1.28	0.85
ISPC3	5.48	1.41	0.69
Security education, training, and awareness (α=0.88; CR=0.87)			
SETA1	4.46	2.04	0.84
SETA2	3.37	2.08	0.62
SETA3	4.44	2.03	0.74
SETA4	4.75	1.97	0.91
SETA5	4.62	2.00	0.78
Access to information security strategy and goals (α=0.76; CR=0.76)			
ACC1	4.49	1.84	0.74
ACC2	4.81	1.64	0.66
ACC3	5.03	1.58	0.74
Participation in information security decision-making (α=0.78; CR=0.78)			
PART1	3.98	1.98	0.81
PART2	3.56	2.11	0.79
Impact (α=0.90; CR=0.87)			
PACT1	4.69	1.79	0.83
PACT2	4.30	1.93	0.90
PACT3	4.43	1.97	0.86
Competence (α=0.89; CR=0.89)			
COMP1	5.08	1.43	0.89
COMP2	5.08	1.34	0.81
COMP3	4.79	1.46	0.87
Meaning (α=0.91; CR=0.91)			
MEAN1	5.09	1.76	0.88
MEAN2	4.94	1.76	0.87
MEAN3	4.98	1.69	0.89
Choice (α=0.78; CR=0.80)			
CHOI1	4.44	1.78	0.87
CHOI2	4.24	1.76	0.53
CHOI3	4.49	1.84	0.84
Notes: α = Cronbach's alpha, CR = composite reliability			

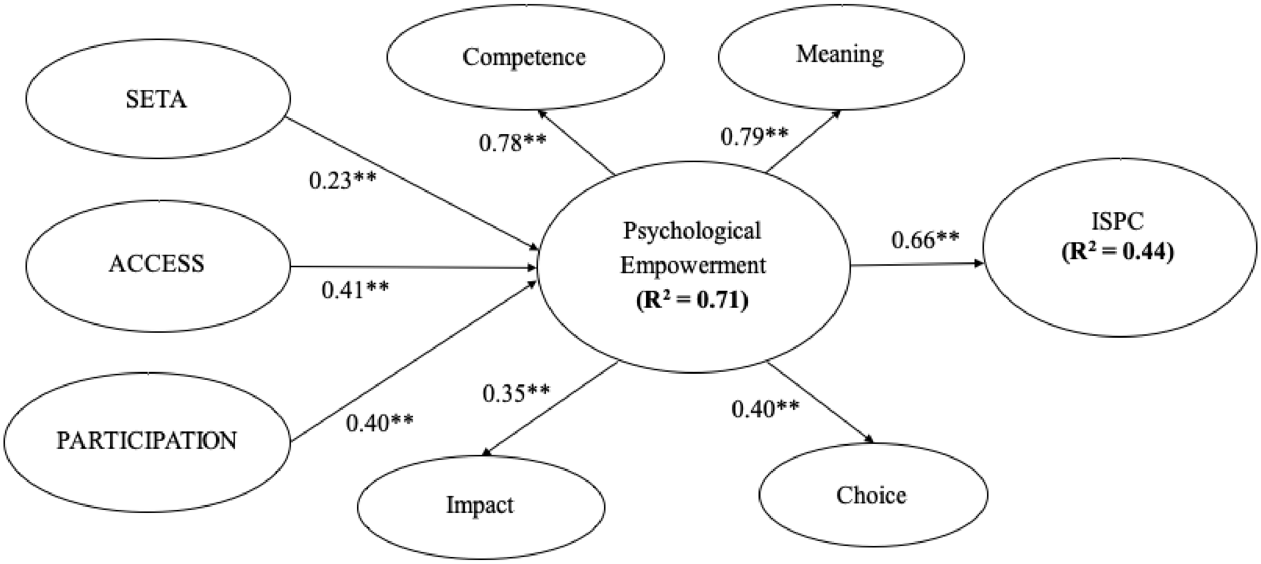
Table 4. Convergent and Discriminant Validities

		AVE	1	2	3	4	5	6	7	8
1	ISPC	0.521	**0.722**							
2	SETA	0.631	0.502**	**0.794**						
3	Access	0.512	0.595**	0.573**	**0.716**					
4	Participation	0.639	0.220**	0.286**	0.482**	**0.799**				
5	Impact	0.740	0.069	0.028	0.239**	0.638**	**0.860**			
6	Competence	0.732	0.541**	0.571**	0.514**	0.466**	0.182**	**0.855**		
7	Meaning	0.772	0.557**	0.381**	0.621**	0.523**	0.281**	0.622**	**0.878**	
8	Choice	0.579	0.211**	0.096*	0.154**	0.524**	0.366**	0.279**	0.271**	**0.761**

Table 5. Measurement Model Fit

	Chi-Square (χ^2) Statistic = 618.87 (*df* = 261, *p* < 0.001)		
Fit Measures	RMSEA	SRMR	CFI
Measurement Model	0.069 CI$_{90}$(0.062, 0.076)	0.077	0.91

Notes: df = degree of freedom; RMSEA = root mean square error of approximation; SRMR = standardized root mean square residual; CFI = comparative fit index; CI$_{90}$ = 90% confidence interval. All results were computed by AMOS.



Notes: † $p < 0.1$; * $p < 0.05$; ** $p < 0.01$ (two-tailed tests); ISPC = information security policy compliance intention; SETA = information security education, training, and awareness; ACC = access to information security strategy and goals; PART = participation in information security decision-making. R^2 = variance explained.

Figure 3. Path Diagram with Standardized Results

5.2 Structural Model

5.2.1 Overall fit

The fit statistics confirmed (see Table 6) that the model provides a good fit for the data (e.g., SRMR = 0.089, RMSEA = 0.072 with CI$_{90}$: (0.065, 0.078), and CFI = 0.91; Hu & Bentler, 1999). Figure 3 provides the standardized path loadings, including measurement model factor loadings, all of which were significant at $p < 0.05$.

5.2.2 Mediation Test

For Hypothesis 1, 2 and 3, we tested for mediation. Sobel's (1982; 1986) Product of Coefficients Test (the Sobel test) and the bootstrapping method (Shrout & Bolger, 2002) in the analysis of moment structures (AMOS) were used to examine the indirect effects. Bootstrapping is a direct technique to examine mediating effects using the standard errors and confidence interval estimates. We utilized bias-corrected bootstrapping techniques (1,000 bootstrap samples) and tested for biased-corrected two-tailed significance to confirm that the indirect effect was present. Table 7 displays the overall results of mediating effects.

Hypothesis 1 predicted that SETA would impact ISP compliance intentions through psychological empowerment. The indirect effect (β_{IND}) was 0.157. Using the Sobel test, the indirect effect of SETA was statistically significant (z = 2.151, SE = 0.007, p < .001). Furthermore, the bootstrap analysis supported the conclusion of mediation (the 95% bias-corrected confidence interval for the total indirect effect excluded zero ([.02, .305]) with a two-tailed significance value of less than 0.05) (Preacher & Hayes, 2008). Thus, psychological empowerment mediates the relationship between SETA and ISP compliance intentions, providing support for Hypothesis 1.

Table 6. Structural Model Fit

	Chi-Square (χ^2) Statistic = 656.21 (*df* = 264, *p* < 0.001)		
Fit measures	RMSEA	SRMR	CFI
Structural model	0.072 CI$_{90}$(0.065, 0.079)	0.089	0.91
Notes: df = degree of freedom; RMSEA = root mean square error of approximation; SRMR = standardized root mean square residual; CFI = comparative fit index; CI$_{90}$ = 90% confidence interval. All results were computed by AMOS.			

Table 7. Results of Mediation Tests

						Bootstrapping		
		Point estimate	**Production of coefficient**			**BC**		
Hypothesis	**Specific indirect**	**(B)**	***SE***	***Z***	***P***	**Lower**	**Upper**	**Signif.**
H1: Psychological empowerment mediates the relationship between SETA and employees' intentions to comply with an ISP.	SETA→ PE→ ISPC	0.15	0.073	2.151	**	0.02	0.305	*
H2: Psychological empowerment mediates the relationship between access to information and employees' intentions to comply with an ISP.	ACCESS→ PE→ ISPC	0.27	0.088	3.091	**	0.125	0.476	**
H3: Psychological empowerment will mediate the relationship between participation in decision-making and employees' intentions to comply with an ISP.	PARTICIPATION→ PE→ ISPC	0.26	0.055	4.764	**	0.146	0.364	***

Hypothesis 2 proposed that psychological empowerment would mediate the relationship between access to information security and employees' ISP compliance intentions. Notably, the indirect effect (β_{IND}) was 0.272. The results of the Sobel test ($z = 3.09$, $SE = 0.088$, $p < 0.001$) and the bootstrap analysis (the 95% bias-corrected confidence interval for the total indirect effect excluded zero [0.125, 0.476] with a two-tailed significance value of less than 0.01) support a conclusion of mediation. The findings thus indicate that psychological empowerment mediates the relationship between access to information security strategy/goals and ISP compliance intention, thus supporting Hypothesis 2.

Finally, Hypothesis 3 predicted that psychological empowerment would act as a mediator of the relationship between participation in information security decision-making and ISP compliance intentions. The indirect effect (β_{IND}) was 0.261. The Sobel test suggests that the indirect effect is statistically significant ($z = 4.764$, $SE = 0.055$, $p < 0.001$). The bootstrap analysis also supports the conclusion of mediation and the results show that the 95% bias-corrected confidence interval for the total indirect effect excluded zero ([0.146, 0.364]), with a two-tailed significance value of less than 0.01. Thus, the results suggest that psychological empowerment mediates the relationship between participation in information security decision-making and ISP compliance intentions, thus supporting Hypothesis 3.

6 Discussion

In this study, we set out to investigate the relationship between structural empowerment, psychological empowerment, and ISP compliance intentions. We found that psychological empowerment plays a mediating role between structural empowerment and ISP compliance intentions. In this section, we discuss what this relationship means and what actions can organizations take to increase information security compliance intentions.

The concept of structural empowerment is intricately linked to Kanter's (1977) social-structural theory. While Kanter's original ethnographic study exclusively focused on how women lacked access to "power tools"—i.e., opportunity, information, support, and resources—the findings have been generalized over the years. The concept of structural empowerment maintains that power resides with individuals and that employees can have a voice in a system. In terms of information security, Kanter defines structural empowerment as: *having access to opportunities* (in terms of security education, training, and awareness); *having access to information* (in terms of where the organization is heading in terms of information security); and *being able to participate in decision-making* (in terms of employee involvement in information security decisions).

Specific practices that indicate a highly structurally empowered organization include:

Skill/knowledge base and training: The focus of prior research has primarily been on how increased information security policy awareness effects attitude (Bulgurcu, Cavusoglu & Benbasat, 2010; Puhakainen & Siponen, 2010). Furthermore, previous studies have not linked the existence of a SETA program to increased structural empowerment. In our research, however, we found that SETA programs enhance structural empowerment, which in turn increases intentions to comply with an ISP. At a practical level, organizations should invest in programs to improve the skill/knowledge training of employees, which will consequently create structurally empowered employees. As our research indicates, enhanced skill/knowledge training programs will increase ISP compliance intentions.

Access to information: The mainstream information security literature has not investigated the access to information and its impact on ISP compliance intentions. This research has found that access to information increases ISP compliance intentions. Increased access to information includes the downward flow of information about security goals and responsibilities, the strategic directions the company wants to take regarding security, and the financial impact of security measures. Employees who have a clearer idea of the security posture of the firm (i.e., a clear line of sight) are more likely to comply with the organization's ISP.

Participative decision-making: The majority of the information security literature does not directly make reference to participative decision-making, particularly in terms of designing controls and implementing security procedures (with the exception of studies like Spears & Barki, 2010). The concept of encouraging participation in decision-making for ISP compliance is akin to forming self-managed teams, supporting the basis for authority and accountability.

Flatter organizational structures: Flatter organizations are a consequence of structurally empowered enterprises (e.g., see Groysberg and Slind, 2012). Many companies are currently moving towards flatter structures for security management, particularly due to the inherent complexity of managing hierarchical security organizations. The emergence of the data steward role is an example of how flatter organizations are being shaped to improve security (see Heilmann et al., 2018 in the context of small businesses).

Similar to Kanter's original conceptualization, access to opportunities, information, and participation in decision-making are powerful tools that individuals can use to be structurally more involved in the drive to improve information security. However, our study found that structural empowerment alone does not render a complete set of benefits. This means that simply providing the tools to employees may not effect increased ISP compliance intentions. Equally important, if not more so, are the personal beliefs of employees regarding their roles in the organization. In situations where there are problems with role definition, accountability issues often ensue. Therefore, when individual employees do not know what their roles are within the information security enterprise, there will likely be more problems related to responsibility and the ownership of certain information assets. Nissenbaum (1994), for example, argues that there are four barriers to accountability, namely: the problem of "many hands," bugs, the computer scapegoat, and ownership without liability. The problem of "many hands" is intricately linked to how roles and responsibilities are created regarding access to computing resources. While the literature has recognized some of these aspects in a piecemeal fashion, our research validates the mediating role of psychological empowerment on ISP compliance intentions.

These mediating effects have an implication for the interpretation of many information security studies that have tested the direct effects of work environments in terms of, for example, participation, communication of the goals, training, and information security outcomes, without integrating the psychological state of employees. The results of our study indicate that not only does SETA have a direct effect on information security behavior, as shown in previous studies (e.g., D'Arcy et al., 2009), but that it also has an indirect effect through the mechanism of psychological empowerment. Similarly, studies that have examined the relationship between participation and effective information security (e.g., Spears & Barki, 2010) have not tested the mediating effects that we include in our study. We found that psychological empowerment mediates the relationship between participation in information security decision-making and information security compliance intentions. Furthermore, Boss et al. (2009) identified that a well-specified ISP that gives clear directions on how to achieve information security goals is related to precautionary behavior by means of the perceptions of the mandatory nature of ISP compliance. Our study offers similar results, but also tested the mediating role of psychological empowerment in the relationship between access to information security strategy and goals and ISP compliance. Thus, a complete understanding of employees' information security behaviors in organizations requires the recognition of both intrinsic and extrinsic factors. Focusing only on providing structural empowerment (i.e., extrinsic factor) without considering psychological empowerment (i.e., intrinsic factor), provides an incomplete picture of information security behavioral intentions.

Specific practices that indicate a high level of psychological empowerment in an organization include:

Meaningfulness: A meaningful engagement is one where employees feel that their work is meaningful and linked to their own beliefs and values. Meaningfulness is of great importance in terms of information security. Often, companies allocate work (or make individuals responsible for tasks) that may not be meaningful to employees. While employees may still complete the activity, they may not feel psychologically empowered and hence may not have strong compliance intentions.

Competence: Competence refers to the belief that one has the ability to complete a specific task. Companies usually train employees in specific security protocols, hoping to make them aware of the information security risks. While such training may familiarize individuals with such risks, this does not necessarily make them competent to complete the task. This was, for example, evidenced in the computer hack case documented by Perez (2005) in which the employees had the requisite training but did not develop the competences to handle the hack.

Self-determination: It is important that employees are given a choice to self-determine the kind of controls that need to be instituted. The choices users make are typically linked to their level of competence. If individual competence is low, there is a likelihood that the quality of self-determination of controls is going to be poor. For instance, in the computer hack case presented by Perez (2005), the security staff had permission to move the server into the DMZ, which left the system vulnerable to a hack. While discretion, self-determination, and choice are important elements of psychological empowerment, these have to be executed in the context of individual competence.

Impact: This is the degree to which employees feel that they can have an influence on the strategic, administrative, or operating outcomes regarding information security management. In a study by Syed et al. (2018), it was found that when individuals have a say in operational outcomes of managing their security and privacy, it results in superior outcomes. Similarly, Sridhar, and Ahuja (2007) found that when stakeholders feel that they can impact security strategy, they become more engaged in ensuring security.

This research makes several significant contributions to the body of literature concerning intrinsic motivation to comply with information security policies. Moving forward, the findings in this study will allow researchers to investigate and develop an integrated model for ISP compliance intentions. Such a model would be a combination of the extrinsic factors model that have already been developed and the intrinsic motivation model presented in this paper. Theoretically, a mediation model in which structural empowerment impacts psychological empowerment, which in turn impacts ISP compliance intentions, was largely supported by our findings. This implies that employees who are given an opportunity to learn via SETA have access to strategic goals related to information security and participate in information security decision-making, meaning that they tend to feel more psychologically empowered. Psychologically empowered employees demonstrate a greater sense of responsibility to their information security tasks. As such, highly empowered employees will typically act in accordance with ISP requirements, even when enticed and given the opportunity violate the ISP.

From a practitioner standpoint, the results of this study have a number of valuable implications for organizations. First this study offers important strategies for organizations to increase employees' compliance with organizational ISPs. Second, our results show that as an alternative to investing in rewards or implementing penalties to incentivize ISP compliance, organizations could simply focus on structural empowerment. Third, our findings strongly suggest that management should share more "power tools" with employees at all levels. Fourth, we would specifically suggest that organizations consider allowing employees to participate in the information security decision-making processes. A participative strategy should give employees the opportunity to contribute their input, ideas, and thoughts about information security that are consistent with their own values or goals. Finally, employees should also be provided opportunities to make decisions regarding information security jointly with their superiors; when employees are allowed to participate, they feel more empowered, and will ultimately feel more motivation to comply with the ISP.

In addition, providing training related to information security is important to increase employees' feeling of competence. We would strongly urge management to create information security training and education programs that help facilitate employees' personal mastery of information security protocols through hands-on exercises and activities, or through the regular demonstration of information security measures and countermeasures. Such programs allow employees to observe the successes and failures associated with different information security behaviors, and can thus support the development of their own information security skills. Thus, when designing an information security training program, managers should pay particular attention to increasing employees' information security skills. Furthermore, given employees access to information security strategy and goals is an important strategy for enhancing employees' sense of empowerment. Thus, we recommend that management improves and diversifies its communication channels so that a well-specified ISP comprising the goals of information security can be conveyed to all employees. When employees understand the direction in which the organization is headed in terms of information security, they are likely to understand how their own information security tasks contribute to the realization of organizational information security goals. This is because employees find connections between the goals of the ISP and their own values. Such strategies are not only capable of directly increasing employees' psychological empowerment, but they can also indirectly influence employee ISP compliance intentions.

7 Conclusions

The information security behavior of employees is critical to the success of an organization, particularly in terms of potential information security breach incidents. The findings of this study indicate that structural empowerment in the form of SETA, access to information security strategic goals, and participation in information security decisions indirectly contribute to making employees ISP compliant through supporting their psychological empowerment. The cultivation of empowerment structures and a sense of psychological empowerment among employees are important strategies that can reduce the potential for insider information security breaches. This study not only expands on the information security and empowerment literatures, but also offers guidance to organizations seeking to increase information security compliance intentions among employees.

Nonetheless, this study is not without some limitations. First, it employed a cross-sectional approach, which does not permit drawing conclusions concerning causal direction. Furthermore, it is possible that the respondents' feelings and thoughts in answering the survey questions were influenced by their environment, which is commonly referred to as the "halo effect" (Herath & Rao, 2009a). Additionally, survey data specifically queried ISP compliance intentions rather than actual ISP compliance behavior. We recognize that intention to comply may not result in actual compliance; thus, an investigation of factors capable of bridging the gap between ISP intentions and actual compliance behavior would be an interesting future research direction. Future research could also extend our study in a number of other ways. For example, it could explore different drivers for enhancing the feeling of empowerment, such as task characteristics, leader-member exchange (LMX), formal and informal power, and personality traits. In addition, future research could investigate whether the effect of psychological empowerment may be moderated by the complexity of the information security task. Finally, further research could also be expanded to consider how emotional aspects may influence ISP compliance intentions.

Acknowledgments

This work was partially supported by FCT, I. P., the Portuguese national funding agency for science, research, and technology, under project number UID/SOC/04521/2019.

References

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, *26*(4), 276-289.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411.

Aurigemma, S., & Leonard, L. (2015) The influence of employee affective organizational commitment on security policy attitudes and compliance intentions. *Journal of Information System Security, 11*(3), 201-222

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems, 5*(1), 2-9.

Bandura, A. (1977). Self-Efficacy: Toward a unifying theory of behavioral change. *Psychology Review, 84*, 191-215.

Bonias, D., Bartram, T., Leggat, S. G., & Stanton P. (2010). Does psychological empowerment mediate the relationship between high performance work systems and patient care quality in hospitals? *Asia Pacific Journal of Human Resources, 48*(3), 319-337.

Borkhataria, C. (2017). Ransomware is on the rise: New report warns black market behind distribution of malicious software is flourishing. *Dailymail.com.* https://www.dailymail.co.uk/sciencetech/article-5021559/The-black-market-economy-ransomware-flourishing.html

Boss, S. R., Kirsch, L., Shingler, I., & Boss, R. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Boulton, C. (2017). Humans are (still) the weakest cybersecurity link. *CIO*. https://www.cio.com/article/3191088/humans-are-still-the-weakest-cybersecurity-link.html

Bowen, D. E., & Lawler, E. E., III. (1992). The empowerment of service workers: What, why, how, and when. *Sloan Management Review, 33*(3), 31-39.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Byrne, B. M. (2016). *Structural equation modeling with AMOS: Basic concepts, applications, and programming*. Routledge.

Campbell, J. P., McCloy, R. A., Oppler, S. H., & Sager, C. E.. (1993). A theory of performance. In N. Schmitt & W. C. Borman (Eds.), *Personnel selection in organizations* (pp. 35-70). Jossey-Bass.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of Information Privacy and Security, 1*(3), 18-41.

Chen, G., & Klimoski, R. J. (2003). The impact of expectations on newcomer performance in teams as mediated by work characteristics, social exchanges, and empowerment. *Academy of Management Journal, 46*(5), 591-607.

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

CompTIA. (2015). *Trends in information security study*. *Comptia*. https://www.comptia.org/content/research/trends-in-information-security-study

Conger, J. A., & Kanungo, R. N. (1988). The empowerment process: Integrating theory and practice. *Academy of Management Review, 13*(3), 471-482.

Cotton, J. L., Vollrath, D. A., Froggatt, K. L., Lengnick-Hall, M. L., & Jennings, K. R. (1988). Employee participation: Diverse forms and different outcomes. *Academy of Management Review, 13*(1), 8-22.

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

Deci, E., & Ryan, R. M. (1985). *Intrinsic motivation and self-determination in human behavior*. Springer.

Deci, E. L., Koestner, R., & Ryan, R. M. (1999). A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. *Psychological Bulletin, 125*(6), 627.

Dhillon, G., (2001) Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, 20(2): p. 165-172.

Dhillon, G., Silva, L., & Backhouse, J. (2004). Computer crime at CEFORMA: a case study. *International Journal of Information Management, 24*(6).

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39-50.

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

Gist, M. E., & Mitchell, T. R. (1992). Self-efficacy: A theoretical analysis of its determinants and malleability. *Academy of Management Review, 17*(2), 183-211.

Groysberg, B., & Slind, M. (2012). Leadership is a conversation. *Harvard Business Review, 90*(6), 76-84.

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

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

Hackman, J. R., & Oldham, G. R. (1980). Work redesign (Vol. 72). Addison-Wesley.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2010). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ.

Heilmann, P., Forsten-Astikainen, R., & Kultalahti, S. (2018). Agile HRM Practices of SMEs. *Journal of Small Business Management* (early access).

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

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

Hoffman, G. M. (2001). *The technology payoff: How to profit with empowered workers in the information age*. iUniverse.

Hon, A. H., & Rensvold, R. B. (2006). An interactional perspective on perceived empowerment: The role of personal needs and task context. *The International Journal of Human Resource Management*, *17*(5), 959-982.

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: a multidisciplinary journal*, *6*(1), 1-55.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496.

Kanter, R. (1977). *Men and women of the corporation.* Basic Books.

Kanter, R. M. (1983). *The change masters: Binnovation and entrepreneturship in the American corporation*. Touchstone.

Ke, W., & Zhang, P. (2011). Effects of empowerment on performance in open-source software projects. *IEEE Transactions on Engineering Management*, *58*(2), 334-346.

Kline, R. B. (2011). *Principles and practice of structural equation modeling* (3rd ed.). Guilford.

Knoop, R. (1995). Influence of participative decision-making on job satisfaction and organizational commitment of school principals. *Psychological Reports*, *76*(2), 379-382.

Kraimer, M. L., Seibert, S. E., & Liden, R. C. (1999). Psychological empowerment as a multidimensional construct: A test of construct validity. *Educational and Psychological Measurement*, *59*(1), 127-142.

Laschinger, H. (1996). A theoretical approach to studying work empowerment in nursing: A review of studies testing Kanter's theory of structural power in organizations. *Nursing Administration Quarterly*, *20*(2), 25-41.

Laschinger, H., Finegan, J., Shamian, J., & Wilk, P (2001). Impact of structural and psychological empowerment on job strain in nursing work settings: Expanding Kanter's model. *Journal of Nursing Administration*, *31*(5), 260-272.

Lawler, E. E, III. (1986). *High-Involvement management. participative strategies for improving organizational performance*. ERIC.

Lawler, E. E., III. (1992). *The ultimate advantage*. Jossey-Bass.

Leach, J. (2003). Improving user security behaviour. *Computers and Security, 22*(8), 685-692.

Liao, H., Toya, K., Lepak, D. P., & Hong, Y. (2009). Do they see eye to eye? Management and employee perspectives of high-performance work systems and influence processes on service quality. *Journal of Applied Psychology, 94*(2), 371.

Logan, M. S., & Ganster, D. C. (2007). The effects of empowerment on attitudes and performance: The role of social support and empowerment beliefs. *Journal of Management Studies, 44*(8), 1523-1550.

Mann, I. (2017). *Hacking the human: Social engineering techniques and security countermeasures*. Routledge.

Manz, C. C., & Sims Jr, H. P. (1987). Leading workers to lead themselves: The external leadership of self-managing work teams. *Administrative Science Quarterly*, 106-129.

Maynard, M. T., Gilson, L. L., & Mathieu, J. E. (2012). Empowerment: Fad or fab? A multilevel review of the past two decades of research. *Journal of Management, 38*(4), 1231-1281.

McDonald, R. P., & Ho, M. H. R. (2002). Principles and practice in reporting structural equation analyses. *Psychological Methods, 7*(1), 64.

Nissenbaum, H. 1994. Computing and accountability. *Communications of the ACM, 37*(1), 73-80.

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). McGraw-Hill.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31*(5), 673-680.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Which factors explain employees' adherence to information security policies? an empirical study. *PACIS Proceedings*.

Perez, S. (2005). The case of a computer hack. *Journal of Information System Security, 1*(2), 53-63.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods, 40*(3), 879-891.

Puhakainen, P., & Siponen, M. (2010). Improving employee's compliance through IS security training: an action research study. *MIS Quarterly, 34*(4), 757-778.

Quinn, R. E., & Spreitzer, G. M. (1997). The road to empowerment: Seven questions every leader should consider. *Organizational Dynamics, 26*(2), 37-49.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.

Scandura, T. A., Graen, G. B., & Novak, M. A. (1986). When managers decide not to decide autocratically: An investigation of leader-member exchange and decision influence. *Journal of Applied Psychology, 71*(4), 579-584.

Seibert, S. E., Wang, G., & Courtright, S. H. (2011). Antecedents and consequences of psychological and team empowerment in organizations: A meta-analytic review. *Journal of Applied Psychology, 96*(5), 981-1003.

Shrout, P. E., & Bolger, N. (2002). Mediation in experimental and nonexperimental studies: new procedures and recommendations. *Psychological Methods, 7*(4), 422-445.

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

Sobel, M. E. (1982). Asymptotic confidence intervals for indirect effects in structural equation models. *Sociological methodology, 13*, 290-312.

Sobel, M. E. (1986). Some new results on indirect effects and their standard errors in covariance structure models. *Sociological Methodology, 16*, 159-186.

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

Spears, J., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*(3), 503-522.

Spreitzer, G. M. (1995a). An empirical test of a comprehensive model of intrapersonal empowerment in the workplace. *American journal of community psychology, 23*(5), 601-629.

Spreitzer, G. M. (1995b). Psychological empowerment in the workplace: Dimensions, measurement, and validation. *Academy of Management Journal*, *38*(5), 1442-1465.

Spreitzer, G. M. (1996). Social structural characteristics of psychological empowerment. *Academy of Management Journal*, *39*(2), 483-504.

Spreitzer, G. M. (2008). Taking stock: A review of more than twenty years of research on empowerment at work. *Handbook of Organizational Behavior, 1*, 54-72.

Spreitzer, G. M., et al. (1997). A dimensional analysis of the relationship between psychological empowerment and effectiveness satisfaction, and strain. *Journal of Management*, *23*(5), 679-704.

Sridhar, V., & Ahuja, D. K. (2007). Challenges in managing information security in academic institutions: case of MDI in India. *Journal of Information System Security*, *3*(3), 51-78

Stanton, J. M., & Weiss, E. M. (2000). Electronic monitoring in their own words: An exploratory study of employees' experiences with new types of surveillance. *Computers in Human Behavior, 16*(4), 423-440.

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

Thomas, K. W., & Velthouse, B. A. (1990). Cognitive elements of empowerment: An "interpretive" model of intrinsic task motivation. *Academy of Management Review, 15*(4), 666-681.

Thorlakson, A. J., & Murray, R. P. (1996). An empirical study of empowerment in the workplace. *Group & Organization Management*, *21*(1), 67-83.

Udeh, I. & Dhillon, G. (2008) An analysis of information security governance structures: The case of Société Générale Bank. *Proceedings of the Annual Symposium on Information Assurance*.

Wat, D., & Shaffer, M. A. (2005). Equity and relationship quality influences on organizational citizenship behaviors: The mediating role of trust in the supervisor and empowerment. *Personnel Review, 34*(4), 406-422.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 26*(6), 2799-2816.

Appendix

Table A1. Operationalization of Constructs

Variable	Item	Source
ISPC1	I intend to comply with the requirements of the ISP of my organization in the future.	Bulgurcu et al. (2010)
ISPC2	I intend to protect information and technology resources according to the requirements of the ISP of my organization in the future.	Bulgurcu et al. (2010)
ISPC3	I intend to carry out my responsibilities prescribed in the ISP of my organization when I use information and technology in the future.	Bulgurcu et al. (2010)
PACT1	My impact of what happens in my department related to information security is large.	Spreitzer (1995)
PACT2	I have a great deal of control over what happens in my department related to information security.	Spreitzer (1995)
PACT3	I have significant influence over what happens in my department related to information security.	Spreitzer (1995)
COMP1	I am confident about my ability to do my job of securing information and information systems.	Spreitzer (1995)
COMP2	I am self-assumed about my capabilities to perform my job of securing information and information systems activities.	Spreitzer (1995)
COMP3	I have mastered the skills necessary for my job of securing information and information systems.	Spreitzer (1995)
MEAN1	My work of securing information and information systems is very important to me.	Spreitzer (1995)
MEAN2	My work of securing information and information systems is personally meaningful to me.	Spreitzer (1995)
MEAN3	My work of securing information and information systems is meaningful to me.	Spreitzer (1995)
CHOI1	I have significant autonomy in determining how I do my job of securing information and information systems.	Spreitzer (1995)
CHOI2	I can decide on my own how to go about doing my job of securing information and information systems.	Spreitzer (1995)
CHOI3	I have considerable opportunity for independence and freedom in how I do my job of securing information and information systems.	Spreitzer (1995)
SETA1	My organization offers training to help employees improve their awareness of computer and information security issues.	D’Arcy et al. (2009)
SETA2	My organization provides employees with education on computer software copyright laws.	D’Arcy et al. (2009)
SETA3	In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.	D’Arcy et al. (2009)
SETA4	My organization educates employees about their computer security responsibilities.	D’Arcy et al. (2009)
SETA5	In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.	D’Arcy et al. (2009)

ACC1	I have access to the strategic information I need to do my job of securing information and information systems well.	Spreitzer (1996)
ACC2	I understand top management's information security vision for the organization.	Spreitzer (1996)
ACC3	I understand the information security strategies and goals of the organization.	Spreitzer (1996)
PART1	I actively participate in defining, reviewing, and approving any information security controls related to protecting the organization's information (e.g., access control, separation of duties, employee training on information security awareness, etc.)	Spears & Henri (2010)
PART2	In managing risk to information and information systems in my company, I actively contribute to decision-making for all risk management activities (e.g., documenting business processes or transactions for risk evaluation, ensuring key controls exit to mitigate specific types of risks, implementing control, etc.)	Spears & Henri (2010)

About the Authors

Gurpreet Dhillon is a professor and head of the Department of Information Systems and Supply Chain Management at the University of North Carolina Greensboro, He has a PhD in information systems from the London School of Economics, UK. He also has an MSc from the Department of Statistical and Mathematical Sciences at the London School of Economics and an MBA specializing in operations management. In 2019, he was honored with an honorary doctorate (PhD, *honoris causa*) from Örebro University, Sweden. His research interests include management of information security and the ethical and legal implications of information technology. His research has been published in journals including *Information Systems Research*, *European Journal of Information Systems*, *Information Systems Journal*, *Journal of Management Information Systems*, *Journal of Business Ethics*, among others. Gurpreet has authored several books including *Information Security: Text and Cases* (Prospect Press, 2018). He is also the editor in chief of *Journal of Information System Security*.

Yurita Yakimini Abdul Talib is a senior lecturer of accounting information systems at Tunku Puteri Intan Safinaz School of Accountancy, Universiti Utara Malaysia. She received her PhD in business information systems from Virginia Commonwealth University. Her research focuses on information systems security behavior, fraud in e-commerce and social commerce, and accounting information systems. She has published in various international conferences proceedings and refereed journals.

Winnie Ng Picoto is an associate professor of information systems and operations management at ISEG, Lisbon School of Economics & Management, at the University of Lisbon. She holds a BA in industrial engineering and management from the Instituto Superior Técnico, a MIS from ISEG and a PhD in management from the Technical University of Lisbon. She is a member of the Advance Research Center. Her previous work experience includes information systems consulting. Her current research interests include the use of innovative IS, IT value, big data and emerging technologies. Her work has been published in journals such as *European Journal of Information Systems*, *Journal of Business Research*, *Industrial Management and Data Systems*, and *Journal of Organizational Computing and Electronic Commerce*.