EFFECT OF ORGANIZATIONAL SECURITY CLIMATE ON INDIVIDUAL'S OPPORTUNISTIC SECURITY BEHAVIOR: AN EMPIRICAL STUDY

Completed Research Paper

Myung-Seong Yim
Post-Doc
Sogang University
phdyim@gmail.com

Jahyun Goo
Associate Professor
Florida Atlantic University
jgoo@fau.edu

Yong-Jin Kim
Associate Professor
Sogang University
yongjinkim@sogang.ac.kr

Tae-Seok Jeong
Associate Professor
Sahmyook University
bigstone@syu.ac.kr

Dan J Kim
Associate Professor
University of North Texas
Dan.Kim@unt.edu

Abstract

Drawing upon Griffin and Neal's (2000) safety climate and performance model, this study developed an information security climate model. The research model is composed of three research variables that include information security climate, information security compliance attitude, and opportunistic security behavior. And their relationships are hypothesized accordingly. Because many studies hint us that organizational climate is a multidimensional factor composed of various organizational characteristics (Griffin and Neal 2000; James and James 1989), this study proposes a multidimensional information security climate model and investigate the relationship between the organizational security climate and individual's opportunistic security behavior. Thus, the information security climate construct was operated as a second-order construct that consists of four first-order constructs: top management attention, security reinforcement, security awareness training, and effectiveness of security policy.

Data for the study were collected through a survey of South Korean IT users. With 581 responses, results of the study strongly support the fundamental proposition that the organizational security climate has significant positive influence on the individual's opportunistic security behavior. However, the study also reveals that the organizational climate may not directly associate with the reduction of opportunistic security behavior. Rather the organizational security climate nurtures the favorable attitude of the employee towards the compliance of information security, which in turn discourages opportunistic security behavior. Overall, the findings support our view that various organizational efforts towards information security collectively create the fertile environment where an organizational member is transformed from a security threat to a security asset.

Keywords: Information Security Climate, Opportunistic Security Behavior, Safety Climate

Introduction

Recently, many companies' interest in information security is globally higher than any other time. Recent security accidents are more and more frequently taking places and those accidents show that the damage is fatal. In cases of South Korea, representative financial companies such as NongHyub, Hyundai Capital, and Samsung Card Co., have suffered security accidents during 2011 and their loss were reported to amount to 100 billion won. According to Computer Crime and Security Survey, security accidents, great and small, were reported to take places in 46% of American companies participated in the survey (Johnston and Warkentin 2010). The loss was reported to grow twice from 2006 to 2007 (i.e., $168,000 to $350,424) (Richardson 2007). As interests in information security increase like this, attentions are being highly paid to how security accidents can be decreased. By and large, security accidents are classified into four dimensions: whether those are derived from human error or non-human error; whether those problems are internal or external. Existing research on security accidents pays attention to the human error occurring internally.

Various investigations show that the number of internal security accidents occurred by insiders of organizations is much greater than that of hacking by outsiders. Cardinali (1995) reports that 80% of database security accidents are taken places by insiders and Ernest and Young (2003, 2008) also suggest that 50~75% of accidents are caused by people within an organization. Like this, as insiders' accidents represent an increasing share of total accidents, scholars have studied how security accidents caused by individuals within organizations can be decreased. In particular, they have continually investigated compliance (or not) with security policy as a way to reduce security accidents in that the kernel of the problems is whether individuals observe security policy or not (e.g., D'Arcy et al. 2010; Herath and Rao 2009a, 2009b). Existing research on security accidents mainly centers on human factors. Although existing research has contributions to identifying various aspects so that individuals may comply to company's security policies, it also reveals its limitation in that it lacks in considering how contextual factors affect individual's compliance with security policy.

According to social information view emphasizes the importance of understanding organizational environment such as organizational climate, suggesting that contextual factors may affect individual behaviors more than personal predisposition factors (Chan et al. 2005; James and James 1989; Salancik and Pfeffer 1977, 1978). Recently, Chan et al. (2005) conceptualized information security climate as an aspect of social influence by using the concept 'safety climate' and empirically analyzed the relationship of information security climate to compliance with security policy. However, a large number of extant studies show that organizational climate is not a unidimensional characteristic but a multi-dimensional one (Ansari et al. 1982; Burke et al. 1992; Griffin and Neal 2000; James and James 1989; Neubaum et al. 2004; Victor and Cullen 1988; Wimbush and Shepard 1994; Wimbush et al. 1997; Wyld and Jones 1997). Individuals within organizations tend to evaluate specific nature and its importance of the environment they belong to. Organizational climate are composed of high-dimensional factors since this nature forms organizational climate (Griffin and Neal 2000; James and James 1989). Whereas information security climate is also high-dimensional factor composed of various natures, existing literature approached the issue just from a unidimensional view.

Therefore, this study will consider security climate from a high-dimensional perspective and try to empirically analyze how security climate affects opportunistic security behaviors of individuals in organizations. Specifically, this study focuses on the relationship of security climate (as an organizational factor) to opportunistic security behaviors (as an individual factor). It is very important to investigate the relationship because organization and individual continuously interact with each other as suggested by socio-psychological view (Ansari et al. 1982).

Information Security Climate

Organizational climate focuses on organizational members' understanding with respect to observable practices and procedures. These practices and procedures are classified into multi-dimensions which can be analyzable by researchers (Denison 1996). Recent research on organizational climate tends to be more specific than existing literature (Denison 1996). This is because existing studies reflect a variety of contexts in its research. Whereas previous research focused on climate from a comprehensive view, recent studies considers climate as specific nature within an organization such as safety climate (Griffin and Neal 2000) or information security climate (Chan et al. 2005). This study focuses on information security climate because it reflects organizational nature which employees experience with regard to information security. When explaining information security climate, this study tries to describe the concept on the basis of safety climate research. There is something in common between safety climate and security climate: firstly, information security and safety do not create organizational value but these are indispensable in running companies continually (Chan et al. 2005); secondly, performance from information security and safety is achieved via non-occurrences of accidents (Chan et al. 2005). Security accidents do not induce physical damage but both can potentially cause organizational loss; thirdly, safety and information security both emphasizes employees' compliance with policies or safety regulations organizations present. However, related employees not only feel uncomfortable but also experience conflicts between job efficiency and job performance (Chan et al. 2005; Herath and Rao 2009b).

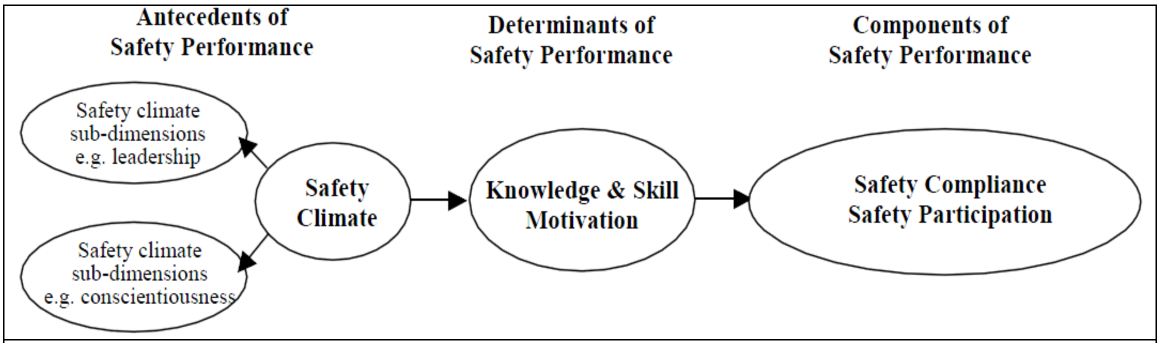


Figure 1. A Model of Safety Climate and Performance (Griffin and Neal 2000)

Depending on these relations, this study tries to develop security climate on the basis of a model of safety climate and performance (Griffin and Neal, 2000) among the safety climate studies. Most of all, in safety climate research, safety climate is composed of organizational climate in general and safety-related characteristics. Security climate is conceptualized as a higher order factor, which is composed of specific first-order factors. This is because safety climate needs to reflect various organizational attributes which drive organizational members to believe that safety is valuable (Griffin and Neal 2000). Agreement exists that safety climate is a higher order factors among the scholars but they have different views regarding what are the first-order factors for consisting the higher order factors. Referring to existing studies, Griffin and Neal (2000) suggested most frequently cited first order factors and empirically analyzed a model of safety climate and performance composed by a second-order structure. Those factors are management values, safety communication, safety training, safety inspection, and etc.. Based on this model framework, this study considers security climate as 4 first-order factors: top management attention, security reinforcement, security awareness training, and effectiveness of security policy. Specific explanation with respect to each construct will be followed in the next section.

Top Management Attention

There exist different opinions regarding what are the first-order factors forming safety climate. However, management values is one of the most frequently mentioned factors among the scholars for forming safety climate (Griffin and Neal 2000). Management values, until now, are measured by management attention toward employees' well-being, management attitude toward safety, awareness level regarding safety is important for running companies, etc. (e.g., Ocasio 1997). That is, these measurements ultimately evaluate management attention, which is a very critical factor forming safety climate. In terms of information security, top management attention can be seen as a very important factor in forming information security climate. Chan et al. (2005) suggest through empirical analysis that top management attention plays an important role in making employees comply with security policy.

Security Reinforcement

Security reinforcement is defined as top management's repetitive behaviors observed by employees (Chan et al. 2005). It includes such behaviors that top management communicate with employees and they emphasize the importance of information security. Griffin and Neal (2000) identified through empirical analysis that safety-related communication in terms of safety ultimately functions as an important factor forming safety climate. In the end, these top management's behaviors are seen as a critical factor forming safety climate in that these induce employees to commit to (involve in) specific behaviors (Purvis et al. 2001).

Security Awareness Training

Security awareness training (SAT) is one of the security countermeasures used by organizations. SAT reinforces organizational members to comply with security policy, and play role in reminding them with potential results (i.e., security accidents) caused by system misuse (D'Arcy et al. 2009). It also functions as a factor that makes employees to clearly understand and accept information security policy suggested by each organization. SAT is provided with organizational members to transfer (deliver) knowledge regarding security environments in various forms: newsletter or Email as well as online or offline training. The main purpose of SAT is to deliver knowledge regarding information danger, provide accident cases related to violations of security policy, and enhance the sense of responsibility with regard to information resources (D'Arcy et al. 2009). The SAT is one of the core factors forming information security climate among the organizational practices (Chan et al. 2005).

Effectiveness of Security Policy

In general, there are two types of security policy: (1) computer/network security policy, which describes the rules of network access control and (2) information security management policy, which includes organizational strategy and plan to ensure organization's overall information security (Goel et al. 2010). Between the two, the latter is more underlined in information security research and all organizational members within each organization is emphasized to comply with information security policy. In particular, this policy is important because it is not only directly related to all organizational members but also it has to be complied in pursuit of their duties. However, security policy should be effective in order to function properly (Goel et al. 2010). Extant literature shows different effectiveness with regard to security policy. For example, Straub (1990) suggested that security policy plays a role in reducing computer abuse whereas Foltz (2000) explained that security policy has no effects on IS (information systems) misuse. These inconsistent outcomes are resulted from the fact that security policies are being used without any assessment regarding its effectiveness. Goel et al. (2010) suggested two standards to evaluate the effectiveness of security policy: security content and security form. Between them, security content research has been widely investigated while little research regarding security form has been executed. International standard was already arranged in the security content area, so that organization's security content is generally developed, on the basis of the standard, by policy makers. Accordingly, existing research has usually evaluated whether people know there is security policy in the organization when they study security policy. However, it is necessary for security policy to be easy to understand, comfortable to read, and delivered clearly because all members in the organization are subjects to comply with security policy. The basic assumption of general deterrence theory, which is frequently used to control security violation behaviors, is that all members understand the security policy (Foltz et al. 2008). It ultimately shows and emphasizes the importance of setting up user-centric security policy. This policy functions as an important factor for forming organization's security climate among the different organizational practices (Chan et al. 2005).

Your references should comprise only published materials accessible to the public. Proprietary information may not be cited.

Research Model and Hypotheses

On the basis of the safety climate and performance model suggested by Griffin and Neal(2000) and Neal et al.(2000), this study will consider information security climate as a multi-dimensional factors and investigate how security climate affects both employees' attitude toward compliance to security policy and employees' opportunistic security behaviors. Opportunistic security behavior is defined as relative interest obtained by not complying with security policy and it implies that no compliance with security policy enhances individuals' values by various uncomportableness in the pursuit of one's duty and by negative perception regarding decreased job productivity. It is important to identify how this individual-level factor is related to organization-level (security climate). Figure 2 shows research model and its hypotheses for this study.

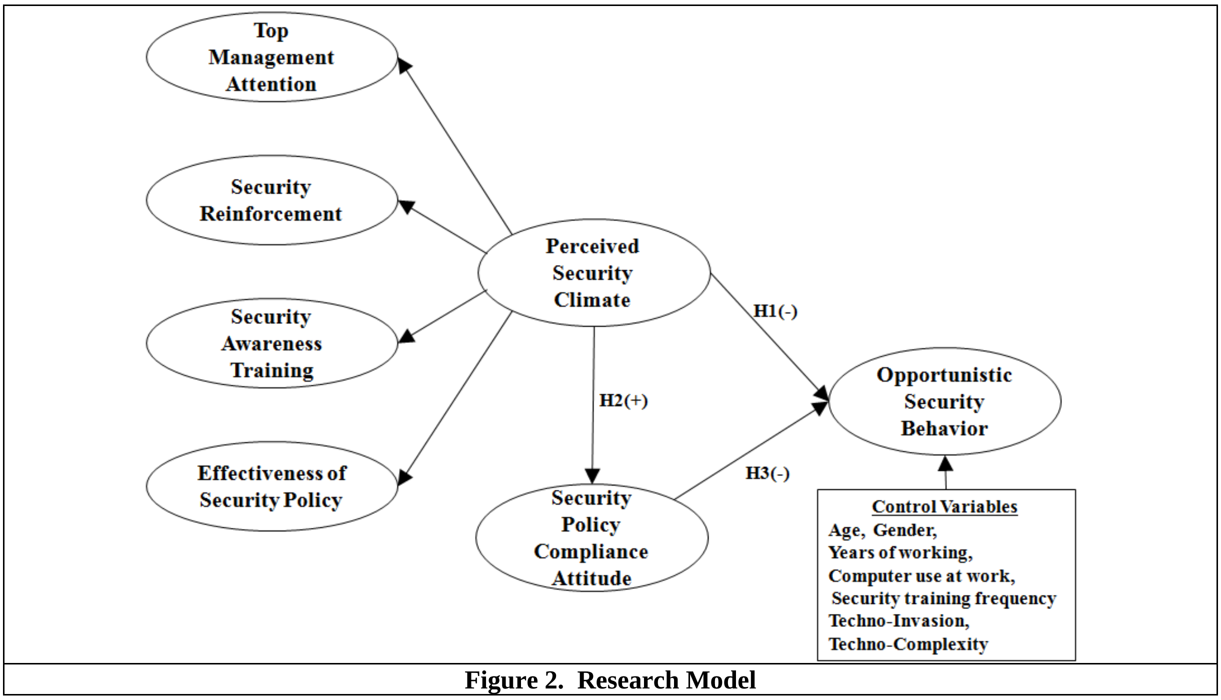

Top Management Attention
Security Reinforcement
Security Awareness Training
Effectiveness of Security Policy
Perceived Security Climate
H1(-)
H2(+)
H3(-)
Opportunistic Security Behavior
Security Policy Compliance Attitude
Control Variables
Age, Gender,
Years of working,
Computer use at work,
Security training frequency
Techno-Invasion,
Techno-Complexity

Figure 2. Research Model

Information Security Climate

Organizational climate affects members' behaviors in the organization (Chan et al. 2005). Social information processing theory suggests that individual behaviors are more affected by contextual factors than individual disposition or characteristics (James and James 1989). This is because an individual experiences organizational climate as he/she continually interacts with his/her organization (Ansari et al. 1982; Tagiuri and Litwin 1968). Ultimately, this experience functions as a factor inducing individual behaviors. In terms of information security, one of the most important behaviors is to comply with information security policy. However, observing security policy at daily work makes employees feel uncomfortableness (Herath and Rao 2009b). Moreover, it can affect negatively employees' job productivity and its effectiveness (Chan et al. 2005). These negative effects, in the end, can induce individuals' opportunistic security behaviors. Opportunistic security behavior is represented as an individual's perceived benefit when he/she does not comply with security policy. For instance, an individual has to log out his/her computer in cases he/she temporarily leaves the office. Complicated procedure with regard to company system access may induce an individual to feel repulsion to compliance with security policy. However, in cases that organizations form information security climate and this climate affects individuals' behaviors, the security climate is likely to lead to reduced opportunistic security behaviors. Moreover, complying with security policy will be thought to be right behaviors. Therefore, related hypotheses are described as follow.

Hypothesis 1. Information security climate negatively affects individuals' opportunistic security behaviors.

Hypothesis 2. Information security climate positively affects individuals' attitude toward compliance with information security policy.

Information Security Policy Compliance Attitude

Attitude is defined as an individual's decision between right and wrong regarding his/her own behaviors (Ajzen and Fishbein 1980). If an individual perceives the results of individual behaviors to be positive, he/she will develop positive attitude. On the contrary, in cases that an individual perceives the results of individual behaviors to be negative, he/she will develop negative attitude (Theoharidou et al. 2005). In terms of information security view, when organizational members perceive that complying with company's information security and it various guidelines finally has positive effects on the company, they are expected to reduce private value seeking behaviors. On the basis of this theoretical explanation, the following hypothesis is developed.

Hypothesis 3. Information Security Policy Compliance Attitude negatively affects individuals' opportunistic security behaviors.

Research Method

Data Collection and Sample

The data were collected using a questionnaire. Demographic characteristics of respondents and exploratory factor analysis were analyzed using SPSS v19. AMOS version 18 was used for confirmatory analysis of the measurement items and hypotheses testing. The unit of analysis of this study is individuals because organizational climate is perceived and assessed by each employee (Griffin and Neal 2000).

The pool of survey participants was obtained from members of the ITSMF (Information Technology Service Management Forum) Korea. The each member received an e-mail explaining the purpose of the research and inquiring about the firm's willingness to participate. ITSMF Korea is the only independent and internationally-recognized forum for IT Service Management professionals worldwide. This not-for-profit organization is a prominent player in the on-going development and promotion of IT Service management best practice. 900 questionnaires were distributed mail and e-mail. A total number of 761 responses were received, out of which 180 were unusable because of missing data items (a response rate of about 64.6 percent). To test for nonrespnse bias, we compared the participating and nonparticipating companies' revenue and number of employees (Babbie 1990). For this test, 100 responses were selected randomly. Results of independent t-tests for revenue and number of employees did not produce a significant t-value (p>0.05) (cf. King and Sabherwal 1992). These results support that respondents did not systematically differ from non-respondents. A summary of the demographic characteristics of 581 respondents is provided in Table 1. 24% of the respondents were female, whereas 76% of the respondents were male. The age of 80% participants was ranged from 25 to 44. About 40% respondents worked in IT industries.

Table 1. Demographic Information (N=581)

		Frequency	%			Frequency	%
Sex	Male	440	75.7	Industry	Manufacturing	82	14.1
	Female	127	21.9		Construction	31	5.3
	Undecided	14	2.4		IT	230	39.6
Age	18~24	3	0.5		Finance/Insurance	75	12
	25~34	253	43.5		Government	97	16.7
	35~44	212	36.5		Education	9	1.5
	45 and above	112	19.2		Other	25	4.3
	Undecided	1	0.2		Undecided	32	5.6

Construct Operationalization

To maximize measurement reliability with respect to the constructs of our research, we selected items that have been tested in extant literatures and measured in a structured format on a 7 point Likert-type scale, ranging from 1 (strongly disagree) to 7 (strongly agree) (see Appendix A). According to Boudreau et al. (2001), using validated and tested questions will improve the reliability of results. Perceived security climate refers to the employee's perception of the current organizational state in terms of information security (Chan et al. 2005). We have conceptualized perceived security climate as second-order construct comprised of four complementary first-order dimensions: (1) Top management attendance, (2) security reinforcement, (3) security awareness training, and (4) effectiveness of security. Top management attendance, which means the customary actions of management as observed by the individual employee (Chan et al. 2005), was measured 7 items adapted from Purvis et al. (2001) and Chatterjee et al. (2002). Security reinforcement, which refers to the repeated actions of management as observed by the individual employee (Chan et al. 2005), was measured 3 items adapted from Chan et al. (2005). Security awareness training, which means the individual's awareness of training program regarding information security, was measured 7 items adapted from D'Arcy et al. (2009). Effectiveness of security policy, which refers to content quality of organizational information security policy, was measured 8 items adapted from Goel et al. (2010). Information security policy compliance attitude, which is the degree to which a person has a favorable or unfavorable evaluation or appraisal of the compliance with information security policy, was measured 6 items adapted from Dinev et al. (2009), Herath and Rao (2009b), and Pavlou and Fygenson(2006). Finally, Opportunistic security behavior, which refers to an employee's belief about the positive outcomes that an individual expects for not complying with organizational information security, was measured 5 items adapted from Kim et al. (2008) and Yoon(2011).

Following Tanriverdi's (2005) approach, this study compared three alternative first-order factor models tests for dimensionality and convergent and discriminant validity of the perceived security climate. Model 1 hypothesizes that a unidimensional first-order factor accounts for the variance among all measurement items of the construct. Model 2 hypothesizes that the measurement items form into hour uncorrelated first-order factors. Model 3 hypothesizes that these first-order factors are freely correlated with each other. Finally, Model 4 hypothesizes a second-order factor that accounts for the patterns of interactions and covariance among the first-order factors. Results of model comparison are shown in Table 2. Comparison Model 1 ($\chi2$ = 5708.549, d.f. = 275) and Model 2($\chi2$ = 2924.016, d.f. = 275) indicates that Model 2 is a better-fitting model (lower chi-square for the same degrees of freedom). This result supports for multidimensionality of perceived security climate. Further comparison Model 2($\chi2$ = 2924.016, d.f. = 275) and Model 3 ($\chi2$ = 1893.360, d.f. = 275) indicates that Model 3 is superior to Model 2 ($\Delta\chi2$ = 1030.656). In Model 3standardized factor loadings of measurement items on their respective factors are all highly significant ($p < 0.001$), providing support for convergent validity of perceived security climate. Superiority of Model 3 (unconstrained model) over Model 2 (constrained model) indicates that pairs of correlations among the first-order factors are significantly different from zero (Bagozzi et al. 1991). This result supports for discriminant validity of perceived security climate (Anderson 1987; Bagozzi et al. 1991). The final test examines whether a second-order factor accounts for the patterns of interaction and covariance among the first-order factors. Security policy compliance attitude as external criterion variable is used for comparison of two models (cf. Tanriverdi 2005). Model 3 represents a direct-effect model and tests direct effects of the four first-order factors on security policy compliance attitude. Model 4 represents a second-order measurement model and tests effect of perceived security climate on security policy compliance attitude.

To do this, we used three criteria: (1) model statistics of the two specifications (Venkatraman 1990), (2) target coefficient (T) statistics (Marsh and Hocevar 1985). The second-order factor model should be preferred because it is more parsimonious with fewer parameters and more degrees of freedom (Venkatraman 1990). The target coefficient value (T = 0.99) is very close to the theoretical upper limit of 1, indicating that the second-order factor accounts for 99 percent of the relations among the first-order factors (Marsh and Hocevar 1985). Furthermore, β coefficient between perceived security climate and security policy compliance intention exceeds 0.2 (Chin 1998) and t-value is significant. In sum, these results suggest that second-order model is more appropriate to explain the perceived security climate.

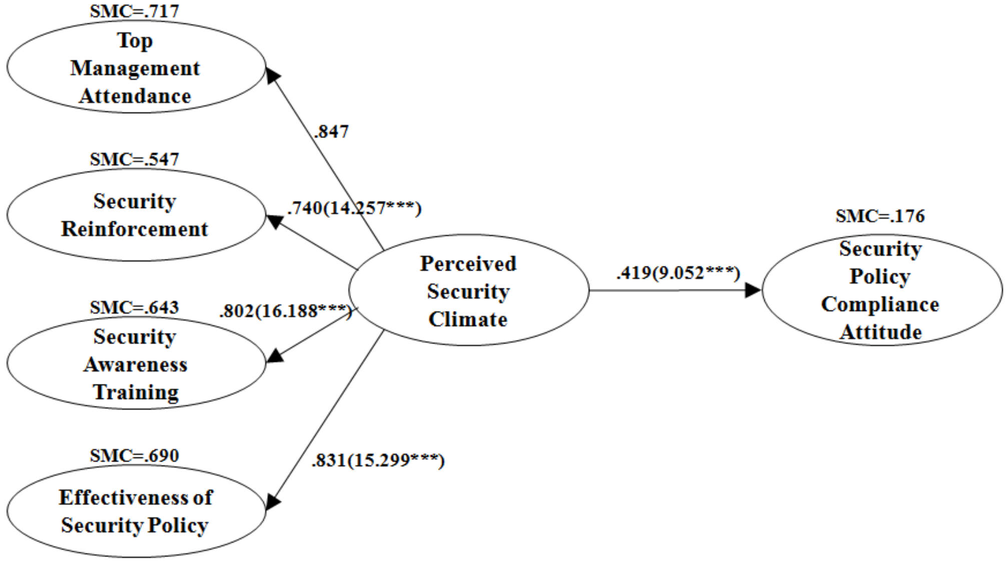
Table 2. Results of Model Comparison

Model #	χ^2	df	χ^2/df	NFI	NNFI	CFI	GFI	RMSEA
Model 1	5708.549	275	20.758	.627	.605	.638	.434	.185
Model 2	2924.016	275	10.633	.809	.808	.824	.684	.129
Model 3	1893.360	275	6.885	.876	.882	.892	.769	.101
Model 4	1886.477	271	6.961	.877	.881	.892	.770	.101

Target Coefficient (T)=0.998175(99.8%)
T value is calculated as F/T.(e.g., 1883.035/1886.477)

T lower limit is calculated as F/FU.(e.g., 1883.035/2924.016=0.643989)

To control for an explanation of results due to extraneous factors, several control variables are added. These variables are age, gender, years of working experience (Loe et al. 2000; Zhang et al. 2009), security training frequency, and computer use at work (Herath and Rao 2009a). In addition, we added techno-invasion and techno-complexity to control of effect of techno stress on opportunistic security behavior. Technostress can affect not only on task performance, but also organizational commitment (Herath and Rao 2009b; Ragu-Nathan et al. 2008; Tarafdar et al. 2007; Wang et al. 2008). Techno-invasion and techno-complexity, which are proposed by Ragu-Nathan et al.(2008), are very important factors in information security context. Techno-invasion refers to the invasive effect of ICTs in situations where employees can be reached anytime and feel the need to be constantly connected (Ragu-Nathan et al. 2008). When employees work outside the company, they may be less sensitive to importance of information security. Techno-complexity means situations where the complexity associated with ICTs leads users to feel inadequate with regard to their computer skills and forces them to spend time and effort in learning and understanding ICTs. Because security training programs in many organizations provide technical skill training, employees may feel more technological complexity. Unlike the other control variables, these two variables are measured using seven-point response scales ranging from strongly disagree to strongly agree.


SMC=.717
Top Management Attendance
.847
SMC=.547
Security Reinforcement
.740(14.257***)
SMC=.643
Security Awareness Training
.802(16.188***)
SMC=.690
Effectiveness of Security Policy
.831(15.299***)
Perceived Security Climate
.419(9.052***)
SMC=.176
Security Policy Compliance Attitude

χ^2 : 2446.934(df: 429), χ^2/df: 5.704, GFI: .769, NFI: .871, NNFI: .882, CFI: .891, RMSEA: .090

Figure 3. Performance Effects of Security Climate: Complementarity of the Four Dimensions

Analyses and Results

Measurement model

Exploratory factor analysis (EFA) is used to reveal the latent structure of the variables (see Table 3). The number of factors was extracted using Kaiser's criterion, that is, factors having eigenvalues greater that I were accepted in the solution. Based on the results of EFA and Cronbach' alpha, we assessed unidimensionality and internal consistency. We found 6 factors that have above 0.5 factor loadings (Campbell and Fiske; Hair et al. 2010). In addition, no substantial cross-loading, which exceeded 0.50, was observed between factors. These results support the unidimensionality of the scales in question. Internal consistency was assessed by using Cronbach's alpha. All scales employed in this study are higher than 0.7 that meant to strong reliability (Nunnally 1978).

Convergent validity was gauged via composite reliability (CR). CR scores equal to or greater than 0.7 are regarded as acceptable (Fornell and Larcker 1981; Segars 1997). As indicated in Table 3, the lowest CR score is 0.883, thereby demonstrating that all constructs have higher reliability.

We compared the square root of AVE score for each construct to test discriminant validity. In the AVE test of discriminant validity, the square root of AVE of a given construct should be larger than any correlation of the given construct with any other construct in the model. As shown in Table 4, all square root of AVEs are greater than each correlation of the given construct. Construct validity is demonstrated if (1) standardized loading estimates are higher than 0.5, (2) AVE are above 0.5 (convergent validity), (3) all square root of AVE are greater than the correlation coefficients between the constructs (discriminant validity), and (4) composite reliability are more than 0.7 (internal consistency or convergent validity) (Hair et al. 2010; Malhotra and Grover 1998). As indicated in Table 3, these conditions have been met, thereby demonstrating that the construct validity was obtained.

Common Method Bias Analysis

We assessed the extent of common method variance (CMV) with two tests: (a) Harman's one factor test (Podsakoff et al. 2003), (b) Lindell and Whitney (2001)'s market variable test (Podsakoff et al. 2003). The Harman's one-factor test on the items was performed to assess the manifestation of common method bias(Podsakoff and Organ 1986). If common method variance exists, most of the variables will load on a single facto which will account for the majority of covariance in the variables (Harrington 1997). The results of a principal components factor analysis (PCA) in this study show them fifteen factors with loadings along the lines of the constructs of interest and with an eigenvalue greater than 1. These factors account for 77.638% of the total variance. Because many factors emerged from the factor analysis and the first factor accounted for only 15.930% of the total variance, common methods bias does not appear to exist in the data (Joshi and Sharma 2004). Next, this study follows the common method variance model proposed by Lindell and Whitney (2001). To use this technique, a researcher should include at least one variable that expected on the basis of prior theory to be unrelated to the criterion variable. The current research interposed a marker variable, named "Outside Activity Preference."(α= 0.95). This variable was considered statistically independent of at least one of the research constructs. To use these equations for the investigation of the common method variance, the correlation matrix should include the partial and adjusted partial correlation between the predictor variables and the dependent variable. The research result shows that the correlation coefficient of CMV was smaller than the correlations between the dependent variable and predictor variables. In general, smaller correlation among the manifest variables is chosen as proxy for CMV (r = 0.060, T = 0.448). However, the post hoc approach has the potential to capitalize on chance factors (Malhotra et al. 2006). Therefore, according to Lindell and Whitney (2001), researchers can use the second-smallest positive correlation as a more conservative estimate of CMV (Malhotra et al. 2006). In addition, the reliability of the constructs (Cronbach's α) was very high, which indicated that the correlation between the constructs was not biased downward. All r^ values are also larger than r values. These results show that the constructs used in this study are not contaminated by CMV effects.

Structural Model

Before examining the structural model, seven common model-fit measures were used to assess the model's overall goodness-of-fit: χ2, Normed χ2, goodness–of-fit Index(GFI), root mean square error of approximation(RMSEA), normed fit index(NFI), nonnormed fit index(NNFI), and comparative fit index(CFI). As shown in Figure 4, two fit indices didn't surpass the recommended minimum threshold (χ2, GFI). χ2(2032.911; df:874; p-value:.000) statistic is overly sensitive to sample size (Meyers et al. 2006). Accordingly, χ2 can produce larger value even if hypothesized model is valid. For this reason, some researchers have suggested to use normed χ2. Normed χ2 on the order of 3:1 are associated with better-fitting model. In this study, this value is 2.32, demonstrating a good fit (Hair et al. 2010). GFI (0.861) is also sensitive to sample size due to the effect of N on sampling distributions (Hair et al. 2010). For this reason, we reviewed less sensitive model fit indices such as CFI, NNFI, and RMSEA. As shown in Figure 4, these fit indices are above the general recommended threshold of 0.9, 0.9, and 0.05 respectively (Hair et al. 2010).

The hypotheses were tested by examining the structural model. The test of the structural model includes estimating the path coefficients, which indicate the strength of the relationships between the independent and dependent variable. Results of structural model are provided in Figure 4. First, perceived security policy has a significant positive effect on security policy compliance attitude (β=0.411, p<0.001), thus supporting hypothesis H2. The result indicates that if importance of information security is perceived throughout the organization, each employee can be recognized that it is important to comply with organizational information security policy. Second, security policy compliance attitude has significant direct effect on opportunistic security behavior (β=-0.174, p<0.001), therefore H3 is supported. However, Not consistent with H1, perceived security climate was not found to have a significant effect on the opportunistic security behavior (β=0.022). The result implies that perceived security climate is related to security policy compliance attitude, rather than opportunistic security behavior directly. This is consistent with Ajzen and Fishbein's (1980) claim that behavior intention is determined by attitude towards the behavior. In addition, work experience and techno-invasion were found to have a significant effect on the opportunistic security behavior. That is, employees who have substantial work experience are less possible to comply with information security policy because of inconvenience. Furthermore, if employees feel that his or her life is invaded by various information technologies, they may not comply with organizational information security policy.

Table 3. The Assessment of the Measurement Models: Evidence of Convergent Validity

	Component						Average Variance Extracted	Composite Relaibillity	Cronbach's Alpha
	1	2	3	4	5	6			
SAT1	0.726	0.326	0.249	0.117	-0.054	0.084	0.736	0.951	0.956
SAT2	0.725	0.282	0.255	0.122	-0.104	0.232			
SAT3	0.821	0.253	0.214	0.108	-0.046	0.204			
SAT4	0.792	0.225	0.214	0.072	-0.027	0.254			
SAT5	0.839	0.277	0.242	0.115	0.041	0.079			
SAT6	0.841	0.28	0.254	0.127	0.067	0.06			
SAT7	0.79	0.222	0.298	0.154	0.025	0.086			
TMA1	0.204	0.813	0.235	0.157	-0.025	0.114	0.74	0.952	0.954
TMA 2	0.212	0.766	0.314	0.176	-0.06	0.14			
TMA 3	0.297	0.823	0.19	0.189	-0.006	0.087			
TMA 4	0.295	0.764	0.277	0.153	-0.022	0.159			
TMA 5	0.343	0.764	0.275	0.172	0.047	0.09			
TMA 6	0.322	0.753	0.251	0.13	0.002	0.18			
TMA7	0.273	0.7	0.213	0.141	-0.024	0.302			
ESP1	0.131	0.206	0.815	0.137	-0.005	0.129	0.646	0.936	0.94
ESP2	0.179	0.159	0.821	0.113	-0.016	0.175			
ESP3	0.28	0.276	0.747	0.199	0.013	0.174			
ESP4	0.277	0.161	0.777	0.071	-0.019	0.189			
ESP5	0.202	0.148	0.799	0.11	-0.043	0.146			
ESP6	0.279	0.351	0.658	0.124	-0.024	0.074			
ESP7	0.324	0.393	0.614	0.114	0.025	0.083			
ESP8	0.304	0.428	0.642	0.104	0	0.072			
SPCA1	0.151	0.243	0.116	0.776	-0.076	0.081	0.717	0.938	0.941
SPCA2	0.119	0.126	0.131	0.796	-0.026	0.063			
SPCA3	0.082	0.157	0.115	0.881	-0.086	0.049			
SPCA4	0.092	0.068	0.097	0.883	-0.054	0.023			
SPCA5	0.103	0.132	0.114	0.883	-0.109	0.027			
SPCA6	0.059	0.086	0.094	0.877	-0.116	0.037			
OSB1	-0.056	0.042	0.016	-0.137	0.72	0.1	0.691	0.917	0.924
OSB2	0.001	-0.047	0.017	-0.032	0.896	0.006			
OSB3	0.006	-0.033	-0.036	-0.073	0.9	0.025			
OSB4	0.001	0.005	-0.016	-0.083	0.92	-0.038			
OSB5	0.012	-0.023	-0.037	-0.066	0.918	-0.036			
SR1	0.263	0.311	0.265	0.127	0.032	0.705	0.716	0.883	0.879
SR2	0.201	0.25	0.284	0.119	0.045	0.806			
SR3	0.3	0.211	0.286	0.017	0.032	0.77			

a) Extraction Method: Principal Component Analysis.

b) Rotation Method: Varimax with Kaiser Normalization.

c) SAT=Security Awareness Training; TMA=Top Management Attention; ESP=Effectiveness of Security Policy; SPCA=Security Policy Compliance Attitude; OSB=Opportunistic Security Behavior; SR=Security Reinforcement

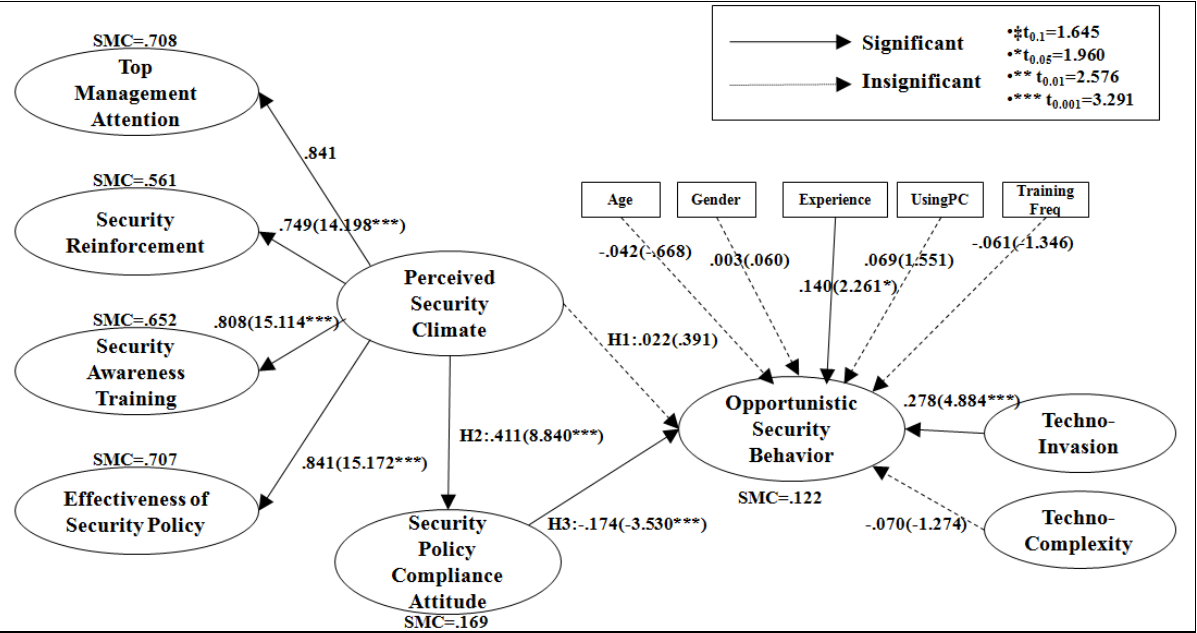
Table 4. Correlations of Latent Variables and Evidence of Discriminant Validity

	Mean	Std. Dev.	TMA	SR	SAT	ESP	SPCA	OSB
TMA	4.932	1.362	**0.86**					
SR	3.919	1.384	.584**	**0.846**				
SAT	4.348	1.400	.670**	.567**	**0.858**			
ESP	4.329	1.186	.665**	.593**	.641**	**0.804**		
SPCA	5.896	0.924	.390**	.251**	.319**	.344**	**0.847**	
OSB	3.717	1.388	-0.045	0.029	-0.036	-0.039	-.178**	**0.831**

a) **. Correlation is significant at the 0.01 level (2-tailed).

b) TMA=Top Management Attention; SR=Security Reinforcement; SAT=Security Awareness Training; ESP=Effectiveness of Security Policy; SPCA=Security Policy Compliance Attitude; OSB=Opportunistic Security Behavior

d) Diagonal values represent the square root of AVE.



Model Fit Indices: χ^2:2032.911; Normed χ^2:2.32; GFI:.861; RMSEA:.048; NFI:.916; NNFI:.946; CFI:.950

Figure 4. Results of Structural Model Analysis

Implication and Conclusion

The aim of this study is to empirically examine the effect of perceived security climate as organizational factor on opportunistic security behavior. The reason why this study focused on the relationship between organizational factor and personal factor is that organizational climate perceptions are crucial determinants of individual behavior. The results of this study are as followed. First, the perceived security climate does not impact opportunistic security behavior. This result suggests that opportunistic behavior cannot be reduced by enhancing perception of information security climate. However, it does not mean that perceived security climate cannot lead to security compliant behavior. Thus, further research is needed to explore the relationship between perceived security climate and security compliance behavior. Second, as expected, perceived security climate is significantly related to security policy compliance attitude. This finding indicates that perceived security climate can affect on opportunistic security behavior through security policy compliance attitude. Finally, security policy compliance attitude was found to be negatively related to opportunistic security behavior. That is, a positive attitude toward security behaviors increases employees' intention to perform those behaviors.

Our study also has several limitations. First, even if Harman's single factor test and market variable test did not identify common method variance as a problem, it still might have been. To ensure that it is not a problem and to prevent the consistency effect resulting from the same subject reporting both independent and dependent variables, future research might use more objective measures of the dependent variable. Second, the two antecedents explained 12.2% of the variance in opportunistic security behavior. In order to increase the explanatory power for opportunistic security behavior, other factors are needed to be considered in future research. Finally, since this study was carried out in Korea which has a very different culture than the US. Thus, it would be tough to generalize the results to American IS users.

Notwithstanding the limitations of this study the results provide valuable guidance for researchers and practitioners trying to identify the mechanisms by which they can improve information security within the organization. First, we conceptualized security climate as a multidimensional construct based on safety literature rather than unidimensional one. Security climate which is perceived by employees within the organization does not be formed by only one factor such as management practice. That is, each employee perceives security climate through interaction with various organizational conditions. This study suggests what factors are important to form the security climate. For practitioner, this study suggests a guideline to lead to security policy compliant behavior of employees. Second, in this study we considered the relationship between organizational factor and individual factors. From the organizational perspectives, the results of this study can be used for practical guideline to build an information security countermeasure.

References

Ajzen, I., and Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliff, NJ: Prentice-Hall.

Anderson, J.C. 1987. "An Approach for Confirmatory Measurement and Structural Equation Modeling of Organizational Properties," *Management Science* (33:4), pp 525-541.

Anderson, J. C., and Gerbing, D. W. 1988. "Structural Equation Modeling in Practice: A Review and Recommended Two-step Approach," *Psychological Bulletin* (103:3), pp. 411-423.

Ansari, M. A., Baumgartel, H., and Sullivan, G. 1982. "The Personal Orientation-Organizational Climate Fit and Managerial Success," *Human Relations* (35:12), pp. 1159-1178.

Babbie, E.R. 1990. *Survey Research Methods*, (2nd ed.) Wadsworth, Belmont, CA.

Bagozzi, R.P., Yi, Y., and Phillips, L.W. 1991. "Assessing Construct Validity in Organizational Research," *Administrative Science Quarterly* (36:3), pp 421-458.

Bentler, P. M., and Chou, C. P. 1987. "Practical Issues in Structural Equation Modeling," *Sociological Methods & Research* (16), pp. 78-117.

Boudreau, M-C., Gefen, D., and Straub, D. W. 2001. "Validation in Information Systems Research: A State-of-the-art Assessment," *MIS Quarterly* (25:1), pp. 1-16.

Burke, M. J., Borucki, C. C., and Hurley, A. E. 1992. "Reconceptualizing Psychological Climate in a Retail Service Environment: A Multiple-Stakeholder Perspective," *Journal of Applied Psychology* (77:5), pp. 717-729.

Byrne, B. M. 2010. Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming, 2nd ed, New York, NY: Routledge.

Campbell, D. T., and Fiske, D. W. 1959. "Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix," *Psychological Bulletin* (56:2), pp. 81-105.

Cardinali, R. 1995. "Safeguarding Databases: Basic Concepts Revisited," *Information Management & Computer Security* (3:1), pp. 30-37.

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

Chan, F., Lee, G. K., Lee, E. J., Kubota, C., and Allen, C. A. 2007. "Structural Equation Modeling in Rehabilitation Counseling Research," *Rehabilitation Counseling Bulletin* (51:1), pp. 53-66.

Chin, W. W. 1998. The Partial Least Squares Approach to Structural Equation Modeling, In G. A. Marcoulides (ed.) *Modern Methods for Business Research*, Mahwah, NJ: Lawrence Erlbaum Associates, pp. 295-336.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Denison, D. R. 1996. "What is the Difference Between Organizational Culture and Organizational Climate? A Narative's Point of View on a Decade of paradigm Wars," *Academy of Management Review* (21:3), pp. 619-654.

Ernst and Young. 2003. Global Information Security Survey, New York.

Ernst and Young. 2008. Global Information Security Survey, New York.

Foltz, C. B. 2000. The Impact of Deterrent Countermeasures upon Individual Intent to Commit Misuse: A Behavioral Approach, Unpublished doctoral dissertation, University of Arkansas, Fayetteville.\

Foltz, C. B., Schwager, P. H., and Anderson, J. E. 2008. "Why Users (Fail to) Read Computer Usage Policies," *Industrial Management & Data Systems* (108:6), pp. 701-712.

Fornell, C., and Larcker, D. E. 1981. "Evaluating Structural Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* (28), pp. 39-50.

Gefen, D., and Straub, D. 2005. "A Practical Guide To Factorial Validity Using PLS-Graph: Tutorial And Annotated Example," *Communications of the Association for Information Systems* (16), Article 5.

Goel, S., and Chengalur0Smith, I. N. 2010. "Metrics for Characterizing the Form of Security Policies," *Journal of Strategic Information Systems* (19), pp. 281-295.

Griffin, M. A., and Neal, A. 2000. "Perceptions of Safety at Work: A Framework for Linking Safety Climate to Safety Performance, Knowledge, and Motivation," *Journal of Occupational health Psychology* (5:3), pp. 347-358.

Hair, Jr. J. F., Black, W. C., Babin, B. J., and Anderson, R. E. 2010. *Multivariate Data Analysis*, 7th ed., Upper Saddle River, NJ: Prentice Hall.

Harrington, S. J. 1997. "A Test of a Person-Issue contingent Model of Ethical Decision Making in Organization," *Journal of Business Ethics* (16), pp. 363-375.

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

Herath, T., and Rao, H. R. 2009b. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-225.

James, L. A., and James, L. R. 1989. "Integrating Work Environment Perceptions: Explorations into the Measurement of Meaning," *Journal of Applied Psychology* (74:5), pp. 739-751.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:1), pp. 1-20.

Joshi, A. W., and Sharma, S. 2004. "Customer Knowledge Development: Antecedents and Impact on New Product Performance," *Journal of Marketing* (68), pp. 47-59.

King, W.R., and Sabherwal, R. 1992. "The Factors Affecting Strategic Information Systems Applications: An Empirical Assessment," *Information and Management* (23), pp 217-235.

Kline, R. B. 2005. Principles and Practice of Structural Equation Modeling, 2nd ed., Guilford Press.

Lindell, M. K., and Whitney, D. J. 2001. "Accounting for Common Method Variance in Cross-Sectional Research Designs," *Journal of Applied Psychology* (86:1), pp. 114-121.

Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), pp. 173-186.

Loe, T. W., Ferrell, L., and Mansfield, P. 2000. "A Review of Empirical Studies Assessing Ethical Decision Making in Business," *Journal of Business Ethics* (25), pp. 185-204.

Malhotra, M. K., and Grover, V. 1998. "An Assessment of Survey Research in POM: From Constructs to Theory," *Journal of Operations Management* (16), pp. 407-425.

Malhotra, N. K., Kim, S. S., and Patil, A. 2006. "Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research," *Management Science* (52:12), pp. 1865-1883.

Marsh, H.W., and Hocevar, D. 1985. "Application of Confirmatory Factor Analysis to the Study of Self-concept: First and Higher Order Factor Models and Their Invariance Across Groups," *Psychological Bulletin* (97:3), pp 562-582.

Meyers, L. S., Gamst, G., and Guarino, A. J. 2006. *Applied Multivariate Research: Design and Interpretation*, Thousand Oaks, California:SAGE Publications.

Neal, A., Griffin, M. A., and Hart, P. M. 2000. "The Impact of Organizational Climate on Safety Climate and Individual Behavior," *Safety Science* (34), pp. 99-109.

Neubaum, D. O., Mitchell, M. S., and Schminke, M. 2004. "Firm Newness, Entrepreneurial Orientation, and Ethical Climate," *Journal of Business Ethics* (52), pp. 335-347.

Nunnally, J. C. 1978. *Psychometric Theory*, 2nd ed., New York, McGraw-Hill.

Ocasio, W. 1997. "Towards an Attention-based View of the Firm," *Strategic Management Journal* (18:Summer Special Issue), pp 187-206.

Podsakoff, P. M., and Organ, D. W. 1986. "Self-Reports in Organizational Research: Problems and Prospects," *Journal of Management* (12:4), pp. 531-544.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y., and Podsakoff, N.P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp 879-903.

Preston, D. S., and Karahanna, E. 2009. "Antecedents of IS Strategic Alignment: A Nomological Network," *Information Systems Research* (20:2), pp. 159-179.

Purvis, R. L., Sambamurthy, V., and Zmud, R. W. 2001. "The Assimilation of Knowledge Platforms in Organizations: An Empirical Investigation," *Organization Science* (12:2), pp. 117-135.

Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., and Tu, Q. 2008. "The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation," *Information Systems Research* (19:4), pp. 417-433.

Richardson, R. 2007. "2007 CSI/FBI Computer Crime and Security Survey," Computer Security Institute.

Salancik, g. R., and Pfeffer, J. 1977. "An Examination of Need-Satisfaction Models of Job Attitudes," *Administrative Science Quarterly* (22:3), pp. 427-456.

Salancik, G. R., and Pfeffer, J. 1978. "A Social Information Processing Approach to Job Attitudes and Task Design," *Administrative Science Quarterly* (23:2), pp. 224-253.

Segars, A. 1997. "Assessing the Unidimensionality of Measurement: A Paradigm and Illustration within the Context of Information Systems Research," *Omega* (25:1), pp. 107-121.

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

Straub, D. W. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

Tagiuri, R., and Litwin, G. 1968. *Organizational Climate: Explorations of a Concept*, Boston: Harvard Business School.

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., and Ragu-Nathan, T. S. 2007. "The Impact of Technostress on Role Stress and Productivity," *Journal of Management Information Systems* (24:1), pp. 301-328.

Tanriverdi, H. 2005. "Information Technology Relatedness, Knowledge Management Capability, And Performance Of Multibusiness Firms1," *MIS Quarterly* (29:2), pp 311-334.

Tanriverdi, H. 2006. "Performance Effects of Information Technology Synergies in Multibusiness Firms," *MIS Quarterly* (30:1), pp. 57-77.

Treiblmaier, H., and Filzmoser, P. 2010. "Exploratory Factor Analysis: How Robust Methods Support the Detection of Hidden Multivariate Data Structures in IS Research," *Information & Management* (47), pp. 197-207.

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. 2005. "The Insider Threat to Information Systems and the Effectiveness of ISO17799," *Computers & Security* (24), pp. 472-484.

Venkatraman, N. 1990. "Performance Implications of Strategic Coalignment: A Methodological Perspective," *Journal of Management Studies* (27:1), pp 19-41.

Victor, B., and Cullen, J. B. 1988. "The Organizational Bases of Ethical Work Climates," *Administrative Science Quarterly* (33), pp. 101-125.

Wang, K., Shu, Q., and Tu, Q. 2008. "Technostress under Different Organizational Environments: An Empirical Investigation," *Computers in Human Behavior* (24), pp. 3002-3013.

Wimbush, J. C., and Shepard, J. M. 1994. "Toward an Understanding of Ethical Climate: Its Relationship to Ethical Behavior and Supervisory Influence," *Journal of Business Ethics* (13), pp. 637-647.

Wimbush, J. C., Shepard, J. M., and Markham, S. E. 1997. "An Empirical Examination of the Relationship between Ethical Climate and Ethical Behavior form Multiple Levels of Analysis," *Journal of Business Ethics* (16), pp. 1705-1716.

Wyld, D. C., and Jones, C. A. 1997. "The Importance of Context: The Ethical Work Climate Construct and Models of Ethical Decision Making- An Agenda for Research," *Journal of Business Ethics* (16), pp. 465-472.

Zhang, J., Reithel, B. J., and Li, H. 2009. "Impact of Perceived Technical Protection on Security Behaviors," *Information Management & Computer Security* (17:4), pp. 30-340.

Appendix A. Instrument items

All items were measured using seven-pint response scales anchored with strongly disagree (1) and strongly agree (7).

경영진의 관심 (Top Management Attention: TMA)	
TAM1.	우리 회사의 경영진들은 정보보안 정책을 중요하게 생각한다.
TAM2.	우리 회사의 경영진들은 회사의 정보보안 정책을 충분히 이해하고 있다.
TAM3.	우리 회사의 경영진들이 정보보안 정책을 준수할 것을 직원들에게 강조한다.
TAM4.	우리 회사의 경영진들은 업무 수행 시 정보보안 정책을 고려한다.
TAM5.	우리 회사는 정보자산을 보호하기 위해 높은(엄격한) 기준을 설정한다.
TAM6.	우리 회사의 다른 정책과 비교하였을 때, 정보보안 정책의 우선순위는 높다.
TAM7.	우리 회사의 경영진들은 정보 보안 정책의 준수가 기업에 잠재적인 이익을 가져다 줄 것이라 믿는다.
보안 강화 (Security Reinforcement: SR)	
SR1.	나의 상사는 정보보안 이슈에 관해 나뿐만 아니라 나의 동료와 함께 논의하는 편이다.
SR2	나의 상사는 내가 적절한 정보보안 활동을 하였을 때 나를 칭찬하는 편이다.
SR3.	나의 상사는 나에 대한 전반적인 성과를 평가 시 정보보안 준수를 핵심요인으로 생각한다.
보안 인지 교육 (Security Awareness Training: SAT)	
SAT1.	우리 조직은 사내 네트워크 접속 계정을 부여하기 전에 컴퓨터 사용자를 대상으로 적절한 보안 교육을 실시하고
SAT2.	우리 조직 내에서 정보 보안 인식에 관한 의사소통이 원활이 이루어지고 있다.
SAT3.	우리 조직에서는 직원들에게 인터넷의 위험성에 관한 교육이 적절히 이루어지고 있다.
SAT4.	우리 조직에서는 정보보안 인식을 고양하기 위해 다양한 의사소통 수단을 활용하고 있다.
SAT5.	우리 조직에서는 직원들에게 컴퓨터 보안 책임에 관한 교육을 하고 있다.
SAT6.	우리조직은 직원들의 컴퓨터 및 정보보안 이슈에 관한 인식수준을 높이기 위해 교육/훈련을 제공하고 있다.
SAT7.	우리 조직의 직원들은 정보기술에 대한 적절한 활용법을 교육받고 있다.
보안정책의 효과성 (Effectiveness of Security Policy: ESP)	
ESP1.	우리 회사의 보안 정책은 이해하기 쉽다.
ESP2.	우리 회사의 보안 정책은 읽기 쉽다.
ESP3.	우리 회사의 보안 정책은 각각의 조항들을 명확하게 제시하고 있다.
ESP4.	우리 회사의 보안 정책은 일반적인 단어와 구문들로 쓰여져 있다.
ESP5.	우리 회사의 보안 정책은 참고자료(혹은 타인의 도움) 없이도 이해할 수 있다.
ESP6.	우리 회사의 보안 정책은 정책위반에 따른 법적 문제로부터 조직을 보호한다.
ESP7.	우리 회사의 보안 정책은 정책위반에 따른 법적 파급효과를 구체적으로 명시하고 있다.
ESP8.	우리 회사의 보안 정책은 각각의 조항들을 빽빽하게 제시하고 있다.
보안정책 준수 태도 (Security Policy Compliance Attitude: SPCA)	
SPCA 1.	나에게 있어서, 우리 회사의 정보보안 정책을 지속적으로 따르는 것은 중요하다
SPCA 2.	나에게 있어서, 우리 회사의 정보보안 정책을 지속적으로 따르는 것은 중요하다
SPCA 3.	회사 내 나의 컴퓨터에서 정보 보안 침해 사고가 발생하지 않도록 스스로 예방하는 것은 중요하다
SPCA 4.	나에게 있어서, 우리 회사의 정보보안 정책을 지속적으로 따르는 것은 편리하다
SPCA 5.	회사 내 나의 컴퓨터에서 정보 보안 침해 사고가 발생하지 않도록 스스로 예방하는 것은 좋은 생각이다
SPCA 6.	나에게 있어서, 우리 회사의 정보보안 정책을 지속적으로 따르는 것은 바람직하다
기회주의적 보안 행위 (Opportunistic Security Behavior: OSB)	
OSB 1.	정보보안 정책을 따르지 않을 경우, 비용이 절감된다.
OSB 2.	정보보안 정책을 따르지 않을 경우, 업무 수행을 위한 시간이 절약된다.
OSB 3.	정보보안 정책을 따르지 않을 경우, 나의 업무 성과가 향상된다.
OSB 4.	정보보안 정책을 따르지 않을 경우, 나의 업무를 더욱더 빨리 끝낼 수 있다.
OSB 5.	정보보안 정책을 따르지 않을 경우, 정해진 시간 동안 더욱더 많은 일을 해낼 수 있다.
기술 침해 (Techno-Invasion: TI)	
TI1	나는 우리 회사가 사용하는 IT로 인해 가족들과 보내는 시간이 줄었다.
TI2	나는 우리 회사가 사용하는 IT로 인해 휴가중에도 내가 맡은 업무를 수행해야 한다.
TI3	나는 새로운 기술에 익숙해지기 위해 주말뿐 아니라 휴가도 희생해야 한다.
TI4	IT 기술로 인해 나의 사생활이 침해당하고 있다고 느낀다.
기술 복잡성 (Techno-Complexity: TC)	
TC1	나는 나의 업무를 만족스럽게 수행하기 위해 알아야 하는 IT기술에 대해 충분히 알지 못한다.
TC2	나는 새로운 기술을 이해하고 사용하는 데 오랜시간이 소요된다.
TC3	나의 기술적 역량을 향상시키기 위한 시간이 충분하지 않다.
TC4	나는 새로운 기술을 이해하고 사용하는 것이 나에게 있어서 너무 복잡하다는 것을 자주 느낀다.