Asian Journal of Information Technology 16 (2-5): 227-239, 2017
ISSN: 1682-3915

Impacts of Security Policy Goals and Motivation on Compliance Intention: The Linkage Between Motivation Theory and Goal Setting

[1]Inho Hwang, [2]Hyunsun Park and [2]Sanghyun Kim
[1]College of Business and Economics, Chung-Ang University, Seoul, South Korea
[2]School of Business Administration, Kyungpook National University, Daegu, South Korea

Abstract: The importance of information management is increasing and organizations are continually investing in information security in addition to adapting and operating systematic security policies. In order to increase employee's information security compliance intention, employee security motivation should be increased via. clear goal setting of the organization's information security policy. This research verifies the positive influence of the attributes (difficulty and specificity) of an organization's security policy goal on an employee's extrinsic motivation (perceived sanction) and intrinsic motivation (perceived value congruence) and verifies the perceived employee motivation increase of security compliance intention. We use structural equation modeling to test the research hypothesis. A survey was conducted with employees of organizations that apply information security policy and technology in South Korea and 346 data samples were collected. The result shows that organization security policy goal difficulty and specificity has a positive influence on employee security compliance motivation. Moreover, an employee's extrinsic and intrinsic motivation has a positive influence on compliance intention. Our result presents, in developing an organizational security policy that the importance of providing a security policy goal can induce the formation of an employee's motivation.

Key words: Security policy goal difficulty, security policy goal specificity, perceived snctions, perceived value congruence, compliance intention, motivation

INTRODUCTION

The targets and measures of organization Information Security (IS) threats are becoming diversified and organizations are trying to mitigate IS threats by implementing specialized IS technology and strict security policy. The global market for IS technology is expected to grow from US $71 billion in 2014 to US $101 billion by 2018 (Gartner, 2014). According to a Verizon report (2013) on the types of security accidents, accidents by extrinsic hacking are being reduced as a result of the implementation of specialized security technology. On the other hand, although security accidents by insiders form a small proportion of 14% out of all accidents, these are steadily increasing in number. Moreover, security errors that cause IS accidents by insiders occur regardless of job position. These positions include Internet Technology (IT) system managers officers, engineers, board members or employees of partner organizations. Therefore, there is a need for IS countermeasures for employees.

According to an organization's IS technology and policy management measure, the organization first adapts the necessary IS technology and policy regardless of the employee's intention and second, establishes an IS strategy to induce employee participation (Tsohou *et al.*, 2015). On the other hand, employees make selective decisions regarding the surrounding security environment, peer behaviors, organizational culture and so on West (2008). In addition, because organizations cannot control and manage employee noncompliance behavior as a whole, the uncertainty regarding an employee's IS compliance is high (Herath and Rao, 2009). Therefore, in order to mitigate security threats by insiders, employee voluntary security behaviors are prioritized.

Previous studies on employee IS compliance take the approach of improving employee security motivation. General Deterrence Theory (GDT) explains employee motivation and argues that the level of IS compliance behavior can become comparable to that required by the organization, emphasizing sanction certainty and severity which are extrinsic motivations (Guo *et al*., 2011; Guo and Yuan, 2012; Ifinedo, 2012; Lee and Larsen, 2009). Recently, there has been emphasis not only on employee extrinsic motivation but also on intrinsic motivation. Studies that take the approach of identifying employee intrinsic conditions with the organizational vision or goal

Corresponding Author: Sanghyun Kim, School of Business Administration, Kyungpook National University, Daegu, South Korea

to induce employee active behavior are being presented (Herath and Rao, 2009; Son 2011). The previous studies have commonality in that they discuss the methods to manage IS at the organizational level via. inducing employees to develop individual motivations. In other words, in order to mitigate the threats of an organization's IS accidents, the studies claim the need for organizations to provide activities to induce security compliance behaviors such as encouraging employee motivation for security compliance via. IS education and training, communication, sharing of knowledge and methodologies.

Although, there are many studies on the motivation for IS compliance, there is a lack of studies on the influence of goal setting: the motivation that intentionally explains employee behavior direction and induces the employee to understand and take action on the IS compliance process. Security policy goal induces the employee to more clearly perceive the organization security requirements and to voluntarily comply with them. Additionally, the goal is to achieve performance at an individual and organizational level (Locke and Latham, 2002). Moreover, clear organizational vision and goal setting form the employee motivation to participate (Berson *et al*., 2015). On the other hand, a goal that is not clearly set decreases individual work performance (Wright and Davis, 2003). The attributes of goal setting are formed from a goal difficulty that is perceived to be achievable and goal specificity that can be clearly understood (Locke and Latham, 1990). D'Arcy *et al.* (2009) argued that employee security compliance motivation is formed when the employee develops awareness on organizational security countermeasures such as security policy, education and training and monitoring. In other words, the employee's awareness of the security policy goal is considered to have an influence on employee compliance motivation. According to previous studies in various contexts, organizations that have policy goal setting appropriate to their environment and characteristics can induce employee development of goal related motivation and bare performance (Berson *et al*., 2015; Wright and Davis, 2003).

Therefore, the purpose of this research is to find the influencing relationship of an organization's IS policy goal setting on employee extrinsic and intrinsic motivation. In order to achieve the research purpose, we have the following sub-categories. First, we apply "goal setting theory" in an IS context, present attributes (difficulty and specificity) for setting the security policy goal and suggest ways to more effectively convey IS policy to the employees. Second, we present the influencing relationship of employee awareness formed via. IS goal setting on extrinsic and intrinsic motivation perception and suggest that goal setting at an organizational level is a critical factor for employee motivation formation. Finally, we present the influencing relationship of employee security motivation on compliance intention and we prove that employee voluntary security compliance is possible through formation of the employee's motivation.

Literature review

Information security policy goal setting: The goal setting theory dictates that under the assumption that individuals act rationally, individuals will do their best to achieve a set goal (Locke and Latham, 2006). Goals are defined as "internal representations of desired end-states" (Austin and Vancouver, 1996). A goal develops individual behavioral motivation. A more specifically stated goal additionally gives the individual direction in order to increase the performance level (Pinder, 1998). In other words, goals supply direction for individual decision-making in both how to perform the work and how much time to invest. Locke and Latham (2002) presented the mechanism of individual goal setting endowing motivation on behavior in four categories. First, goals boost behavior by encouraging individuals to expend greater effort. Second, goals serve a directive function to keep the individual focused on the goal. Third, goals lead to persistence in the face of difficulty. Finally, goals lead to exploration and excitement. Moreover, the word "goal" is a part of the group of descriptors that include intention, aim, task, deadline, purpose and objective and refers to the state of either consciously or unconsciously influencing human behavior (Koskosas, 2008).

Goal is a motivation that drives individual performance as well as the performance of an organization. Locke and Latham (2002) presented the influencing relationship of an organizational goal on employee performance, stating that the goal of the organization has a positive influence on the individual's performance. Pritchard *et al.* (1988) explained the importance of setting goals in terms of organizational performance. They argued that because most of the tasks are complex and mutually interdependent, there is a need for goal setting at a group level. Additionally, they verified that organization performance is increased up to 76% when an organizational goal is established and both feedback on performance and incentive to achieve the goal are provided. Indeed, more than when specific goal

setting is not provided. Wright and Davis (2003) claimed that procedural constraints which reduce an organization's goal achievement by fostering a negative working environment, decrease the individual's goal specificity and influence work satisfaction. Wright (2004) presented the need for an organization to strive to provide goal attribute (difficulty and specificity) to employees since the employee's work motivation is influenced by the formulated individual goal attributes. In other words, organizational goal setting has an influence on an employee's goal and can enhance individual performance required by the organization.

In the perspective of IS, the goal setting of an organization's IS policy is an important factor for an employee achieving security performance. Since, the organization IS performance is decided by employees who apply the IS policy and security system within the organization, it is important to present a security policy goal that employees can comprehend and accommodate (Ruighaver *et al*., 2007). Previous research takes the approach of utilizing motivation as a tool to increase employee IS compliance intention and as such, presented the importance of IS goal setting. Hu *et al.* (2012) claimed that an organization should develop organizational culture to induce an employee's voluntary security behavior. The organizational culture is established by presenting the goal orientation to employees by which the employees perceive the value of security.

Additionally, they claimed that an employee's goal orientation perception for an organization's IS goal positively influences the employee's compliance intention. Koskosas (2008) presented the importance of goal setting in terms of IS management. They suggested that an organization should conduct appropriate goal setting planning and execution and take the approach of utilizing an evaluation stage when adapting an IS policy to ensure the system is adequate for an organization. Moreover, they proposed goal setting in terms of both physical and system security goals. Detert *et al.* (2000) argued that in order to form an IS compliance culture, the organization should take the approach of setting a suitable organizational goal in the process of establishing IS policy planning. The developed security culture will then lead to IS compliance.

Goal attributes are defined as the object or aim of an action and are categorized into goal specificity and difficulty (Locke and Latham, 2002). Goal specificity refers to the degree that the goal has been defined, thus, encouraging employees to follow defined objectives or targeted actions (Vollmeyer *et al*., 1996). In other words, the more specific and challenging the goal, the higher the performance. Goal difficulty refers to the goal being achievable, yet difficult to accomplish (Diefendorff and Seaton, 2015). Moreover, assuming the individual accepts the goal, goal difficulty has a positive influence on performance and satisfaction by inducing additional effort and attention to work. In an organizational or individual goal, performance is influenced according to the goal attributes (specificity, difficulty).

Locke and Latham (1990) similarly argued that the more specific and more difficult the goal (compared to "do your best goal"), the higher the level of work performance. They argued that goal commitment is proportionate to the goal's difficulty and the more difficult goal encourages employees to commit themselves to achieving the goal. Additionally, the more specific the goal, the more effort and attention is given by the individual to achieve the goal, thus, fostering related behaviors. Pinder (1998) claimed that the more specific and difficult a goal, the more likely it is for individuals to invent innovative methods to achieve the goal. Diefendorff and Seaton (2015) likewise argued that a specific and difficult goal motivates the employee to draw strategies and measures to achieve the goal.

Security extrinsic and intrinsic motivation: Pinder (1998) defines work motivation as follows: "a set of energetic forces that originate both within as well as beyond an individual's being, to initiate work-related behaviors and to determine its form, direction, intensity and duration". In other words, work motivation in an organization denotes both energy and direction for action and a source of behavior maintenance. In the context of IS, motivation is a critical factor that can encourage individual needs and expectations in order to reinforce the security behavior requested from employees by the organization (Safa and Solms, 2016). Therefore, motivation is an important antecedent that changes employee compliance behavior to meet the IS goal required by the organization. Motivation can be categorized into extrinsic and intrinsic motivation (Herath and Rao, 2009). Extrinsic motivations include money, compliments, bonuses or trophies and are related to attaining a reward from the organization. Intrinsic motivation is related to the ability to perform the task without expecting a reward from the organization, including a sense of accomplishment or doing something because it makes one feel good (Fair and Silvestri, 1992).

Extrinsic motivation has traditionally been used as the paradigm for understanding employee rule-following behavior (Son, 2011). Extrinsic motivation refers to the results of a particular behavior as it relates to attaining a

desired outcome (Safa and Solms, 2016). Since, IS adherence is a behavior that must be executed by employees, generally sanction is emphasized (Guo and Yuan, 2012). From this perspective, most organizations enforce termination on employee IS non-compliance behavior and explicitly present the security policy as such. According to GDT, the use of assured and severe sanction deters employee IS non-compliance. GDT was originally developed to explain how to prevent individuals from engaging in undesirable activities (Son, 2011). When employees do not clearly perceive an organizational sanction, they do not completely execute the organization IS policy. Therefore, there is a need to emphasize security compliance behavior by conveying and clarifying an extrinsic motivation like sanction to employees.

Intrinsic motivation is derived from individually varying norm and moral beliefs which lead to employee obedience to organization rules regardless of desire for reward from the organization (Safa and Solms, 2016). In employee behavior, intrinsic motivation has stronger results than extrinsic motivations such as compensation and sanction (Herath and Rao, 2009). Davis *et al.* (1997) suggested that employees reinforced by intrinsic intangible rewards such as self-actualization have higher motivation to perform better. Intrinsic motivation is the source of achieving good results for the community or the organization one is affiliated with. In terms of IS, the importance of intrinsic motivation is presented in various studies. On IS policy compliance, Bulgrucu *et al.* (2010) claimed that employee intrinsic benefits are an important source for deciding positive IS compliance attitude. Son (2011) verified that employee compliance to IS policy was more influenced by intrinsic motivation based on value, rather than extrinsic motivation based on sanction. Particularly, he claimed that organizational activity that increases perceived value congruence is important for increasing employee compliance intention.

Information security compliance intention: The possibility of an information breech by employees is a threat to IS and the importance of controlling information leakage by employees is increasing (Chu and Chau, 2014). Organization IS will be at risk when employees have access to the organization information system whenever and wherever (Bulgurcu *et al.*, 2010). Employees who have access to the organization information system are capable of intentionally causing an information breach accident via. hacking and of leaking organizational information resources through carelessness (West, 2008).

However, according to the relationship between an organization and an employee in terms of IS, first, the organization cannot fully detain its employee IS-related behaviors. On the other hand, employee security behaviors can cause impediments to effective work performance and anxiety about appropriate security behaviors. In order to increase the employee compliance level on organization IS policy in such a relationship, it is important to support employees to induce voluntary security behaviors (Chen *et al.*, 2012). Indeed, in order to mitigate IS threats by employees, a strategic approach by the organization is needed to increase security intention.

Intention is a mental state that shows a commitment to execute a particular action now or in the future (Safa and Solms, 2016). Since intention refers to the employee's mental plan to achieve a goal, it is highly likely for employees with high intentions to perform positive behaviors. In IS, intention is applied as security compliance intention. Vance *et al.* (2012) defined the term as an employee's intention to protect organization information resources from intrinsic and extrinsic threats. Bulgurcu *et al.* (2010) defined the term as an employee's intention to protect the organization information technology resources from potential security breaches. In other words, because security compliance intention is dependent on an employee's voluntary will to participate in activities to protect information against external threats, an organization should develop and provide its employees with strategies to enhance security compliance.

Research model and hypotheses

Research model: This study, presents the influencing relationship of security policy goal setting attributes (difficulty and specificity) on the employee perception of security compliance in addition to the influencing relationship of the perception of developed sanction and value congruence on employee compliance intention (Fig. 1). Through this, we prove that a security policy goal provided by an organization is an important antecedent for formulating employee motivation for increased compliance intention. Further, we present the research direction for developing an organizational security policy goal.

Hypothesis development: Extrinsic motivation is an important source for increasing employee IS policy compliance intention. An employee will attempt to comply with IS policies when perceived that non-compliant behavior will bring about a severe and negative outcome.

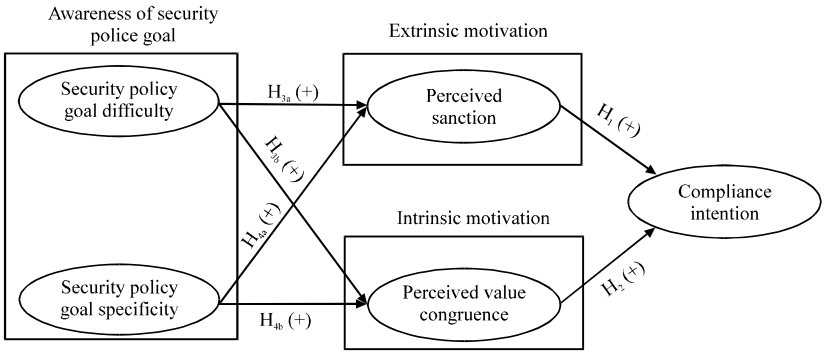

Fig. 1: Research model and hypotheses

In other words, to mitigate an IS threat by an employee, the organization should impose sanctions for employee non-compliance as the employee will deter security behaviors when a sanction has been perceived (Guo *et al*., 2011). Perceived sanction is defined as perception of tangible or intangible penalties such as demotions, loss of reputation, reprimands, monetary or nonmonetary penalties and unfavorable personal mention in oral or written assessment reports (Guo and Yuan, 2012).

In IS, previous studies reveal that sanctions have a positive influence on security policy compliance intention. Herath and Rao (2009) verified that when extrinsic motivations such as severity and certainty of penalty, are clearly delivered to employees is policy compliance intention is increased. Boss *et al.* (2015) proved that perceived threat severity and vulnerability are important antecedents for increasing employee anti-malware software use intention. Moreover, Chen *et al.* (2012) verified that not only does an organization's punishment have a positive influence on employee compliance intention, it has an enhancing moderation effect, the higher the control level certainty. Particularly (Guo and Yuan, 2012) presented that organization sanction levels include organizational sanctions, workgroup sanctions and personal self-sanctions and verified that the various organization sanctions have a positive influence on compliance intention. We propose the following hypothesis on the basis of previous studies.

- H_1: perceived sanction will be positively associated with compliance intention

In recent studies on employee security behaviors, intrinsic motivation was presented as a more important factor than extrinsic motivation (Son, 2011). Particularly, on behalf of the IS manager, an organization should induce employees to develop shared motivation by interacting with other individual's behavioral values in order to achieve the IS goal (Safa and Solms, 2016). Individuals have a tendency to verify and reinforce beliefs by sharing and interacting in other group's similar beliefs. Beliefs built in such a way help employees commit to the organization (Li *et al*., 2010). In other words, the organization should encourage employees to positively adjudge the IS value congruence. In this context, we apply perceived value congruence as an intrinsic motivation. Perceived value congruence was defined as an employee assessment of the extent to which the employee and employer share the same value set (Son, 2011).

In IS, intrinsic motivation has positive influence on IS policy compliance intention. Son (2011) verified that extrinsic motivation (perceived deterrent certainty and perceived deterrent severity) and intrinsic motivation (perceived legitimacy and perceived value congruence) have a positive influence on adherence to the IS policy required by the organization and in particular, claimed that intrinsic motivation (perceived legitimacy and perceived value congruence) is the more important source. Safa and Solms (2016) suggested in a study on employee behavior in IS knowledge sharing that intrinsic motivation (curiosity and self-worth satisfaction) positively influences employee attitudes and induces actual behavior related to knowledge sharing. Guo *et al.* (2011) claimed that the non-compliance intention decreases with employees who have a perceived identity match. Li *et al.* (2010) claimed that organizational identification develops personal norms, thus increasing IS policy compliance intention and has a buffering moderation effect on the negative relationship between employee perceived risks and compliance intention. We propose the following hypothesis on basis of previous studies.

- H_2: perceived value congruence will be positively associated with compliance intention

Employee IS motivation is influenced by organizational security environments that surround them (D'Arcy *et al*., 2014). In other words, the organization should clearly provide IS policy to employees in order for them to perceive the compliance motivation. In this perspective, in order to formulate employee security compliance motivation, it is necessary to clearly set a security policy goal at the organizational level (Berson *et al*., 2015). The IS policy definition is given as the rules and guidelines for an organization's effective use of the IS system (Whitman, 2004). Security policy includes explanations for the organizational IS goal, explanations for the security standard and rules, responsibility for security behavior and process for reporting security accidents (Kwok and Longley, 1999).

If the organization formulates employee awareness on security policy via. clear goal setting of such security policy, it has a positive influence on IS compliance intention via. the increase of employee extrinsic and intrinsic IS motivation. Security policy that is systemized to harmonize with an organization's characteristics and environments can induce employee reliability. Moreover, the more specific the security policy, the better the management of an employee's security behavior (Safa *et al*., 2015). Therefore, the better the goal setting, the higher the employee's perceived motivation of security behavior.

Locke (1996), in a study on motivation via. conscious goal setting, argued that goal commitment has influence on incentives (supportiveness, recognition and rewards) that increase personality traits and performance. In other words, if an organization provides a goal that is achievable by the employee and provides additional incentives, the employee's goal commitment increases; thereby having a positive influence on performance. Additionally, Berson *et al.* (2015) claimed that employees formulate motivation adequate for the organizational goal, if they have a narrow temporal distance between their goal or vision and that of the organization; by sharing their goal or vision with the organization (for example, when a goal or vision is provided that is difficult, yet comprehensible and achievable). Colquitt and Simmering (1998) verified that goal orientation has a positive influence on motivation during goal initiation. In other words, the organization's security policy goal setting has a positive influence on employee motivation for IS compliance.

In particular, goal attributes (difficulty and specificity) have an influence on goal commitment and performance. Locke (1996) claimed that in particular when goal difficulty is high, satisfaction is positively influenced and the more specific or explicit goal further increases the performance. A goal's difficulty and specificity mitigates the variance in individual performance in an organization via. the individual having control over the performance. In other words, difficulty and specificity which are attributes of organizational goal setting, are antecedents for forming an individual's positive motivation for achieving the goal.

Moreover, in the IS context, there have been studies on the influence of employee security policy awareness on security motivation. D'Arcy *et al.* (2009) claimed that employee awareness of an organization's IS policy forms a perception of an IS non-compliance behavior sanction, which is an extrinsic motivation and decreases the intention to misuse the information system. Bulgurcu *et al.* (2010) verified that after building awareness of an organization's IS policy, the employee formulates a perception on the benefit and cost of compliance and cost of noncompliance in which the result is assured. The employee will then arrive at a decision regarding IS compliance intention while considering the intrinsic benefits and cost alone.

Additionally, Hu *et al.* (2011) claimed that employee perception of an organization's IS policies has a positive influence on intrinsic and extrinsic motivation for rational choice calculus and as a result has influence on compliance intention. Flores and Ekstedt (2016) claimed that an organization's security structure (leadership and security culture) forms employee intrinsic beliefs, increasing compliance intention. In other words, through awareness on security policy provided by the organization, the employee considers the costs and benefits of compliance and compliance intention is induced. Considering previous studies, when an organization provides an IS policy goal to an employee, contemplating goal difficulty and specificity, the employee perceives a sanction, an extrinsic motivation and value congruence, an intrinsic motivation. We propose the following hypothesis on basis of previous studies.

- H_{3a}: goal difficulty of security policy will be positively associated perceived sanction
- H_{3b}: goal difficulty of security policy will be positively associated perceived value congruence
- H_{4a}: goal specificity of security policy will be positively associated perceived sanction
- H_{4b}: goal specificity of security policy will be positively associated perceived value congruence

MATERIALS AND METHODS

Participants and data collection: The purpose of this study is to find methods for enhancing employee IS compliance intention through IS policy goal setting of an

organization. The participants chosen as suitable for the study are employees of organizations with an IS policy in place and are employees that apply IS policy at their work. Therefore, we chose South Korean organizations that are categorized as financial institutions or conglomerates that have a good IS policy. Additionally, in terms of job responsibilities in these organizations, we chose those individuals that are not employed in the IS department of the organization. Because the task of the IS department employee is to adapt and operate security technology to minimize the organization's IS accidents and monitor employees for security purposes, unlike other employees, these have more security information than those of other departments. As such, they were excluded as participants.

First for the survey, we visited the branch offices of the chosen institutions. Then, we obtained permission to perform the survey in the office. We explained the purpose of the survey to the participants at the office, distributed the survey and collected the responses. Moreover, those who were in locations where collection of the survey was impractical, were requested to send a soft copy via. post or email. We visited 65 offices that were contacted in advance. The survey was distributed to a total of 658 individuals and 379 responses were collected. The 346 responses were used in the research as the remaining 33 were incomplete. Descriptive statistics for the respondents are shown in Table 1.

The gender ratio was relatively similar. Among 346 responses, 56.1% (194 cases) were male and 43.9% (152 cases) were female. In terms of age distribution, 17.6% (93 cases) consisted of those younger than 30 years old, 26.5% (140 cases) consisted of those 31-40 years old, 19.3% (102 cases) consisted of those 41-50 years old and 2.1% (11 cases) consisted of those >50 years old. For the industry type distribution, the financial/insurance industry totaled 68.8% (238 cases), manufacturing totaled 23.1% (80 cases) and distribution totaled 8.1% (28 cases). In the context of job position, the staff group was the largest as it was comprised of 41.6% (144 cases) and the assistant manager group followed with 26.6% (92 cases).

Table 1: Demographic characteristics of participants

Demographic categories	Frequency	Percentage
Gender		
Male	194	56.1
Female	152	43.9
Age		
< 30	93	17.6
31~40	140	26.5
41~50	102	19.3
> 50	11	2.1
Type of industry		
Finance/insurance	238	68.8
Distribution	28	8.1
Manufacturing	80	23.1
Job position		
Staff	144	41.6
Assistant manager	92	26.6
Middle manager	55	15.9
General manager	55	15.9
Total	346	100.0

Measurement development: We presented five constructs necessary for the research model and hypothesis based on previous studies related to goal setting and motivation theory. The security policy goal difficulty was defined as "the difficulty of organization's IS policy goal" and utilized four items of Wright (2004). The security policy goal specificity was defined as "the specificity of an IS policy goal that is comprehensible" and utilized three items of Wright (2004). Perceived sanction was defined as "the degree of employee perception of the organization's sanction on IS non-compliance" and utilized three items of Guo *et al.* (2011). The perceived value congruence was defined as "the degree of congruence between the organization's value and that of the individual" and utilized four items of Son (2011). Compliance intention was defined as "employee intention to protect the organization's information resource and prevent accidents" and utilized four items of Chen *et al.* (2012) that applied a compliance intention variable in IS.

Items for these constructs were modified to match with the purpose and situation of IS. The survey items were modified and reinforced in two steps. First, we interviewed five individuals, graduate students who were employed at the organizations with an IS policy. We were able to gain an understanding of the current status of the organizational policy and goals. The five constructs examined were then modified. Second, we performed a content validity check on the items developed by the 10 IS and ICT researchers. We checked for the understandability of the items and validity of the variables. Ultimately, we used 18 items in the survey. All items were measured on a seven-point Likert scale: 1 strongly disagree to 7 strongly agree.

RESULTS AND DISCUSSION

Reliability and validity analysis: This research verifies the propriety of the research model via. testing reliability and validity. First, in order to test the model's reliability analysis, we measured Cronbach's alpha using SPSS 21.0. Cronbach's alpha should be higher than the minimum cutoff score of 0.70 (Nunnally, 1978). As a result, we selected 16 items out of 18; the excluded items (PGD4, PVC2) have a problem with reliability. The perceived value congruence, the variable with the lowest Cronbach's alpha reading, displayed a value of 0.886 and was adjudged most appropriate.

Table 2: Results for construct validity and reliability

Construct/Item	Mean	SD	Factor loading	Cronbach's alpha	CR	AVE
Security policy goal difficulty						
PGD1	5.18	1.22	0.747	0.889	0.820	0.603
PGD2			0.826			
PGD3			0.755			
Security policy goal specificity						
PGS1	5.08	1.25	0.826	0.920	0.848	0.651
PGS2			0.860			
PGS3			0.728			
Perceived sanction						
PS1	5.27	1.44	0.880	0.969	0.935	0.827
PS2			0.893			
PS3			0.883			
Perceived value congruence						
PVC1	5.14	1.18	0.817	0.886	0.831	0.622
PVC3			0.839			
PVC4			0.742			
Compliance intention						
CI1	5.61	1.12	0.885	0.969	0.958	0.852
CI2			0.876			
CI3			0.888			
CI4			0.820			

Table 3: Results for discriminant validity

Construct	1	2	3	4	5
Security policy goal difficulty	0.777				
Security policy goal specificity	0.630**	0.807			
Perceived sanction	0.620**	0.596**	0.909		
Perceived value congruence	0.544**	0.573**	0.513**	0.789	
Compliance intention	0.546**	0.559**	0.597**	0.609**	0.923

*, **p<0.05<0.01; values in bold type along the diagonal indicate the square root of the AVE

Table 4: Fit Indices of the structural model

Fit indices	χ^2/df	GFI	AGFI	CFI	NFI	RMSEA
Value in this study	1.897	0.939	0.914	0.986	0.970	0.051

Second, we assessed the convergent and discriminant validity of the measurement model through a Confirmatory Factor Analysis (CFA) using AMOS 22.0. The fitness between the characteristic of the measurement model and that of the dataset were tested to purify the measurement model. The decision evaluating the overall fit of the measurement models was based on a number of factors, including the relative χ^2 (χ^2 /df), Goodness-of-Fit Index (GFI), Adjusted Goodness-of-Fit Index (AGFI), Comparative Fit Index (CFI), Normed Fit Index (NFI) and Root Mean Square Error of Approximation (RMSEA). A good fit is indicated when the GFI, NFI and CFI exceed 0.90 (Bentler, 1990); the AGFI exceeds 0.8 (Fornell and Larcker, 1981) and RMSEA is smaller than 0.06 (Joreskog and Sorbom, 1996). In addition, the value of χ^2/df should range from 3-5 (Goodhue, 1995).

The result of analysis revealed that all fit indices of the model were appropriate to advised value (χ^2 = 1.704, GFI = 0.947, AGFI = 0.923, CFI = 0.989, NFI = 0.974, RMSEA = 0.045). Convergent validity was calculated by Construct Reliability (CR) and Average Variance Extracted (AVE). The CR of all constructs should be higher than the minimum cutoff score of 0.70 (Wixom and Watson, 2001) and AVE should exceed 0.5 (Fornell and Larcker, 1981). The result of the construct reliability ranged from 0.818-0.958 and AVE values ranged between 0.600 and 0.852. Thus, the convergent validity is shown to be acceptable (Table 2).

Discriminant validity was assessed using AVE. Discriminant validity can be checked by examining whether the correlations between the variables are lower than the square root of the AVE (Fornell and Larcker, 1981). In this case, the correlations between the constructs did not exceed the square root of the relevant AVE, demonstrating appropriate discriminant validity (Table 3).

Structural model: We examined the hypotheses using Structural Equation Modeling (SEM) with AMOS 22.0. We derived the fit indices for the structural model, path coefficients and R^2 of the endogenous variables. We utilized the same indices from the earlier CFA. Six common model-fit measures were utilized to estimate the measurement model fit. The values show that the fitness of the structural model is above the required level (Table 4).

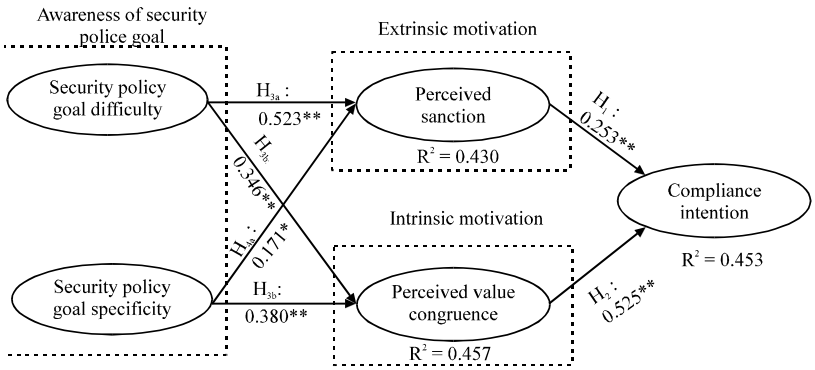

Fig. 2: Results of the structural model

Table 5: Summary of hypothesis tests

Hypothesis	Path	Path coefficient	t-value	Result
H_1	Perceived sanction→compliance intention	0.253**	5.309	Supported
H_2	Perceived value congruence→compliance intention	0.525**	9.920	Supported
H_{3a}	Goal clarity→perceived sanction	0.523**	7.310	Supported
H_{3b}	Goal clarity→perceived value congruence	0.346**	4.757	Supported
H_{4a}	Goal specificity→perceived sanction	0.171*	2.485	Supported
H_{4b}	Goal specificity→perceived value congruence	0.380**	5.244	Supported

*, **p<0.05<0.01

Given the good fit, the proposed hypotheses were examined using standardized path coefficients (β). Both Fig. 2 and Table 5 display the results of model testing. The result of analyzing the hypothesis H_1 where perceived sanction increases compliance intention, reveals that the two variables have a positive influencing relationship ($\beta = 0.253$, $p < 0.01$). Thus, H_1 is supported. The result of analyzing hypothesis H_2 where perceived value congruence increases compliance intention, reveals that the two variables have a positive influencing relationship ($\beta = 0.525$, $p<0.01$). Thus, H_2 is supported. The result of analyzing hypotheses H_{3a} and H_{3b} which argue that security policy goal difficulty increases perceived sanction and perceived value congruence, reveals that the two variables have a positive influencing relationship (H_{3a} :$\beta = 0.523$, $p<0.01$, H_{3b}: $\beta = 0.346$, $p<0.01$). Thus, H_{3a} and H_{3b} are supported. The result of analyzing the hypotheses H_{4a} and H_{4b} which argue that security policy goal specificity increases perceived sanction and perceived value congruence, reveals that the two variables have a positive influencing relationship (H_{4a}: $\beta = 0.171$, $p<0.05$, H_{4b} :$\beta = 0.380$, $p<0.01$). Thus, H_{4a} and H_{4b} are supported.

Finally, we derived the R^2 values of the endogenous variables. The R^2 value denotes the percentage of the variance that is explained by each construct within the model. Compliance intention was shown to explain 45.3% of perceived sanction and perceived value congruence variance. Perceived sanction was shown to explain 43.0% of security policy goal difficulty and security policy goal specificity variance and perceived value congruence was shown to explain 45.1% of security policy goal difficulty and security policy goal specificity variance.

CONCLUSION

This study verified the influencing relationship between motivation by which employee IS compliance intention is increased and an organization's security policy goal setting. Specifically by applying the attribute (difficulty and specificity) factor of goal setting in IS, we presented the necessary goal setting methods in developing an organization's IS policy. Additionally, we verified the influence of the security policy goal setting at the organizational level on an employee's perception of IS motivation and influence of an employee's established security motivation on compliance intention.

We presented a research model and hypotheses to explain the study purpose and performed actual proof analysis based on structural equation modeling. The survey targets were individuals employed at South Korean financial institutions and conglomerates having an IS policy and 346 responses were used in the study. As the result of proving the hypothesis, first, we verified that an employee's extrinsic factor of perceived sanction and intrinsic motivation factor of perceived value congruence have positive influence on security compliance intention (H_1 and H_2). Such result is congruent with the result of previous studies (Herath and Rao, 2009; Son, 2011) that argued that the development of employee

motivation has a positive influence on security compliance intention. The t-value of perceived value congruence was shown to be higher than that of perceived sanction. This reveals that intrinsic motivation is a greater factor in the increase of compliance intention than extrinsic motivation. In other words, the level of organizational IS policy compliance refers to employee compliance activity; an organization should induce employees to perceive motivation and support employees to perceive the values of security greater than imposed sanctions.

Second, we proved that in performing security policy goal setting, goal difficulty has positive influence on employee sanction and value congruence perception (H_{3a} and H_{3b}). Such result is congruent with the previous study of Berson *et al*. (2015) that argues that goal setting increases employee motivation. Goal difficulty refers to a goal being achievable and at the same time having a high standard. Taking the long-term approach to the level of an organization's security goal can increase employee extrinsic and intrinsic motivation for compliance intention. Therefore, an organization should consider an appropriate amount of difficulty befitting the needs of the organization when performing security policy goal setting.

Third, we proved that in performing security policy goal setting, goal specificity has positive influence on employee sanction and value congruence perception (H_{4a} and H_{4b}). Such result is congruent with the result of previous research (Berson *et al*. 2015) that argues that goal setting increases employee motivation. Goal specificity refers to the level of clarity for the goal. When employees have a clear understanding of security policy goal concept and method of performance, employees have a higher level of extrinsic and intrinsic motivation for compliance intention. Therefore, an organization should induce employees to clearly understand the security policy goal and behave by increasing the security policy goal specificity. The result of this research presents direction for developing security policy by proving that the influence of an organization's IS policy goal setting on employee compliance intention increases based on the perception of extrinsic and intrinsic motivation.

LIMITATIONS

This research has limitations from a few perspectives and needs reinforcement in future studies. First, further studies are required for finding the influence of goal setting on employee security motivation and compliance behavior based on an actual organization IS policy goal. Since, this research analyzed goal setting difficulty and specificity of organization security policy based on employee thoughts at the time the survey was conducted, we could not objectively examine the organization's form of security policy goal setting. Additionally, we only measured IS compliance intention by self-reported information on the survey and we were unable to examine what kind of influence existed in terms of behavior. Therefore, future studies are needed to measure an employee's actual security behavior by grouping security policy goals by attributes and providing them to employees.

Second, further studies should categorize employee security compliance motivation, present the factor that changes the influencing relationship between security motivation and result and verify it. We presented sanction and value congruence categorizing employee compliance motivation as extrinsic and intrinsic motivation. However, various motivations exist on previous motivation related studies. Moreover, there exists an additional factor that mediates or moderates the influencing relationship of motivation on compliance intention. Therefore, future studies should present alternative methods to more effectively influence compliance intention, rather than formed motivation by presenting various detailed motivations and additional consideration factors in the process leading to compliance intention.

Third, in performing security policy goal setting, further study is needed to present the factor for increasing security performance and verifying the relationship. We surveyed for current security policy goal and motivation and compliance intention, targeting the employees of conglomerates and financial institutions that have an IS policy. Recently, methodology such as the IT governance framework, COBIT is being presented for more effective adaption of information technology. The operational usefulness of security policy goal setting can be increased when additional factors of consideration are presented in performing security policy goal setting based on such methodologies.

IMPLICATIONS

This study contributes to IS and organization research in several ways. First, we presented the importance of security policy goal setting by applying a goal setting theory in IS. Goal setting is the critical factor that formulates the motivation of an organization and employee. Particularly, goal setting is a theory that provides a good explanation for an employee's will to voluntarily participate in terms of the direction pursued by the organization in the relationship between organization and employee. However, there is a lack of studies on the

methods of security policy goal setting and processes of the employee perceiving the goal by which the formation of the employee's intention to act on the security policy is influenced.

This research proposes goal setting attributes (goal difficulty and goal specificity) as the specific factors of the security policy goal and proved that goal setting attributes are factors that have an influence on employees. Essentially, this study proposed the methods of security policy goal setting to be pursued in order to increase both the organization's level of security and employee participation. In other words, an organization should continuously induce its employees to make security efforts by having an organizational security policy that is more difficult than the currently achievable security goal. Additionally, the specificity of the organization's security policy goal should be increased in order to induce employees to pursue a higher understanding of the security policy goal. Moreover, we suggested policy goal setting methods for an organization developing an effective security policy operation by presenting detailed goal attributes (difficulty and specificity) to induce employees to both clearly understand and act on the organizational IS goal.

Second, we verified that security policy goal setting positively influences employee perception of security motivation. Theoretically, security compliance motivation is an important antecedent that increases employee security compliance intention. The security policy goal at the organizational level was adjudged the core antecedent for employee perception of security motivation and proved the positive relationship between motivation factors and goal setting attributes. Essentially, the result demonstrates an organization's plan for inducing employees to perceive motivation to formulate their compliance intention. Previous studies generally proposed critical success factors such as top management support, education, visibility, communication and help desk operation as the effort factors of an organization.

Additionally, we verified when planning for security policy, that goal setting appropriate to the organization and understood by employees has a positive influence on formulating employee motivation for security behavior. In other words, when an organization's security department establishes security policy, the result suggests the importance of goal setting and defines an approach for inducing employees to actively comply with the policy.

Third, we proved the employee perceived motivation is a factor that has positive influence on compliance intention. We presented perceived sanction and value congruence by applying both extrinsic and intrinsic motivation perspectives in IS, proving that they have positive influence on compliance intention. Theoretically, the result proved that it can be applied in IS. This same result has been presented in various motivation related studies and has argued that intrinsic motivation has more influence on the object of motivation than extrinsic motivation. Therefore, organizations should consider employee formation of intrinsic motivation for the purpose of inducing employees to voluntarily and continuously perform security compliance activities.

ACKNOWLEDGEMENT

This research was supported by Kyungpook National University Bokhyeon Research Fund, 2015

REFERENCES

Austin, J.T. and J.B. Vancouver, 1996. Goal constructs in psychology: Structure, process and content. Psychol. Bull., 120: 338-375.

Bentler, P.M., 1990. Comparative fit indexes in structural models. Psychol. Bull., 107: 238-246.

Berson, Y., N. Halevy, B. Shamir and M. Erez, 2015. Leading from different psychological distances: A construal-level perspective on vision communication, goal setting and follower motivation. Leadersh. Q., 26: 143-155.

Boss, S.R., D.F. Galletta, P.B. Lowry, G.D. Moody and P. Polak, 2015. What do users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. MIS. Q., 39: 837-864.

Bulgurcu, B., H. Cavusoglu and I. Benbasat, 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS. Q., 34: 523-548.

Chen, Y., K. Ramamurthy and K.W. Wen, 2012. Organizations' information security policy compliance: Stick or carrot approach?. J. Manage. Inf. Syst., 29: 157-188.

Chu, A.M. and P.Y. Chau, 2014. Development and validation of instruments of information security deviant behavior. Decis. Support Syst., 66: 93-101.

Colquitt, J.A. and M.J. Simmering, 1988. Conscientiousness, goal orientation and motivation to learn during the learning process: A longitudinal study. J. Applied Psychol., 83: 654-665.

D'Arcy, J., A. Hovav and D. Galletta, 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Inf. Syst. Res., 20: 79-98.

D'Arcy, J., T. Herath and M.K. Shoss, 2014. Understanding employee responses to stressful information security requirements: A coping perspective. J. Manage. Inf. Syst., 31: 285-318.

Davis, J.H., F.D. Schoorman and L. Donaldson, 1997. Toward a stewardship theory of management. Acad. Manage. Rev., 22: 20-47.

Detert, J.R., R.G. Schroeder and J.J. Mauriel, 2000. A framework for linking culture and improvement initiatives in organizations. Acad. Manage. Rev., 25: 850-863.

Diefendorff, J.M. and G.A. Seaton, 2015. Work Motivation. In: International Encyclopedia of the Social and Behavioral Sciences, Wright, J.D. (Ed.). Elsevier Publisher, Oxford, England isBN:9780080970875, pp: 680-686.

Fair, E.M. and L. Silvestri, 1992. Effects of rewards, competition and outcome on intrinsic motivation. J. Instructional Psychol., 19: 1-3.

Flores, W.R. and M. Ekstedt, 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Comput. Secur., 59: 26-44.

Fornell, C. and D.F. Larcker, 1981. Evaluating structural equation models with unobservable variables and measurement error. J. Market. Res., 18: 39-50.

Gartner, 2014. Gartner says worldwide information security spending will grow almost 8 percent in 2014 as organizations become more threat-aware. Gartner Inc., Stamford, Connecticut. http://www.gartner.com/newsroom/id/2828722.

Goodhue, D.L., 1995. Understanding user evaluations of information systems. Manage. Sci., 41: 1827-1844.

Guo, K.H. and Y. Yuan, 2012. The effects of multilevel sanctions on information security violations: A mediating model. Inf. Manage., 49: 320-326.

Guo, K.H., Y. Yuan, N.P. Archer and C.E. Connelly, 2011. Understanding nonmalicious security violations in the workplace: A composite behavior model. J. Manage. Inf. Syst., 28: 203-236.

Herath, T. and H.R. Rao, 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decis. Support Syst., 47: 154-165.

Hu, Q., T. Dinev, P. Hart and D. Cooke, 2012. Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decis. Sci., 43: 615-660.

Hu, Q., Z. Xu, T. Dinev and H. Ling, 2011. Does deterrence work in reducing information security policy abuse by employees?. Commun. ACM., 54: 54-54.

Ifinedo, P., 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Comput. Secur., 31: 83-95.

Joreskog, K.G. and D. Sorbom, 1996. PRELIS 2 User's Reference Guide: A Program for Multivariate Data Screening and Data Summarization; A Preprocessor for Lisrel. Scientific Software International, New York City, New York isBN:0-89498-041-6, Pages: 200.

Koskosas, I., 2008. Goal Setting and Trust in A Security Management Context. Inf. Secur. J. Global Perspect., 17: 151-161.

Kwok, L.F. and D. Longley, 1999. Information security management and modelling. Inf. Manage. Comput. Secur., 7: 30-40.

Lee, Y. and K.R. Larsen, 2009. Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. Eur. J. Inf. Syst., 18: 177-187.

Li, H., J. Zhang and R. Sarathy, 2010. Understanding compliance with internet use policy from the perspective of rational choice theory. Decision Support Syst., 48: 635-645.

Locke, E. A. and G.P. Latham, 2002. Building a practically useful theory of goal setting and task motivation: A 35-year odyssey. Am. Psychol., 57: 705-717.

Locke, E.A. and G.P. Latham, 1990. Work motivation and satisfaction: Light at the end of the tunnel. Psychol. Sci., 1: 240-246.

Locke, E.A. and G.P. Latham, 2006. New directions in goal-setting theory. Curr. Directions Psychol. Sci., 15: 265-268.

Locke, E.A., 1996. Motivation through conscious goal setting. Appl. Preventive Psychol., 5: 117-124.

Nunnally, J.C., 1978. Psychometric Theory. 2nd Edn., McGraw-Hill Publisher, New York, USA. isBN:9780070474659, Pages: 701.

Pinder, C.C., 1998. Work Motivation in Organizational Behavior. Prentice Hall, Upper Saddle River, New Jersey.

Pritchard, R.D., S.D. Jones, P.L. Roth, K.K. Stuebing and S.E. Ekeberg, 1988. Effects of group feedback, goal setting and incentives on organizational productivity. J. Appl. Psychol., 73: 337-358.

Ruighaver, A.B., S.B. Maynard and S. Chang, 2007. Organisational security culture: Extending the end-user perspective. Comput. Secur., 26: 56-62.

Safa, N.S. and R.V. Solms, 2016. An information security knowledge sharing model in organizations. Comput. Hum. Behav., 57: 442-451.

Safa, N.S., M. Sookhak, R.V. Solms, S. Furnell and N.A. Ghani *et al*., 2015. Information security conscious care behaviour formation in organizations. Comput. Secur., 53: 65-78.

Son, J.Y., 2011. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Inf. Manage., 48: 296-302.

Tsohou, A., M. Karyda, S. Kokolakis and E. Kiountouzis, 2015. Managing the introduction of information security awareness programmes in organisations. Eur. J. Inf. Syst., 24: 38-58.

Vance, A., M. Siponen and S. Pahnila, 2012. Motivating IS security compliance: Insights from habit and protection motivation theory. Inform. Manage., 49: 190-198.

Verizon, 2013. Verizon 2013 data breach investigations report. Verizon, Basking Ridge, New Jersey.

Vollmeyer, R., B.D. Burns and K.J. Holyoak, 1996. The impact of goal specificity on strategy use and the acquisition of problem structure. Cognit. Sci., 20: 75-100.

West, R., 2008. The psychology of security. Commun. ACM., 51: 34-40.

Whitman, M.E., 2004. In defense of the realm: Understanding the threats to information security. Int. J. Inform. Manag., 24: 43-57.

Wixom, B.H. and H.J. Watson, 2001. An empirical investigation of the factors affecting data warehousing success. MIS Quart., 25: 17-41.

Wright, B.E. and B.S. Davis, 2003. Job satisfaction in the public sector the role of the work environment. Am. Rev. Public Administration, 33: 70-90.

Wright, B.E., 2004. The role of work context in work motivation: A public sector application of goal and social cognitive theories. J. Public Administration Res. Theor., 14: 59-78.