Employee ISP Compliance Intentions: An Empirical Test of Empowerment

Yurita Yakimin Abdul Talib
Universiti Utara Malaysia
School of Accountancy, College of Business, 06010 Sintok Kedah
Malaysia
yurita@uum.edu.my

Gurpreet Dhillon
Virginia Commonwealth University
School of Business, 301 W Main St.
Richmond 23284 VA
USA
gdhillon@vcu.edu

Abstract

Incidents of computer abuse, proprietary information leaks and other security lapses have been on an increase. Most often, such security lapses are attributed to internal employees in organizations subverting established organizational information security policy (ISP). As employee compliance with ISP is the key to escalating information security breaches, understanding employee motivation for following ISP is critical. Using the Thomas and Velthouse's (1990) intrinsic motivation model, we investigate the role of intrinsic motivation for ISP compliance. Through survey data collected from 289 participants, the study assesses how psychological empowerment, as derived from information security task, may impact the information security performance of the participants, which is measured by their compliance with ISP. The study demonstrates that the psychological empowerment has a positive impact on participants' ISP compliance intention. Furthermore, the psychological empowerment can be predicted by structural empowerment practices, particularly security education, training, and awareness (SETA), access to information security strategy and goals, and participation in information security decision-making. In addition, the psychological empowerment may act as a mediator for the relations between structural empowerment practices and participants' ISP compliance. Theoretical contributions, managerial implications, and directions for future research of this study are discussed.

Keywords: Information security, ISP compliance, intrinsic motivation, psychological empowerment, structural empowerment
Introduction

This study concerns employee Information Security Policy (ISP) compliance intentions in organizations. ISP compliance is the act or process of conformity to official requirements, including disposition to yield to others (Herath and Rao, 2009a; Bulgurcu et al., 2010). In other words, ISP compliance intentions reflect a person intention to perform IS security task activities as prescribed in the ISP while utilizing organization’s information systems in the course of performing one’s primary work tasks. Employee ISP compliance is important to ensure protection of organizational information assets (Hu et al., 2011). However, the expectations of an ISP do not necessarily translate into desirable security actions (Bulgurcu et al., 2010). For instance, a survey by Ponemon (2009) found that while more than 71% of respondents were aware of their organizational password sharing security policy, 47% admitted sharing passwords with coworkers. This type of disconnect between information security responsibilities and real-world practices poses a significant challenge for managing insider information security breaches. Given that information security lapses are attributed to employees in subverting established organizational ISP, it is therefore, essential for organizations to understand what factors motivate employees to perform the information security task stipulated in the ISP. Understanding of the factors that motivate employees to comply with their organization’s ISP would provide input to the management on how to improve to information security behavioral issues.

Empirical evidence indicates that employee compliance with organizational ISP may be influenced by extrinsic or/intrinsic factors (e.g., Boss et al., 2009; Herath and Rao, 2009b). While both extrinsic and intrinsic factors have been well-researched, this study aims to extend the knowledge about employee compliance with ISP by identifying intrinsic factors grounded in Thomas and Velthouse’s (1990) intrinsic motivation/empowerment model, which is psychological empowerment. Psychological empowerment reflects individuals’ assessment of their work task in term of competence, meaning, impact, and choice. One would expect factors intrinsic to the task itself to motivate and influence them to invest energy in the task and perform adequately (Thomas and Velthouse, 1990). Additionally, intrinsic motivation theorists have argued the need for drivers to enhance one’s intrinsic motivation (Hackman and Oldham, 1980; Thomas and Velthouse, 1990). While prior studies in IS security have suggested various antecedents to enhance employee intrinsic motivation to comply (Herath and Rao, 2009a; Bulgurcu et al., 2010; Son, 2011), they were not empirically tested. Call has been made for authors to empirically investigate the antecedents of intrinsic motivation of ISP compliance (Herath and Rao, 2009a; Son, 2011). Hence, our study adheres to the call and aims to fill the gap of prior research to investigate factors to drive employee psychological empowerment. We identify structural empowerment practices as antecedents of psychological empowerment. Structural empowerment reflects management practices to increase individuals’ level of power (Kanter, 1977). Studies have shown that structural empowerment practices are effective means to increase individuals’ psychological empowerment of their work task (Spreitzer, 1996; Kraimer et al., 1999).

In so doing, we address two research questions: (1) What is the impact of employee's psychological empowerment of information security task on ISP compliance intentions? (2) What is the role of structural empowerment practices, including information security education, training, and awareness (SETA), access to information regarding information security strategy and goals, and participation in information security decision-making, in shaping an employee’s perceptions about psychological empowerment of IS security task? We answer the research questions related to factors to motivate employees to comply with their organization’s ISP using data collected through a survey of 289 employees from various organizations in the US.

Literature Review

A person who feels the impetus or inspiration to act is considered motivated (Deci and Ryan, 2000). Ryan and Deci (2000), in their self-determination theory (SDT), organized the distinction of factors to motivate people to take action into two paradigms, extrinsic and intrinsic motivation. The term ‘extrinsic motivation’ (Ryan and Deci, 2000) refers to “doing something because it leads to a separable outcome” (p. 55). It relates to an individual’s belief that he/she will attain some separable outcome or instrumental value when carrying out specific activity.
One extrinsic motivational factor for IS security policy compliance, which has received a great deal of attention in the scientific literature is sanctions. A sanction is described as a negative stimulus or a negative incentive to discourage individuals from performing acts or taking decisions that are not aligned with organizational goals. Straub (1990) explained that the concept of sanction is derived from general deterrence theory (GDT) and is used by traditional disciplinary systems to intimidate employees. GDT has had significant influence amongst the IS security scholars (Straub, 1990; Siponen et al., 2007; Myyry et al., 2009; Bulgurcu et al., 2010; Chen et al., 2012). They found that sanctions had a significant impact on actual compliance with IS security policies. However, Son’s (2011) study showed that perceived certainty and severity of sanctions were not significantly related to ISP compliance intentions.

Information security literature has also focused on the role of reward. A reward is an element of positive control, which is implemented with the goal of encouraging conformity with the desired behaviors (Boss et al., 2009). In the information security setting, employees are encouraged to comply with ISP when they are sufficiently motivated to attain rewards and recognitions. Such ISP is not accorded much importance by employees in the absence of any reward for compliance (Boss et al., 2009). Studies found that rewards were positively correlated with ISP compliance (Stanton et al., 2005; Bulgurcu et al., 2010). However, contrary to the expectations, some studies found that reward was not significantly related to ISP compliance intentions (Boss et al., 2009; Pahnila et al., 2007).

While the information security literature has highlighted the effects of extrinsic factors (i.e., sanctions, rewards), employee motivation to perform IS security task as stipulated in the ISP may not necessarily be influenced only by those strategies. Employee intrinsic motivation to follow the requirements of ISP may provide an alternative explanation (Son, 2011). Intrinsic motivation has been summarized by Broedling (1977) as a “catchall explanation whenever behaviors occur which cannot be clearly linked to external outcomes” (p. 268). Intrinsic motivation is based on an assessment of how the task provides satisfaction or fulfillment of innate psychological needs or desires (Ryan and Deci, 2000). In other words, the reward is in the task activities itself (Deci and Ryan, 2009). We expect that similar motivations exist in employees with respect to their ISP compliance intentions.

An employee’s intention to perform information security task as postulated in the ISP is formed when the individual assesses the innate positive values he/she will obtain in completing or even working on the information security tasks. Information security researchers have incorporated feelings of competence (Chan et al., 2005; Workman et al., 2008; Herath and Rao, 2009b; Rhee et al., 2009) and feelings of contribution from one’s security actions (Herath and Rao, 2009a) in their models in recognizing the importance of intrinsic motivation in influencing employee ISP compliance. In our context, an employee intentions to perform the information security tasks prescribed in the ISP is formed when he assesses his personal experience of psychological empowerment in the IS security tasks, in term of perceived competence, meaning, impact, and choice. Hence, this study seeks to extend our understanding of the role of factors intrinsic to the information security tasks to influence employee’s intention to comply with ISP.

Finally, intrinsic motivation theorists postulate that although empowerment are innate feelings of individual regarding a specific task, factors external to the individuals may also be important to energize the feelings (Deci and Ryan, 1985; Conger and Kanungo, 1988; Thomas and Velthouse, 1990). Ryan and Deci (2000) called for additional research to investigate factors that enhance an individual intrinsic motivation. A few IS security studies (e.g., Herath and Rao, 2009a; Bulgurcu et al., 2010; Son, 2011) have highlighted the importance of various strategies, such as IS security training, IS security climate, and etc, to enhance employee intrinsic motivation. However, rather than exploring the range of strategies empirically, the studies simply acknowledged their importance in influencing employee intrinsic motivation. Prior studies show that structural empowerment practices were significantly related to psychological empowerment (Spreitzer, 1996; Siu et al., 2005; Seibert et al., 2011). Still, to the best of our knowledge, the association has never been tested in the context of information security. Hence, this study investigate the role of structural empowerment practices (information security education, training, and awareness [SETA]), access to information security strategy and goals, and participation in information security decision-making), and postulates that they are likely to influence an employee’s perceptions of psychological empowerment.
Theoretical Framework

This study seeks to understand the antecedents of an employee’s intention to comply with the ISP of their organization. Our effort to understand the factors that influence employee’s intention to comply based on the conceptual ideas of Thomas and Velthouse’s (1990) intrinsic motivation/empowerment model. We begin by adopting the underlying set of psychological empowerment beliefs—perceived competence, meaning, impact, and choice—in the information security context as antecedents of employee’s intention to comply. Then, we add to the model the structural empowerment practices, which are rooted in Kanter’s (1977) structural empowerment model, as antecedents to psychological empowerment.

Thomas and Velthouse’s (1990) Intrinsic Motivation/Empowerment Model

Thomas and Velthouse (1990) defined intrinsic motivation as “positively valued experiences that the individual derives directly from the task” or “those generic conditions by an individual, pertaining directly to the task, that produce motivation and satisfaction” (Thomas and Velthouse, 1990, p. 668). This indicates that a motivation to act occurs within a person and refers to the task itself. For intrinsically motivated individuals, they are seeking for fulfillment of their innate desires or needs, such as enjoyment, empowerment, and self-determination, derived from completing or even working on a task. According to the theory, individual determines how he/she will act by assessing the psychological empowerment he/she will experience or obtain from the task (Thomas and Velthouse, 1990). Psychological empowerment is formed based on individuals’ assessments of a task regarding four feelings: competence, meaning, impact, and choice (Thomas and Velthouse, 1990).

**Competence** refers to an assessment of one’s own capability to perform task activities skillfully (Thomas and Velthouse, 1990). Self-efficacy theory states that when a person has low self-efficacy regarding a particular skill to execute a specific task, he or she will avoid such a task where this skill is required (Bandura, 1977). **Meaning** refers to judgments of the value of task goals with individual’s own goals and standards (Thomas and Velthouse, 1990). The cognitive assessment of task meaningfulness relates to individuals’ belief concerning whether a given task is trivial or not. If a task is important or meaningful to individuals, they will invest their energy to accomplish the goal of the task (Thomas and Velthouse, 1990). In contrast, individuals who perceive that a task is meaningless tend to be apathetic and detached from the said task (Thomas and Velthouse, 1990).

**Impact** refers to judgments concerning how a behavior or an action regarding a task may make a significant difference to the organization in terms of accomplishing the goal of the task (Thomas and Velthouse, 1990). Thus, the cognitive assessment of impact relates to an individual’s belief regarding whether they can contribute to or influence the organization by performing or executing a specific task. If individuals are aware that the results of their action will benefit others, it encourages them to invest their time and energy to perform the task (Thomas and Velthouse, 1990). Finally, perceptions of **choice** means believing that one has control or discretion in initiating and regulating a specific task, and has the authority to make decisions related to the task. When individuals experience a sense of choice over their task, they feel personal responsibility concerning the outcomes of their task (Oldham and Hackman, 1980), hence they will put more effort in the task (Thomas and Velthouse, 1990).

Thomas and Velhouse’s (1990) intrinsic motivation model postulates that the level of psychological empowerment is likely to affect outcomes, such as active and concentration of energy upon task. Active and concentration of energy upon task can be described as putting more “effort” or “working hard” towards accomplishing the goals of the task (Thomas and Velthouse, 1990). This indicates that the stronger the cognitions of competence, meaning, impact, and choice deriving from a task, the greater the individuals’ motivation to invest more energy in behaviors towards achieving that task. Findings across a wide range of studies showed that psychological empowerment influences outcomes, including individual task performance, work effort, and task effectiveness (Spreitzer et al., 1997; Ke and Zhang, 2011; Campbell et al., 2003; Chen and Klimoski, 2003).
Empowerment and ISP Compliance Intentions

Kanter’s (1977) Structural Empowerment Theory

Structural empowerment refers to conditions or practices where an organization provides subordinates with an amount of power (Kanter, 1977). According to Kanter, power is derived from the structural conditions in an organization, not inherent from personality traits or effects of socialization. Thus, the focus of Kanter’s theory is on the employees’ perception of the work conditions, rather than the individuals, which determine what happened. Kanter (1977) discussed several practices that indicate structural empowerment, including: (1) access to opportunity, (2) access to information, and (3) participation in decision-making. First, access to opportunity relates to job or task conditions that provide individuals with chances for growth and development within the organization, as well as chances to develop their skills, abilities, and knowledge. Access to opportunity allows an individual to learn about skills and the economies of the larger organization (Lawler, 1986). Lanchshinger (1996) defined access to opportunity as opportunities for growth and movement within an organization as well as opportunities to enhance and develop one’s knowledge and skills. This could be achieved through training and education programs.

Second, Kanter (1977) posited that access to information refers to ability to obtain knowledge and information necessary to carry out an individual’s task as well as information concerning what is going on in the larger organization. Lanchshinger (1996) referred to access to information as having information regarding organizational goals and policy changes. More specifically, previous researchers have focused on information regarding the mission and future direction of the organization (Lawler, 1992; Spreitzer, 1995b, 1996; Bordin et al., 2006). Access to information related to goals and strategic directions allows an individual to see the “big picture”, which creates an understanding on how his or her work contributes to the firm’s goals (Bowen and Lawler, 1992). Thus, such an individual will be able to make better decisions related to his/her task.

Third, Kanter’s (1977) theory also suggests an empowerment through participation. This indicates that employees are able to provide inputs and influence over decisions. Inputs in this context consist of strategic and day-to-day operational decisions related to their job or task. Knoop (1995) stated that participation is the act of sharing decision-making with others to achieve organizational goals. As employees are at the operational level, they know better how specific actions related to their job or task affect the organization. Employees are also more likely to offer valuable ideas on how operations may be improved. Subsequently, their meaningful suggestions are more likely to be accepted and adopted.

Research Model and Hypotheses

Figure 1 depicts our research model. We develop our research model by identifying key constructs for the two theories: Thomas and Velthouse’s (1990) intrinsic motivation model and Kanter’s (1977) structural empowerment theory. There is one dependent variable of interest, ISP compliance intentions.

Psychological empowerment and ISP compliance intentions

Intrinsic motivation/empowerment theory purports that individuals appear to evaluate the information regarding their competence of a specific task, the value of a task goal or purpose in relation to their own ideals and standards, their impact or their ability to make a significant difference or contribute to an organization, and their freedom or self-determination in a specific task (Thomas and Velthouse, 1990). Thomas and Velthouse (1990) argue that psychological empowerment is likely to affect outcomes, such as active and concentration of energy upon task. Active and concentration of energy upon task can be described as putting more “effort” or “working hard” towards accomplishing the goals of the task (Thomas and Velthouse, 1990).
Prior research suggests that individuals’ level of psychological empowerment is associated with various outcomes, including individual task performance, work effort, and task or work effectiveness (Spreitzer et al., 1997; Ke and Zhang, 2011; Campbell et al., 2003; Chen and Klimoski, 2003). There is extensive research linking competence or self-efficacy on task-related behaviors and actual performance (e.g., Stajkovic and Luthans, 1996; Hsu and Chiu, 2004; Ke and Zhang, 2011). For instance, studies found that perceptions of competence of IT provide motivation for employees to engage in IT usage (Hsu and Chiu, 2004; Ke and Zhang, 2011). These findings suggest that an individual who has confidence in their capabilities to undertake a task is more likely to take the required associated actions. Impact of a task has also been found to be associated with task engagement, as well as performing well with the task (e.g., Spreitzer et al., 1997; Kraimer et al., 1999; Wang and Lee, 2009; Liao et al., 2009; Herath and Rao, 2009; Agarwal and Anderson, 2010). For example, Spreitzer et al. (1997) found that perceived impact significantly related to work effectiveness, which is the degree to which individuals fulfill or exceed work expectation. These results indicate that empowered individuals who see themselves as able to influence the work processes and competent in their work, are more motivated to invest their energy in the job and perform effectively (Spreitzer et al., 1997).

Meaning is found to be associated with courtesy behavior, higher commitment to work, engagement at work, and work performance (e.g., Liden et al., 2000; Wat and Shaffer, 2005; Wang and Lee, 2009; May et al., 2004). For instance, feelings of meaningfulness of a given work activity have been positively linked to employee engagement in the associated work activities (May et al., 2004). A study by Wang and Lee (2009) found an increased propensity to commit to work when said work was perceived as personally meaningful. Empowered employees who believe that the work activities are personally meaningful were willing to invest themselves more fully in the associated activities. Choice or self-determination has been found to result in individual’s identification with and involvement in a particular organization (Kraimer et al., 1999). This indicates that employees who experience a high degree of discretion in carrying out their task feel a personal responsibility towards the outcomes of the task. Consequently, they put more effort to improve the performance of the task.

Thomas and Velthouse’s (1990) notion of psychological empowerment (i.e., feelings of competence, meaning, impact, and choice) of a task can be extended to information security context for two reasons. First, tasks in information security are similar to job tasks in organizations, which has activities and goals (Thomas and Velthouse, 1990). IS security task consists of activities such as appropriate selection of a password, updating of anti-virus software, backing up of data, checking for encryptions, not sharing the

---

**Figure 1 - Research Framework**
Empowerment and ISP Compliance Intentions

Thirty Sixth International Conference of Information Systems, Fort Worth 2015

computer with others, etc. (Stanton et al., 2005; Albrechtsen, 2007; Dhillon, 2007; Herath and Rao, 2009a). These activities protect the organization’s information with the goals of ensuring the confidentiality, integrity, and availability of the information (Loch et al., 1992). Second, similar to other job tasks (e.g., payroll, teaching students, serving customers, and so on) information security task is important to organizations. In order for employees to create value for their organization, they must complete the information security task. For instance, employees that create a strong password help to protect their organization from security threats and vulnerabilities. It is through exerting effort on information security task (e.g., complying with the ISP) that employees contribute to the organization and other stakeholders.

Drawing from the intrinsic motivation/empowerment theory (Thomas and Velthouse, 1990), we define psychological empowerment as individuals’ belief regarding their competence to carry out the information security task, individuals’ belief of meaningfulness of the information security task, individuals’ belief of the impact of their information security task, and individuals’ belief of the freedom in the information security task. Consistent with the theory and previous studies, we postulate that psychological empowerment derived or experience from the information security task is the determinants of one’s intention to initiate security actions (i.e., ISP compliance intentions). This prediction is formally recognized in the following hypothesis:

**H₁:** Perceived psychological empowerment of information security tasks positively affects one’s intention to comply with the requirements of the ISP

Theory and literature have acknowledged that an individual’s work environment may influence his or her perceptions of psychological empowerment (Hackman and Oldham, 1980; Thomas and Velthouse, 1990; Spreitzer, 1995a). Thomas and Velthouse (1990) contend that an individual’s work environment is an important factor that can influence his or her level of psychological empowerment. They note, “Judgments regarding the task assessments (and thus empowerment) are shaped in part by “objective” variables in the individual’s environment”. Support for this notion can also be found in Spreitzer (1995a; 1996), Kraimer et al. (1999), and Carless (2004). Overall, the literature suggests that the work environment influences psychological empowerment.

Specifically, this current study focuses on work environment that foster empowerment, based on Kanter’s (1977) structural empowerment theory. The work environment (or social-structural) perspective of empowerment focuses on idea of sharing of power with all employees in the organization (Spreitzer, 2007). When management transfers power to subordinates, feelings of empowerment should follow (Spreitzer, 1996). Based on Kanter’s (1977) work on structural empowerment, three social-structural empowerment factors were investigated; (a) security education, training and awareness (SETA) programs, (b) access to information about the strategy and goals of organizational information security, and (c) participation in information security decision-making.

**SETA and Psychological Empowerment**

An important part of the social-structural empowerment is access to opportunity for growth and development within the organization, as well as chances to develop knowledge, skills, and abilities (KSAs), obtained through training and education programs. Theory and empirical studies suggest that educational efforts contribute to individuals’ intrinsic motivation in terms of increasing their belief in their capability to perform task activities skillfully (Hackman and Oldham, 1980; Thomas and Velthouse, 1990; Spreitzer et al., 2007). In a meta-analysis study, Seibert et al. (2011) examined the impact of training on perceived competence. The authors concluded that employees’ feelings of competence in work roles were reflected by enhanced knowledge, skills, and abilities resulting from the training programs. Thus, we contend that SETA programs will significantly and positively influence employees’ feeling of empowerment, specifically the competence dimension.

SETA programs focus on providing users with general knowledge of IS security environment, along with the skills necessary to perform the required IS security tasks (Whitman et al., 2001; Lee and Lee, 2002; c.f. D’Acrey et al., 2009). Bandura (1997) proposed that self-efficacy beliefs are developed through enactive
mastery experiences, vicarious experiences, and verbal persuasion. Through SETA individuals gather personal mastery of IS security via hands-on exercises and activities of IS security or regular demonstration of IS security issues and respective countermeasures. Further, SETA provides opportunities to observe the successes and failures of other IS security behaviors. Consequently, this information provides a guideline to employees against which they compare their own self-efficacy (Gist et al., 1989). In addition, verbal persuasion is regularly delivered in a SETA program. Individuals receive suggestions from instructors that encourage and support their IS security skills and foster a responsible development. Thus, it is expected that psychological empowerment (i.e., competence) in IS security may be developed through the ongoing acquisition of knowledge related to IS security, such as knowledge about IS security issues, the consequences, the controls to cope with the issues, and how to take action when such issues occur through SETA. This leads to the following hypothesis:

**H₂:** There is a positive direct relation between SETA programs and employees’ psychological empowerment.

### Access to Information Security Strategic Goals and Psychological Empowerment

Another important part of social-structural empowerment is access to information. Hoffman (1994), in the context of emerging information technology (IT), stated that, “to support worker empowerment throughout our 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, 1994, p. 55). Information might include data about a firm’s strategy and goals (Lawler, 1992; Spreitzer, 1996). Access to information about organizational goals helps employees in perceiving that his or her task as meaningful and important (Conger and Kanungo, 1988; Liao et al, 2009). Information about a strategy or operational goals allows employees to see their work as personally meaningful because they understand how it fits into their organization’s 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 creates and understanding on how one’s work can contribute to organizational goals (Bowen and Lawler, 1992).

In addition, access to information is associated with an individual’s feelings of empowerment in term of increases his or her ability and capability to make decisions in aligned with the goals (Lawler, 1992). Spreitzer (1996) showed that providing access to information about the strategy and goals of an organization enhances employee knowledge about the direction of the organization. As a result, employees felt empowered as it increases their confident in how their work roles can contribute to these goals. In support of this, a meta-analysis by Seibert et al. (2011) concluded that there was a significant relation between high performance work system (HPWS), including sharing of information about organizational strategy and goals and the four dimensions of psychological empowerment (i.e., competence, meaning, impact, and choice).

Accordingly, in the context of this study, 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 the organization’s information security strategic information, objectives, and goals. This could be accomplished by communicating a IS security policy that consists of the goals regarding information security (Straub, 1990; Boss et al., 2009). Access to information regarding security strategies and goals should allow individuals to feel informed about where an organization is headed in the context of information security. When employees understand the direction in which the organization is heading, they tend to be more aware about how their own information security task contributes to achieving the stated information security goals. That is, employees acquire a greater sense that the information security task is meaningful and serve a purpose, and enhances their ability to make decisions in aligned with the goals. Thus, access to an organization’s information security strategies and goals is expected to correlate with employees’ psychological empowerment. This leads to the following hypothesis:

**H₃:** There is a positive direct relation between access to information regarding information security strategies and goals, and employees’ psychological empowerment.
Participation in Security Decision-Making & Psychological Empowerment

Participation in decision-making refers to the act of sharing decision-making with others to achieve organizational goals (Knoop, 1995). Thus, participation in decision-making indicates that employees at all levels are able to provide input and influence over decisions related to a specific task or job (Cotton et al., 1988). In the context of IS security, participation relates to an individual’s involvement in the IS security decision-making process. Spears and Barki (2010) defined participation in security risk management (SRM) as a set of activities assigned to individuals during risk assessment, design, and implementation of IS security controls. Participation in IS security decision-making should allow individuals to contribute their inputs and thoughts pertinent to the IS security in order to achieve the organizational IS security goals. Fostering participation in decision-making in turn strengthens the motivation of employees to engage in IS security-related behaviors by providing them with the opportunity to attain intrinsic rewards from their work, including a greater experience of self-determination, meaningfulness, and impact (Scandura et al., 1986; Manz and Sims Jr, 1987; Lawler, 1992; Spreitzer, 1996).

When employees are involved in decision-making processes related to IS security tasks, they have the opportunity to contribute their inputs, such as ideas and thoughts, to accomplish the goals of the IS security policy. Thus, participation allows employees to feel that they have the opportunity for freedom and independence for IS security task-related decisions. Participation is an influential source of self-determination because it provides evidence that one’s inputs, thoughts, contribution, and activities related to their job matter (Lawler, 1992; Spreitzer, 1996). In a case study setting in IS security, Dhillon et al. (2004) found that most employees in an organization did not feel a sense of freedom because they were left out from all major decision-making and had no say on the latest developments related to IS security in the organization.

In addition, greater participation might be the impetus to enhance individuals’ feeling of impact (Seibert et al., 2011). When employees participate in the decision-making process related to their IS security task, they have the opportunity to set decisions jointly with the superiors. This likely influences the extent to which employees feel that they can impact their work environment. Spreitzer (1996) provided empirical evidence of the relations between participation in decision-making and perceived impact. The study concluded that participation signals to the employees that they are an important asset of the organization and that they can impact, or make a significant difference to the organization (Spreitzer, 1996). Further, when employees are allowed to participate in the decision-making process related to their IS security task, they have the opportunity to provide input that is consistent with their own values or needs. That is, the information security task is shaped by their own values and needs. Because of this, they are more likely to perceive that the information security task is meaningful and important. Hon and Rensvold (2006) has provided evidence showing that participation was strongly related to meaning of a task. Collectively, it is thus expected that if employees involved in decision-making processes related to the IS security tasks, they have opportunities to contribute their input to accomplish the IS security objectives and affect the work environment. Consequently, their perceptions of meaning, impact, and choice of the information security task should be higher. Hence, we predict that participation in decision-making processes related to information security will be associated with employees’ psychological empowerment. This predicted effect is formally recognized in the following hypotheses:

\[ H_4: \text{There is a positive direct relation between participation in information security decision-making and employees’ psychological empowerment.} \]

The concept of psychological empowerment serving as mediator between structural empowerment and individual performance-related outcomes has been repeatedly supported in numerous studies (e.g., Spreitzer, 2007; Maynard et al., 2012). Spreitzer (1995b) found that psychological empowerment partially mediated the relation between social structural and innovative behavior. In addition, Liao et al. (2009) found that cognitions of empowerment fully mediate the relations between a HPWS and service performance. Further, Laschinger et al. (2001) found that psychological empowerment mediates the relations between structural empowerment and individual satisfaction. Based on our argument underlying \( H_2, H_3, \) and \( H_4 \), that social-structural empowerment conditions increases psychological empowerment, and the literature supporting a relation between psychological empowerment and
individual behaviors, as discussed earlier, we also predict that the structural empowerment practices (i.e., SETA, access to information regarding information security strategies and goals, and participation in decision-making processes related to information security) will be indirectly associated with ISP compliance intentions.

H5a: The relation between SETA and employees’ intention to comply with ISP is mediated by psychological empowerment.

H5b: The relation between access to information security strategies and goals and employees’ intention to comply with ISP is mediated by psychological empowerment.

H5c: The relation between participation in information security decision-making and employees’ intention to comply with ISP is mediated by psychological empowerment.

Research Method

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 relations between individuals’ perception of psychological empowerment related to their information security task and ISP compliance intentions at the workplace, employees in different jobs and levels were thought to be appropriate. Potential employees who were targeted for this study were drawn from MBA, Executive MBA, and Executive MIS students enrolled in two public universities in the US. A self-administered survey instrument and a cover letter explaining the purpose of the study, the information about voluntariness, confidentiality, and anonymity was distributed (in class and/or via email) to 410 respondents in the sample. Of the 410 instruments distributed, 326 complete responses (79.5%) were returned within five months. Thirty-six of them met the exclusion criteria questions, hence, excluded from the study. This resulted in a final sample size of 290 responses with potentially useable data. Assessment of missing data identified that one case has an excessive number of missing values (40%), hence, deleted from further analysis.

Measurement of Variables

The constructs of this study were measured using multi-items scale adapted from previously validated studies. All measures used seven-point Likert-type scales with anchors ranging from 1 (strongly disagree) to 7 (strongly agree). The survey instrument was pilot tested on eight management and information systems academics, and they were generally satisfied with the clarity and wording of the questions. The measures for each constructs and the results are discussed below.

Three items were used from Bulgurcu et al. (2010) to measure ISP compliance intentions. For instance, respondents were asked how much do they agree or disagree with statements, such as “I intend to comply with the requirements of the IS security policy of my organization,” and “I intend to protect information and technology resources according to the requirements of the IS security policy of my organization.” The measure had an acceptable level of internal consistency ($\alpha = .75$).

Psychological empowerment is a four-dimensional construct (Spreitzer, 1995a). In order to assess the appropriateness of representing the individual dimensions instead of a single, global psychological empowerment construct, confirmation factor analysis (CFAs) were performed. The CFAs shown that the hypothesized four-factor model ($\chi^2 = 91.45$ with $df = 48$; RMSEA = .056; SRMR = .047; CFI = .98; NFI = .96) fit the data better than a model with one construct ($\chi^2 = 111.85$ with $df = 50$; RMSEA = .066; SRMR = .075; CFI = .97; NFI = .95). These results are consistent with previous research that showed that the four dimensions of psychological empowerment are distinct (e.g. Spreitzer et al., 1997; Kraimer et al., 1999). Consistent with this, we used separate scales to measure each dimension of psychological empowerment. The scales were adapted from Spreitzer (1995a).
Three items were used to measure perceived competence. Respondents were asked how much do 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 has a high level of internal consistency reliability ($\alpha = .89$). A perception of meaning was measured using three items. 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.” The scale had a high level of internal consistency reliability ($\alpha = .91$). Perceived impact from the employees’ perspective was measured using three items such as “my impact of what happens in my department related to IS security is large”. The scale had a high level of internal consistency ($\alpha = .90$). Finally, perceived choice was measured using three items, such as “I have significant autonomy in determining how I do my job of securing information and information systems”. The scale had an acceptable level of internal consistency ($\alpha = .78$).

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 IS 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 ($\alpha = .88$). Access to information security strategy and goals was measured using three items adapted from Spreitzer (1995a) such as “I have access to the strategic information I need to do my job of securing information and information systems well”. The scale showed an acceptable level of internal consistency ($\alpha = .76$). 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 agree or disagree with statements, including “I actively participate in defining, reviewing or approving any IS security controls related to protecting the organization’s information”. The scale had an acceptable level of reliability ($\alpha = .78$).

Results

We analyzed the data gathered using the covariance approach to structural equation modeling (SEM), with AMOS version 18. SEM, a multivariate statistical technique, is a powerful quantitative data analytical tool that enables researchers to observe the structural element (path model) and measurement element (factor model) simultaneously (Gefen et al., 2000). Nunnally (1978) suggested that in SEM estimation, a good rule is to have at least ten times as many subjects as variables. In our model, we have 25 indicators, which implies a minimum sample size of 250. Our sample size of 289 is, therefore, is adequate for modeling. Anderson and Gerbing’s (1988) two-step approach, in which the measurement model was assessed and improved prior to testing of the structural model, was used.

Discussion of the Measurement Model

The measurement model estimates the relations 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.

Individual item reliability is assessed by examining the factor loading of each item to its related construct. At a minimum, all the factor loadings must be statistically significant ($p < .05$). A good rule of thumb is that the standardized loading estimates should be 0.5 or higher (Hair et al., 2010). In our measurement model, all items loaded significantly ($p < 0.05$, two-tailed) to the respective constructs (Table 1). Nunnally (1978) suggests that composite reliability should be 0.7 or higher for a construct to demonstrate adequate composite reliability. As shown in Table 2, the composite reliability for all the constructs in our model ranges from 0.76 to 0.91, indicating adequate composite reliability.
### Table 1 – Reliabilities

<table>
<thead>
<tr>
<th>Latent Variable</th>
<th>Mean</th>
<th>SD</th>
<th>Loadings</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISP Compliance Intentions (Composite Reliability = 0.76)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISPC1</td>
<td>6.24</td>
<td>1.13</td>
<td>0.61</td>
</tr>
<tr>
<td>ISPC2</td>
<td>5.71</td>
<td>1.28</td>
<td>0.85</td>
</tr>
<tr>
<td>ISPC3</td>
<td>5.48</td>
<td>1.41</td>
<td>0.69</td>
</tr>
<tr>
<td>Security Education, Training, and Awareness (Composite Reliability = 0.87)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SETA1</td>
<td>4.46</td>
<td>2.04</td>
<td>0.84</td>
</tr>
<tr>
<td>SETA2</td>
<td>3.37</td>
<td>2.08</td>
<td>0.62</td>
</tr>
<tr>
<td>SETA3</td>
<td>4.44</td>
<td>2.03</td>
<td>0.74</td>
</tr>
<tr>
<td>SETA4</td>
<td>4.75</td>
<td>1.97</td>
<td>0.91</td>
</tr>
<tr>
<td>SETA5</td>
<td>4.62</td>
<td>2.00</td>
<td>0.78</td>
</tr>
<tr>
<td>Access to Information Security Strategies and Goal (Composite Reliability = 0.76)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACC1</td>
<td>4.49</td>
<td>1.84</td>
<td>0.74</td>
</tr>
<tr>
<td>ACC2</td>
<td>4.81</td>
<td>1.65</td>
<td>0.66</td>
</tr>
<tr>
<td>ACC3</td>
<td>5.03</td>
<td>1.58</td>
<td>0.74</td>
</tr>
<tr>
<td>Participation in Information Security Decision-Making (Composite Reliability = 0.78)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PART1</td>
<td>3.98</td>
<td>1.08</td>
<td>0.81</td>
</tr>
<tr>
<td>PART2</td>
<td>3.56</td>
<td>2.11</td>
<td>0.79</td>
</tr>
<tr>
<td>Impact (Composite Reliability = 0.90)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PACT1</td>
<td>4.69</td>
<td>1.79</td>
<td>0.83</td>
</tr>
<tr>
<td>PACT2</td>
<td>4.30</td>
<td>1.93</td>
<td>0.9</td>
</tr>
<tr>
<td>PACT3</td>
<td>4.43</td>
<td>1.97</td>
<td>0.86</td>
</tr>
<tr>
<td>Competence (Composite Reliability = 0.89)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COMP1</td>
<td>5.08</td>
<td>1.43</td>
<td>0.89</td>
</tr>
<tr>
<td>COMP2</td>
<td>5.08</td>
<td>1.34</td>
<td>0.81</td>
</tr>
<tr>
<td>COMP3</td>
<td>4.79</td>
<td>1.46</td>
<td>0.87</td>
</tr>
<tr>
<td>Meaning (Composite Reliability = 0.91)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEAN1</td>
<td>5.09</td>
<td>1.76</td>
<td>0.88</td>
</tr>
<tr>
<td>MEAN2</td>
<td>4.94</td>
<td>1.76</td>
<td>0.87</td>
</tr>
<tr>
<td>MEAN3</td>
<td>4.98</td>
<td>1.69</td>
<td>0.89</td>
</tr>
<tr>
<td>Choice (Composite Reliability = 0.80)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHOL1</td>
<td>4.44</td>
<td>1.78</td>
<td>0.87</td>
</tr>
<tr>
<td>CHOL2</td>
<td>4.24</td>
<td>1.76</td>
<td>0.53</td>
</tr>
<tr>
<td>CHOL3</td>
<td>4.49</td>
<td>1.84</td>
<td>0.84</td>
</tr>
</tbody>
</table>

The convergent and discriminant validities are summarized in Table 2. Convergent validity measures the extent to which items for each construct are related to each other, assessed by average variance extracted (AVE). AVE measure of 0.5 or higher demonstrates adequate convergent validity (Hair et al., 2010). The AVEs for all the constructs in our model were above the cut-off value, indicating adequate convergent validity. Finally, to confirm the discriminant validity of the constructs, the square root of the AVEs for each construct were compared to the correlations of the constructs with their latent variables (Fornell and Larcker, 1981). The square root of the AVEs for all constructs, reported in the diagonal of the correlation matrix, were larger than the corresponding off-diagonal correlations, which provide evidence of adequate discriminant validity. The above analyses and evaluations indicate that our measurement model is satisfactorily reliable and valid.
Further, we assessed for overall measurement model fit. Table 3 presents the values of the fit indices for the measurement model of this study. The overall measurement model fit was $\chi^2=484.45$ (df=247, $p<.001$), SRMR=.063, RMSEA .058 with CI90: (.05, .065), and CFI=.94. The results reported that the values of SRMR and RMSEA are less than the selected cut-off values of .08 (Hu and Bentley, 1999; Byrne, 2009; Kline, 2011) corresponds to an “acceptable” fit (McDonald and Ho, 2002). Further, the value of CFI is marginally lower than the cut-off of .95 (Hu and Bentley, 1999; Klein, 2011). However, many researchers use a cut-off value of .90 as acceptable fit (McDonald and Ho, 2002). Thus, overall, the results signify a reasonably good fit for our measurement model.

### Table 3 - Measurement Model Fit

<table>
<thead>
<tr>
<th>Fit Measures</th>
<th>RMSEA</th>
<th>SRMR</th>
<th>CFI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measurement Model</td>
<td>0.058</td>
<td>0.063</td>
<td>0.943</td>
</tr>
</tbody>
</table>

Common Method Variance (CMV)

Given that self-report data was collected in this study, the possibility of CMV was present. Harman’s one-factor test was conducted to assess whether CMV is present (Podsakoff and Organ, 1986). In conducting the Harman’s single-factor test, all items were entered into factor analysis using principal axis factoring with varimax rotation. Results showed the presence of six distinct factors with eigenvalues greater than 1.0. These six factors together accounted for 70.3% of the total variance and the largest factor did not account for the majority of the variance (i.e., 32.0%), indicating that CMV should not pose a pervasive issue (Podsakoff et al., 2003).

Discussion of the Structural Model

The purpose of structural model validity is to test the hypothesized relations from one construct to another, as proposed in our model. We used the covariance approach wherein the estimated covariance matrix was compared with the observed covariance matrix. The overall fit indices of the proposed structural model are presented in Table 4. The fit statistics confirmed that the model provides a good fit to the data (e.g., SRMR=.089, RMSEA .072 with CI90: (.065, 0.078), and CFI=.91; Hu & Bentler, 1999; Klein, 2011).

### Table 4 - Structural Model Fit

<table>
<thead>
<tr>
<th>Fit Measures</th>
<th>RMSEA</th>
<th>SRMR</th>
<th>CFI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structural Model</td>
<td>0.072</td>
<td>0.089</td>
<td>0.91</td>
</tr>
</tbody>
</table>

Cl$_{90}$ (.065, 0.079)
Empowerment and ISP Compliance Intentions

Figure 2 provides the standardized path loadings, all of which were significant at $p<.001$. Hypothesis 1 stated that feelings of psychological empowerment of information security task positively relate to ISP compliance intentions, and the findings supported the hypothesis ($\beta = .66$, $p<.001$). This result suggests that a high degree of psychological empowerment tends to increase one’s intentions to comply with organizational IS security policy. 44% of the variance in ISP compliance intentions can be explained by psychological empowerment. Hypothesis 2 stated that SETA positively relates to psychological empowerment. The results show that SETA was positively related to psychological empowerment ($\beta = .23$, $p<.01$).

Figure 2 - Path Diagram with Standardized Results

Hypothesis 3 stated that access to information security strategy and goals positively relates to psychological empowerment. The result shows that access to IS security strategy and goals predicted psychological empowerment ($\beta = .41$, $p<.01$). Hypothesis 4 stated that participation in IS security decision-making is associated with perceptions of psychological empowerment. The results indicate that participation in information security decision-making was significantly related to empowerment ($\beta = .40$, $p<.01$). Overall, all structural empowerment facets were related to psychological empowerment as hypothesized. SETA, access to information security strategy and goals, and participation in IS security decision-making explained 71% the variance of psychological empowerment.

For Hypotheses 5a – 5c we tested mediation with product-of-coefficients test by Sobel (1982), and the bootstrapping method (Shrout and Bolger, 1992), using the SPSS macro from Preacher and Hayes (2008). Table 5 displays the three hypotheses for mediating effects. Hypothesis 5a predicted that SETA was related to ISP compliance intentions via psychological empowerment. The indirect effect ($\beta_{IND}$) was .157. Using the Sobel test, the indirect effect of SETA was statistically significant ($z=2.151$, $SE=.007$, $p <.001$). Also, the bootstrap analysis supported the conclusion of mediation (the 95% bias-corrected confidence interval for the total indirect effect excluded zero ([.02, .305]) (Preacher and Hayes, 2008). Thus, psychological empowerment did mediate the relations between SETA and ISP compliance intentions, providing support for Hypothesis 5a.

Hypothesis 5b stated the effect from access to information security strategy and goals to ISP compliance intentions will be mediated by psychological empowerment. Notably, the indirect effect ($\beta_{IND}$) was .272. The results of the Sobel test ($z=3.09$, $SE=.088$, $p <.001$), and the bootstrap analysis (the 95% bias-corrected confidence interval for the total indirect effect excluded zero ([.125, .476])) support a conclusion of mediation. As a result, the findings indicated that the psychological empowerment mediated the
relations between access to information security strategy and goals, and ISP compliance intentions. Hypothesis 5b was thus supported.

Finally, Hypothesis 5c proposed that psychological empowerment act as a mediator of the relation between participation in information security decision-making and ISP compliance intentions. The indirect effect ($\beta_{IND}$) was .261. The Sobel test suggested that the indirect effect is statistically significant ($z=4.764$, $SE=.055$, $p < .001$). The bootstrap analysis supported the conclusion of mediation as well. The results show that the 95% bias-corrected confidence interval for the total indirect effect excluded zero ([$.146$, $.364$]). Thus, the results suggest that psychological empowerment mediated the relations between participation in information security decision-making and ISP compliance intentions, supporting for Hypothesis 5c.

![Table 5 - Result of Mediation](image)

**Discussion and Conclusion**

Our findings have a number of theoretical implications. First, while prior literature in information security has investigated the extrinsic motivational factors, our study takes a different perspective and explores the intrinsic motive to comply with organizational ISP. Perhaps this is a first study investigating effects of psychological empowerment derived from information security task. Experienced psychological empowerment from the task in term of feelings of competence, meaning, impact, and choice, increases employees’ motivation to expend effort to execute and to perform their information security task, as postulated in the ISP. Such an investigation extends the use of Thomas and Velthouse’s (1990) intrinsic motivation model into a very specific task in a different domain. Our findings are consistent with Thomas and Velthouse’s (1990) model, which argues for the importance of psychological empowerment derived from a task, and how such perceptions then impact on individuals’ task effort and performance.

Second, researchers in information security have made several suggestions of work practices to employees employees’ intrinsic motivation (e.g., Herath and Rao, 2009b; Bulgurcu et al., 2010; Son, 2011), yet this is the first attempt to investigate the association empirically. This study used the variables from Kanter’s (1977) structural empowerment theory, including training, access to information, and participation, as antecedents of the intrinsic motivation. Although the variables are not new in information security literature, they are used in this study to predict psychological empowerment, and ultimately to influence information security behavior. Unlike other studies (e.g., D’Arcy et al., 2009; Spears and Barki, 2010) the variables were used to predict the direct association with information security behaviors. We found that SETA, access to information security strategy and goals, and participation in information security decision-making influenced employees’ perceptions of psychological empowerment. Through an increased feeling of empowerment indirectly related to their compliance intentions. The results of this
study are able to show that structural empowerment practices can contribute to improve information security behaviors via psychological empowerment.

Our study also has practical implications. The results of the present study suggest that employees do have intrinsic needs, such as a need of feeling in control of their task. When employees’ intrinsic needs are met, for instance in our study, they experience that their information security task is psychologically empowering, it increases their motivation to expend more efforts towards accomplishing the goal of the task. As such, organizations should note that in order to encourage employees to take security actions, they should find ways or strategies to provide intrinsically motivating workplace.

Our study offers important strategies for organizations to increase employees’ intrinsic motivation, hence their ISP compliance intentions. Rather than providing a controlling work structure (i.e., rewards, penalties, and social pressures) to encourage the employees security compliance behaviors, organizations may actually change to empowering work structure. Our findings demonstrate that providing structural empowerment practices are important given their effect on employees’ psychological empowerment. The practices include enhancing employees’ knowledge and skills through training and education related to the information security, providing them access to information security strategy and goals, and involving them in decision-making processes related to information security. Not only that these strategies directly increase employees’ psychological empowerment, but also indirectly influence their intention to comply with the ISP.

Our study has some limitations. We employed a cross-sectional approach, which does not permit us to draw conclusions concerning causal direction. Also, it is possible that the respondent feelings and thoughts in answering the survey questions were influenced by their environments (the ‘halo effect’) (Herath and Rao, 2009a). And finally, the use of student data in the US only limits its generalizability. Future research can extend our study in a number of ways. First, we have focused on structural empowerment practices only as antecedent of psychological empowerment. Future research can explore different drivers to enhance feeling of empowerment, such as task characteristics, leader-member exchange (LMX), formal and informal power, and personality traits. In addition, future research can investigate whether the effect of the psychological empowerment may be moderated by the complexity of the information security task.

References


Empowerment and ISP Compliance Intentions


Empowerment and ISP Compliance Intentions


