Security Awareness: The First Step in Information Security Compliance Behavior

Inho Hwang, Robin Wakefield, Sanghyun Kim & Taeha Kim

JOURNAL OF COMPUTER INFORMATION SYSTEMS
https://doi.org/10.1080/08874417.2019.1650676

Taylor & Francis
Taylor & Francis Group

Security Awareness: The First Step in Information Security Compliance Behavior

Inho Hwang[a], Robin Wakefield[b], Sanghyun Kim[c], and Taeha Kim[d]

[a]Korea Polytechnic University, Siheung, South Korea; [b]Baylor University, Waco, TX, USA; [c]Kyungpook National University, Daegu, South Korea; [d]Chung-Ang University, Seoul, South Korea

ABSTRACT

In this study, we use the attentional phase of social learning theory to link workplace security-related experiences and observations to employees' security awareness. The responses of 398 organizational employees serve to test our research model using structural equational modeling with AMOS 22.0. The results show security awareness arises from both explicit and subjective security experiences in the workplace. Our respondents indicate knowledge of a physical system has little, if any, effect on security awareness. However, security education, policy, visibility and managerial security participation are important for producing security awareness. Furthermore, managerial participation strengthens the links between organizational security efforts and security awareness. We discuss the implications of our study for future security compliance research and practice.

KEYWORDS

Word; information security; awareness; social learning theory; compliance intention; security visibility; management participation; security policy

Introduction

Organizations invest significant portions of their budgets in reducing information security threats. According to International Data Corporation[1], global firms' spending on IT security is predicted to increase from 83.5 billion USD in 2017 to 119.9 billion USD by 2021. The budget for information security in the US has nearly doubled that of IT[2] in part because information security breaches that expose customers' private information often result in substantial financial losses and jeopardize the organization.[3] While security threats are both external and internal, internal threats are controllable due to technological advancements in security systems.[4] However, individuals remain the weakest link in internal security.[5]

Data breach reports[6] indicate insiders, such as office employees and engineers, cause 14% of all security incidents in organizations. Employees present a huge threat to information security[5,7] and their behavior is a significant factor in the ability of organizations to comply with IS security mandates. Most internal security incidents are a consequence of misuse actions including privilege abuse, unapproved hardware, embezzlement, ignorance of information security policies, and data mishandling. It is difficult to deter or prevent internal security threats because an organization cannot easily monitor or control employee behavior.[8] Thus, organizations invest heavily in securing physical information systems and creating security policies to create an environment of security *awareness*. The focus of our study is on internal organizational factors that contribute to employees' security awareness to facilitate their security compliance behavior.

In the information system security literature, information security awareness is defined as "a state where users in an organization are aware of – ideally committed to – their security mission."[9] (p31) Security awareness is expected to minimize security-related carelessness and maximize the effectiveness of security techniques and procedures. The emphasis on awareness has prompted information security researchers to explore various types of security-related awareness factors as determinants of security compliance behavior. These include technology awareness,[10] security countermeasure awareness,[11] threat awareness[12] and information security awareness.[13] Although these studies contribute to understanding how awareness, in its different forms, influences individuals' security compliance, they are limited in describing how organizational actions and attitudes contribute to employees' security awareness. Thus, our study attempts to identify and explore factors that create a posture of organizational security awareness. Our main research question is: What technical, managerial and social factors are favorable to the formation of employees' security awareness? Exploring the antecedents of security awareness and how they interact would benefit organizational security strategy and practice.

Information security researchers promote the importance of basic research to study phenomenon relevant to security practice.[14] Thus, we create a parsimonious research model and test it with the responses of 398 organizational employees from a variety of industries. We use the attentional phase of social learning theory (SLT) by Bandura[15] to explore how typical information security-related experiences and observations in the workplace motivate security awareness. SLT is applicable to security compliance research because it describes how a prescribed behavior is enacted following the processes of attention, memory, physical or intellectual capability, and motivation to perform.[16] Our study provides a richer understanding of *what* organizational practices contribute to employees' security awareness, and *how* they contribute, to motivate security compliance behavior.

CONTACT Sanghyun Kim ✉ ksh@knu.ac.kr School of Business Administration, Kyungpook National University, Daegu, South Korea

Background and theoretical frameworks

Information security awareness

Information security awareness is defined as *the focus of users' attention on security*, with the purpose of helping employees recognize security concerns and respond appropriately.[17] Information security awareness is not primarily about training, but rather the individual's receiving of information to better inform conscious decision-making. The construct labeled *awareness* emerged from the innovation diffusion process model that defines awareness as the extent to which potential users are conscious of an innovation and have a general perception of its attributes.[18] The awareness construct is conceptualized in the information security literature in several ways. The first is as *technology awareness*. Technology awareness is described as users' interest in, and knowledge of, technical issues and the strategies to solve technical problems. Dinev and Hu[10] used the theory of planned behavior, linking individuals' beliefs and behavior and the technology acceptance model (TAM). They found technology awareness positively influences users' attitudes and intentions toward using anti-spyware technology.

Security countermeasure awareness was conceptualized by D'Arcy et al.[19] as the knowledge of formal security policies and guidelines, security education and employee monitoring activities. They used general deterrence theory to explain how countermeasure awareness influences users' intentions to misuse systems. Their study shows security countermeasure awareness influences users' perceptions of the severity of sanctions, leading to lower inclination to misuse systems. Security countermeasure awareness is also found as an antecedent of the desktop security behavior of home users in a study based on protection motivation theory to clarify the motivation for individuals to take specific actions.[11]

Researchers have defined security awareness generally. For example, security awareness is defined as the awareness of threats,[20] the awareness or security policies and guidelines,[21] and the awareness of security policies and violations.[22] *Information security awareness*, specifically, is conceptualized as employees' awareness of their roles and responsibilities concerning information security[23] and as knowing and understanding the security rules and regulations as well as one's responsibility toward information security.[13] Bulgurcu et al.[13] incorporated the theory of planned behavior and rational choice theory that aggregates social behavior outcomes from individual actors' behaviors to examine the effects of information security awareness on beliefs and attitude. Findings indicate awareness influences employees' compliance attitude directly and indirectly via employee beliefs.

Information security researchers have also conceptualized information security awareness as a second-order construct formed by elements of protection motivation theory and technology threat avoidance theory to explain how IT users become involved in threat avoidance behavior.[11] The objective of their study is to increase the generalization of security awareness by identifying core dimensions applicable across security-related contexts. Hanus et al.[11] define security awareness as an aggregate of factors including the dimensions threat severity, susceptibility, self-efficacy, effectiveness and responsibility. In summation, security awareness, in some form, is a key factor in pro-security behavior. However, security awareness is a complex construct that does not conform to a uniform definition or application. Because our interest is in examining employees' workplace security experiences, we define *information security awareness* as the employee's conscious awareness of organizational security activities, security effort and security attitude.

Social learning theory

We rely on the principles of social learning theory (SLT) by Bandura[15] to link typical workplace security experiences to information security awareness. SLT, in general, is a theory of behavior replication. It posits the steps by which an individual obtains knowledge, learns, and reproduces behavior via direct observation of others performing a behavior within a context of social interactions and social experiences. Bandura[15] describes the full process of learning as noticing, remembering, acting and experiencing the consequences (reward or punishment) of an action. In SLT, noticing or attention occurs first in an exposure to a stimulus and is defined as the allocation of limited cognitive processing resources to the stimulus.[24] Attention indicates the activation of perceptual and cognitive processing of a stimulus, which then leads to retention (or remembering), prior to motor reproduction processes. Attributes of a stimulus include distinctiveness, affective valence, complexity, prevalence and functional value that influence what one notices. Importantly, attentional processes are more complex than observation. Attention means to 'attend to,' or a focused observation. It is described as selective observation or what one extracts from an observation, which is influenced by numerous personal and social variables.[15]

We base our study on the attentional facet of SLT because attention is necessary for observers to learn[16] and occurs prior to remembering and reproducing a behavior. Attention indicates the acquiring of information and knowledge conducive to creating an awareness of what one was not previously aware. In security research, security *awareness* is conceptualized as 'consciousness of,' 'knowledge of' or 'understanding of' security.[10,13] Thus, security awareness would occur in the attentional phase where the perceptual and cognitive processing of security-related stimuli happen and where security understanding would increase.

In the organization, formal and informal workplace security experiences focus employees' attention on information security through the dissemination of information by various means. Through exposure to security-related stimuli (e.g. programs, education, posters), employees 'attend to' and 'focus on' security. Importantly, one's attention is selective,[15] indicating individuals differ in what is placed as the focus of attention. Thus, employees exposed to the same security-related stimulus are likely to attend to different aspects of the stimulus. This would affect the perceptual and cognitive processing of the stimulus, the knowledge or understanding obtained, and the depth of awareness.

Workplace security awareness

Organizations provide a variety of workplace experiences to stimulate employees' awareness of information security. For example, information security policies and procedures are communicated formally and informally to educate employees regarding proper security practices and employees' roles in security. Formal security education and training programs are regarded as the vehicle for communicating the information needed by users to do their job.[17] Interestingly, awareness may be a past, present or future-oriented occurrence and not solely the conscious awareness of stimuli in a present experience. Thus, past security programs and training experiences as well as current experiences would contribute to employees' information security awareness.

However, individual experiences are subjective and processing results in individual interpretation of the experience.[25] This suggests that although a security-related exposure may be identical, the security knowledge gained by employees and their level of awareness is likely to differ. In fact, federal security awareness programs consist of numerous and varied activities to disseminate security information. For example, the NIST awareness program recommends exposing employees to promotional trinkets with security slogans as well as banners on computer screens to provide a variety of experiences that increase security consciousness.

Hypotheses

Information security education

Information security education often occurs through formal programs to communicate the information needed for employees to do their jobs.[26] Security education programs are specific events intended to emphasize and develop security knowledge, awareness and capabilities. Security education may include seminars, workshops, and drills to educate employees regarding an organization's information security environment, policies, rules, methods, and physical systems[19] and guide employees toward compliance.[27] Employees' awareness of security education was found to have a positive influence on organizations' security culture.[26]

The literature describes three levels of organizational security education.[28] The foundational level is awareness education in which the objective is the recognition of, and response to, organizational security concerns. An awareness program is typically an organizational-wide activity to disseminate security information. At the next level, security training programs function to develop security skills and competencies. The highest level of security education consists of specialized teaching and training to develop the expertise of information security professionals. Importantly, regardless of the level, the dissemination of security information begins the process in which an employee's attention is captured and awareness increases.

Noticing starts the learning process.[15] As employees experience security education, no matter the form, perceptual and cognitive processes attend to the information, and security awareness develops. Prior research acknowledges education and training are effective for employee knowledge formation and knowledge sharing,[29] security education leads to security awareness,[19] and organizational education and training are important to increase awareness levels. Thus, we hypothesize the following:

H1: Information Security Education is positively related to Information Security Awareness.

Information security policy

An information security policy is an organizational tool to define the parameters of information security and employee requirements for compliance. An information security policy is defined as rules and guidelines for the appropriate use of information security resources in an organization.[19] Security policies may include security objectives, an explanation of employees' compliance requirements, employees' responsibility for security behavior, and the processes for dealing with security incidents.[30] A security policy that corresponds to the security environment can secure the trust of the employees[31] and is, in effect, a legitimizing structure. Employees' trust in a security structure becomes an adequate response to external pressures, such as industry standards, or legal and regulatory requirements. Therefore, a security policy builds a structural framework to define the scope and procedures for security compliance. Furthermore, Hwang and Kim[32] claim a security policy may induce security behavior by presenting anticipated outcomes and consequences.

A security policy may mandate compliance for simple tasks, such as password changes, sign-out policies, reporting rules for information sharing, or information access rights. A security policy may also detail appropriate sanctions for non-compliant behavior. Researchers suggest that clear and concretely presented security policies raise security knowledge and skill levels for favorable compliance behavior[33] and an information security policy facilitates the effectiveness of security education programs.[32] An information security policy is generally the official source of the organization's security beliefs, goals, objectives, processes, procedures and mandated tasks. As a document detailing employees' security responsibilities and sanctions for non-compliance, a security policy would garner employee attention and stimulate security awareness. This leads to the following hypothesis:

H2: An Information Security Policy is positively related to Information Security Awareness.

Physical security system

A physical security system may be composed of numerous elements including physical entry or access controls to data centers and computer rooms, isolated delivery and loading areas, cable security, equipment maintenance, security of equipment off premises, and the secure disposal of equipment.[30] An enterprise security system enhances the security knowledge of managers[34] and is an important element to establish a security environment and minimize information abuse.[35] An effective information security system minimizes security incidents caused by insiders and sustains a stable information security level within an organization.[36]

In addition, a physical security system is an aspect of an organization's security strategy that increases employees' awareness of information security.[37] As employees implement physical security systems, their security-related activities are noticeable and others become aware of security.[38] Research also suggests that organizational security-related concerns are abated when physical security systems facilitate employees' security awareness.[32] In sum, prior research indicates that as various physical security systems are developed and implemented throughout an organization, employees notice and become more aware of information security. What prior research describes corresponds to the attentional phase of social learning theory in which a stimulus (e.g. physical security system) captures one's attention and creates awareness of the stimulus.[15] Thus, we expect employees' physical security system will positively influence their awareness of information security.

H3: A Physical Security System is positively related to Information Security Awareness.

Security visibility

IS researchers define technology visibility as the extent to which employees see others using the system in an organization.[39] However, visibility is not merely the observation of another using a system; visibility encompasses the degree or extent of system use by others. Rationally, the extent a phenomenon is observed or noticed would increase awareness of the phenomenon because memory becomes involved in the learning process.[15] We conceptualize security visibility as the *extent* to which employees observe information security processes, information security activities and security incidents in the organization.

Additionally, security compliance researchers find visibility activities contribute to employees' security awareness.[40] As security visibility increases, awareness is facilitated and the non-compliance behavior of employees decreases.[34] This indicates a positive relationship between the extent of security visibility, awareness and compliance. Creating awareness of organizational security goals may be as simple as displaying visualizations of goals and objectives, that is, increasing visibility. Similarly, the promotion or advertising of information security, security activities and security incidents would increase security visibility and stimulate awareness. The above discussion leads to the following hypothesis.

H4a: Security Visibility is positively related to Information Security Awareness.

Although security visibility is likely to have a significant impact on the information security awareness of organizational members, this relationship would be further strengthened as the organization continues to develop, modify and expand security policies and education programs. That is, as employees' knowledge and understanding of security policies increase and as involvement in security education activities continues and expands, the relationship between visibility and awareness is likely to strengthen. Puhakainen and Siponen[33] argue that a clear and concretely presented information security policy acts like a mast in the relationship between organizational security visibility and information security awareness. In other words, security policies and education will enhance the formation of awareness through augmenting security visibility. Researchers assert that codified information security policies must be accompanied by visibility to work effectively.[32]

Because we conceptualize security visibility as the extent of security-related observations, it is logical that employees' security awareness is hindered or expanded depending on the amount of exposure to policies and education. For example, an employee with basic security education would not have the security awareness of an employee involved in cybersecurity training and education, because exposure (security visibility) is limited. That is, the extent of security policy and education exposure would augment security awareness through its effect on visibility. Kim et al.[41] claim that education and training programs are a vehicle for communicating the information needed by users to do their job. In other words, without appropriate and ongoing information security training, employees' information, and thus awareness, remains narrow. In this respect, prior research (e.g. Nesheim and Gressgård[29]) acknowledges that education and training programs are not only effective for employee knowledge formation and knowledge sharing, but they also create potentially positive effects on information security awareness. Thus, we hypothesize the following moderation effects.

H4b: Security Policy positively moderates the relationship between Security Visibility and Information Security Awareness.

H4c: Security Education positively moderates the relationship between Security Visibility and Information Security Awareness.

Management security participation

When introducing new technologies in an organization, a key determinant of successful implementation is the ability of managers to reconfigure and adapt the technology to the characteristics of the organization.[42] This requires managers to actively engage in the development and implementation process. Researchers argue management involvement is critical to the success of organizational information security[43] and transformational organizational leaders directly influence security behavior.[44] Additionally, employee awareness and security culture are key policy elements in information security management.[45] Extant research supports managerial involvement for effective security outcomes.

Bandura[15] posits social learning results from casual or direct observation of the behavior performed by others. However, a noteworthy concept of social learning is some individuals in a group command greater attention and positively influence the effectiveness of modeled behavior.[15] Because managers possess greater social status, their involvement in security programs, procedures and protocols would capture the attention of subordinates. Thus, we expect employees' security awareness will be directly and positively influenced by management participation in security.

H5a: Management Security Participation is positively related to Information Security

Awareness

Because managerial participation in security is likely to attract the attention of employees and amplify security awareness, we expect managerial participation will also strengthen the relationships between security education, policy and visibility, with awareness. That is, other efforts to stimulate security awareness will be enhanced and strengthened as managerial participation becomes a focus of employee attention.

Prior research shows top management support is a significant moderator to strengthen the relationships between institutional influences and information security management assimilation.[45] Specifically, managerial participation plays a role in the successful implementation of information technology-related innovations. Dutta and McCrohan[46] claim that in cyber world, the voluntary participation of managers is a catalyst for enhancing information security awareness among organizational members. In contrast, when an organization implements security education and policies, the security consciousness of organizational members may be limited (e.g. Bulgurcu et al.[13]; Hwang and Kim[32]) to the information provided. However, Bandura[15] argues the positive impact of influential others on the learning process should not be underestimated. Thus, managerial participation should act as a catalyst to augment employees' security awareness.

We suggest that as employees 'attend to' or 'take notice of' organizational security education, security policies and security visibility, then security awareness increases. However, managerial participation in security is likely to strengthen the above relationships as employees observe the activities and actions of 'important' organizational personnel that heighten the level of 'noticing' (c.f., Bandura.[15]) As prior research suggests, the actions and attitudes of managers influence the attitudes and behaviors of employees, leading to the following moderation hypotheses:

H5b: Management Participation positively moderates the relationship between Security Education and Information Security Awareness.

H5c: Management Participation positively moderates the relationship between Security Policy and Information Security Awareness.

H5d: Management Participation positively moderates the relationship between Security Visibility and Information Security Awareness.

Security compliance

The Theory of Planned Behavior (TPB)[47] is one of the most widely used frameworks for the study of user behavior in the IS literature. TPB posits behavior is determined by intention to perform the behavior with intention motivated by salient beliefs that produce an attitude toward performing the behavior. The IS security literature defines intention as an employee's intent to protect the information and technology resources of the organization from potential security breaches,[13] or an employee's intention to protect an organization's information resources from internal and external threats.[48] When compliance intention is high, employees' security violations generally decrease,[4] supporting intentions as a direct antecedent of behavior.

Security awareness describes employees who are cognizant of security policies, rules, systems, and the organization's approach to security. In prior studies, technology awareness is a key determinant of positive attitudes toward protective technologies such as anti-virus software and firewalls,[10] such that users are more inclined to implement the protection. Research suggests employees' awareness is the causal antecedent of a target behavior,[49] such as the awareness of an organization's security mission that results in behavior to fulfill the mission.[38] Furthermore, activities related to security awareness (e.g. sharing, collaboration) increase security compliance intention in the information security policy compliance model.[50] Other studies support the positive relationship between employees' security awareness and the intention to implement security systems[37] and security policy compliance intentions.[13] Based on past findings, we hypothesize the following:

H6: Information Security Awareness is positively related to Security Compliance Intention.

Research model and method

Research model

The research model in Figure 1 diagrams the determinants of information security awareness and the hypothesized relationship between awareness and compliance intention. Security policy, physical security systems, management security participation, security education program, and security visibility are the antecedents of information security awareness. Awareness, in turn, has a positive influence on compliance intention. Prior studies suggest the inclusion of control variables (i.e. firm size and industry) to account for variance in the dependent variable, compliance intention.[51]

Construct measures

The survey items to measure each latent variable were adopted from prior studies. Measures for a security policy and a physical security system were developed based on D'Arcy et al.[19] and Lee et al.[36], respectively. Security education, management security participation, and security visibility were adopted from D'Arcy et al.[19] and Kankanhalli, et al.[52], respectively. Items to measure employees' security awareness were derived from Kim et al.[41] and compliance intention items originated with Herath and Rao.[53] All items were modified to reflect the information security context of our study. After modifying the items, 10 employees at organizations implementing information security and 10 scholars in information security reviewed the items to verify face

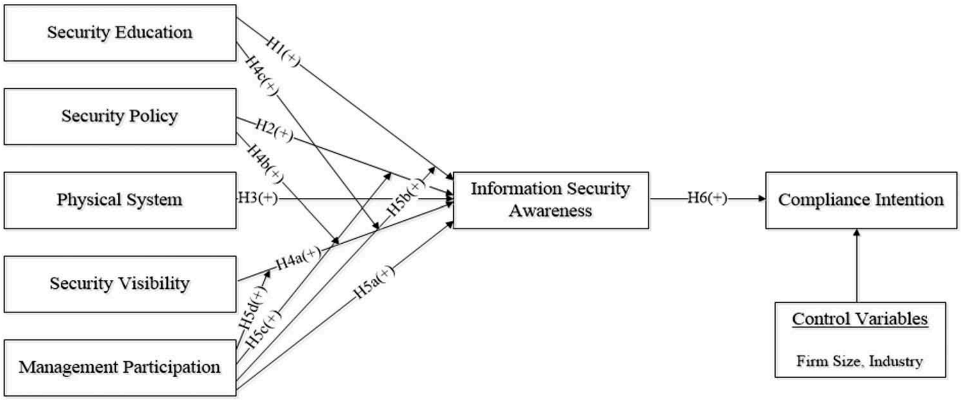

Figure 1. Research Model and Proposed Hypotheses.

validity. Subsequent modification of some items was required to increase clarity and face validity. All items were measured using a 7-point Likert-type scale ranging from “strongly disagree” (1) to “strongly agree” (7).

Data collection and sample

Data collection was outsourced to a professional research firm, which used on-site, online, and telephone surveys to deliver a total of 3,000 surveys to a random sample of companies from three sources: the Korea Composite Stock Price Index, the Korean Securities Dealers’ Automated Quotation, and the Korea Foreign Company Association. The surveyed firms were diverse in size, industry and location to increase generalizability. A total of 429 responses were collected and 31 were excluded due to missing data. A final sample size of 398 usable responses were used to test the research model. The demographic characteristics of the 398 respondents are presented in Table 1. Respondents consisted of 221 males (55.5%) and 177 females (44.5%). Respondents’ ages show about 65 percent under the age of 50 and 35 percent over the age of 50. Most respondents were from finance/banking (34.4%) and the IT industry (22.9%), followed by logistics/transportation (22.1%) and manufacturing (15.8%) industries.

All respondents indicated knowledge of information security policies, security systems and other security procedures at their companies. Regarding information security actions, the respondents indicated most of their firms (86.9%) were cautious about using and setting system passwords, and 72.4% of firms updated software and maintained PCs on a regular basis. Other information security actions included locking PCs or other systems and devices (68.1%), providing continuous security-related education and training programs (58.8%), and using caution with email (50.8%).

Table 1. Respondent demographics.

Demographic Categories		Frequency	%
Gender	Male	221	55.5
	Female	177	44.5
Age	< 40 years	133	33.4
	41–50 years	126	31.7
	51–60 years	91	22.9
	> 60 years	48	12.1
Type of Industry	IT	91	22.9
	Manufacturing	63	15.8
	Logistics/transportation	88	22.1
	Finance/banking	137	34.4
	Other	19	4.8
Job Tenure	< 10 years	73	18.3
	11–15 years	81	20.4
	16–20 years	69	17.3
	21–25 years	103	25.9
	> 25 years	72	18.1
Actions Related to Information Security (Multiple Responses)	Caution about using email	202	50.8
	Caution about using and setting password	346	86.9
	Locking PC or other systems and devices	271	68.1
	Updating software and maintaining PC	288	72.4
	Participating in a security-related education and training program	234	58.8
	Other	37	9.3
Total		398	100.0

Results

Validation of the measurement model

Before testing the research model, the fitness between the characteristics of the measurement model and that of the dataset was evaluated. Three validation tests – overall fitness, internal consistency, and convergent and discriminant validity – were conducted using AMOS 22.0. An acceptable fit is indicated when the GFI, NFI, and CFI exceed 0.90,[54] the AGFI exceeds 0.8, and the RMSEA is below 0.05.[55] As shown in Table 2, all fit indices exceed their cutoff values indicating acceptable model fit.

We evaluated the reliability and convergent validity of the 28 measurement items and a summary of results is shown in Table 3. Cronbach’s alpha for each of the latent variables ranged from 0.84 to 0.94, higher than the recommended threshold of 0.70[56] for internal consistency. One item (sv4) measuring security visibility was deleted due to its negative effect on reliability. We evaluated the convergent validity of the measurement model using confirmatory factor analysis. Each individual factor loading was greater than 0.7 on its associated construct and composite reliability values were greater than the 0.7 threshold.[57] The results indicate our items demonstrate acceptable reliability and validity.

Table 2. Measurement model fit indices.

Fit indexes	χ2/df	GFI	AGFI	CFI	NFI	RMSEA
Value in this study	1.98	0.93	0.90	0.94	0.94	0.04
Recommended value	≤ 3	≥ 0.9	≥ 0.8	≥ 0.9	≥ 0.9	≤ 0.05

Table 3. Construct validity and reliability.

Constructs	Items	Mean	Std. Dev.	Factor Loading	Cronbach's Alpha	CR
Security Policy	sp1	5.6	0.73	0.732	0.90	0.83
	sp2			0.750		
	sp3			0.767		
	sp4			0.720		
Physical Security Systems	pss1	5.5	0.91	0.757	0.87	0.77
	pss2			0.722		
	pss3			0.731		
Management Security Participation	msp1	5.6	0.68	0.860	0.89	0.89
	msp2			0.843		
	msp3			0.817		
	msp4			0.774		
Security Education Program	sep1	5.4	1.05	0.738	0.90	0.83
	sep2			0.790		
	sep3			0.726		
	sep4			0.701		
Security Visibility	sv1	5.7	0.90	0.808	0.84	0.83
	sv2			0.755		
	sv3			0.802		
	sv4			Dropped		
Security Awareness	sa1	6.1	1.03	0.781	0.89	0.87
	sa2			0.800		
	sa3			0.825		
	sa4			0.749		
Compliance Intention	ci1	6.1	0.96	0.860	0.94	0.92
	ci2			0.859		
	ci3			0.864		
	ci4			0.789		
	ci5			0.769		

Note: CR: Composite Reliability

Table 4. Correlation among the latent constructs.

Construct	1	2	3	4	5	6	7
1. Security Policy	**0.742**						
2. Physical Security System	0.403	**0.737**					
3. Management Security Participation	0.352	0.404	**0.824**				
4. Security Education Program	0.236	0.337	0.265	**0.739**			
5. Security Visibility	0.317	0.422	0.237	0.291	**0.789**		
6. Security Awareness	0.288	0.296	0.361	0.398	0.254	**0.789**	
7. Compliance Intention	0.292	0.200	0.407	0.266	0.352	0.518	**0.829**

Note: Bold numbers on the diagonal are the square root of the AVE

Table 5. Fit indexes of the structural model.

Fit indexes	χ2/df	GFI	AGFI	CFI	NFI	RMSEA
Value in this study	1.89	0.94	0.91	0.94	0.96	0.04
Recommended value	≤ 3	≥ 0.9	≥ 0.8	≥ 0.9	≥ 0.9	≤ 0.05

We compared the square root of the average variance extracted (AVE) with the variable correlations to evaluate the discriminant validity of the constructs as shown in Table 4. The bolded values on the diagonal represent the square root of the AVE and each exceeds the horizontal and vertical correlation values, supporting discriminant validity.

Structural model assessment

The structural model was tested with AMOS 22.0 to evaluate the hypothesized relationships among the constructs. The fit indices shown in Table 5 indicate the data fit well to the structural model. We first tested the hypothesized direct effects in the research model. Then, moderation effects were tested using the method proposed by Carte and Russell[58], Moderated Multiple Regression (MMR). Figure 2 presents the results of the direct effects, and Table 6 summarizes the results of the hypotheses tests of the direct effects.

The structural equation results indicate H1 and H2 are supported. Information security education H1 (β = 0.395, p < .001) and information security policy H2 (β = 0.324, p < .001) are significantly related to information security awareness. Unexpectedly, H3 is not supported (β = 0.083, p > .05). A physical security system, as measured by our items, is not significantly related to security awareness. Hypotheses H4a, H5a and H6 are likewise supported by our data. Security visibility is significantly related to security awareness (H4a; β = 0.233, p < .001) as is management security participation (H5a, β = 0.408, p < .001). Information security awareness, in turn, is positively related to compliance intentions supporting H6 (β = 0.513, p < .001). Overall, the antecedents explain about 58 percent of the variance in information security awareness and the model explains 26 percent of the variance in compliance intention.

Assessment of moderating effects

The MMR approach was applied to test the three moderators (security policy, security education and management security participation). The MMR verifies the moderating effect with the F-value by evaluating the R^2 difference between the model with the interaction effect and the model without the interaction effect. For example, H4b proposes security policy will moderate the relationship between security visibility and security awareness. We first tested the direct effects of the antecedents on security awareness. The results as shown in Figure 3a yield an R_a^2 of .227. When the interaction term (visibility * security policy) is included in Figure 3b, the R_m^2 increases to .239. If the ΔR^2, which is the difference between the R_a^2 value and the R_m^2 value, is sufficiently large, a moderating effect is indicated. The F statistic value was calculated with the following equation to account for the number of predicted variables and sample size in two models.

$$F_{(df_m - df_a, N - df_m - 1)} = \frac{\Delta R^2 (N - df_m - 1)}{(1 - R_m^2)(df_m - df_a)}$$

For H4b, the F-value result of 6.213 (significant at p < .05) was obtained by calculating the difference in the two R^2 values (ΔR^2 = 0.012), number of preceding variables (df_a = 2, df_m = 3), and

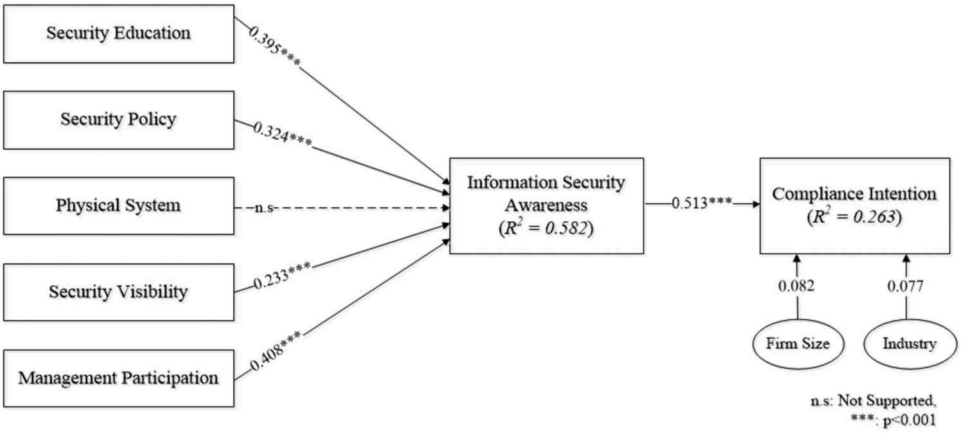

Figure 2. Direct Effects Results.

Table 6. Summary of Hypothesis Tests (Direct Effects).

Hypothesis	Path	*Std. β*	t-value	Result
H1	Security Education → Security Awareness	0.395[a]	5.851	Supported
H2	Security Policy → Security Awareness	0.324[a]	4.865	Supported
H3	Physical System → Security Awareness	0.083	1.001	Not Supported
H4a	Security Visibility → Security Awareness	0.233[a]	3.681	Supported
H5a	Management Participation → Security Awareness	0.408[a]	6.572	Supported
H6	Security Awareness → Compliance Intention	0.513[a]	8.759	Supported

[a]p < .001

sample size (*N* = *398*). H4b is supported and the other moderating effects were tested similarly. Table 7 summarizes the analysis of the moderating effects.

Discussion

In the information security literature, *awareness* is a key factor in the success or failure of compliant security behavior (e.g. Bulgurcu et al.[13]) Hence, the practical implementation of an organizational security strategy to achieve security compliance would require knowledge of the factors related to security awareness and how those factors might interact. Yet, little is known of the variables directly contributing to employees' awareness. Our study addresses this deficiency to further the understanding of how employees' security compliance may be motivated and to encourage the identification and refinement of awareness antecedents.

The results of analyses indicate information security awareness occurs when employees are exposed to security education, security policy, security visibility and management security participation. Interestingly, a physical security system was not significantly related to awareness. We surmise security hardware, software and other means of information access prevention are not observed by employees if they exist in the background, unnoticed (e.g. Symantec security software, off-premise hardware), may not be associated with information security (e.g. locked computer room) or inaccessible to employees (e.g., data center). Logically, awareness would occur with the explicit association of physical security system hardware, software, and procedures with the attainment of security knowledge. Additionally, our items measuring a physical security system focused on perceptions of organizational investment rather than specific information security components. Nonetheless, we believe this result is informative. It suggests a security-related stimulus that is vague or elusive in its relationship to information security may not be adequate to elicit awareness.

However, employees' security awareness does respond to stimuli related to security education, security policy, security visibility and managerial security participation. These factors capture attention, focus attention on security, increase security knowledge and facilitate awareness. For example, when employees are exposed to formal security education, their attention is drawn to and focused on the stimuli presented – security processes, procedures and behaviors. "People cannot learn much by observation unless they attend to, and perceive accurately, the significant features of the modeled behavior."[15] (p. 24) According to SLT, individual's attentional processes determine what is selected as the focus from observations or

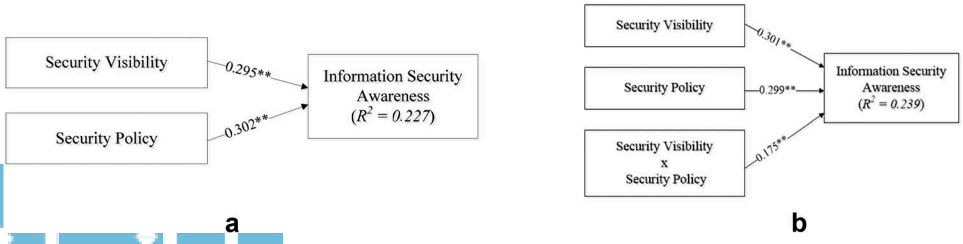
Security Visibility
Security Policy
0.295**
0.302**
Information Security Awareness (R^2 = 0.227)
a
Security Visibility
Security Policy
Security Visibility x Security Policy
0.301**
0.299**
0.175**
Information Security Awareness (R^2 = 0.239)
b

Figure 3. (a). Direct effect Model. (b). Interaction Model (H4b).

Table 7. Summary of Moderation Effects.

Hypothesis/ Path	Model	Path (Std. β/t-value)	R^2	□R^2	F-value	Result
H4b: SV → SA ↑ SP	No Interaction	SV → SA (β = 0.295/4.883**) SP → SA (β = 0.302/5.125**)	0.227	0.012	6.213*	Supported
	Interaction	SV → SA (β = 0.301/4.869**) SP → SA (β = 0.299/4.008**) SV x SP → SA (β = 0.175/3.166**)	0.239			
H4c: SV → SA ↑ SEdu	No Interaction	SV → SA (β = 0.276/3.654**) SEdu → SA (β = 0.397/5.223**)	0.234	0.003	1.549	Not Supported
	Interaction	SV → SA (β = 0.265/4.207**) SEdu → SA (β = 0.376/4.752**) SV x SEdu → SA (β = 0.183/2.117*)	0.237			
H5b: SEdu → SA ↑ MSP	No Interaction	SEdu → SA (β = 0.411/6.169**) MSP → SA (β = 0.367/5.930**)	0.302	0.039	23.317**	Supported
	Interaction	SEdu → SA (β = 0.406/5.863**) MSP → SA (β = 0.370/4.654**) SEdu x MSP → SA (β = 0.197/2.200*)	0.341			
H5c: SP → SA ↑ MSP	No Interaction	SP → SA (β = 0.329/4.100**) MSP → SA (β = 0.426/6.753**)	0.290	0.024	13.784**	Supported
	Interaction	SP → SA (β = 0.331/5.217**) MSP → SA (β = 0.399/5.872**) SP x MSP → SA (β = 0.158/2.961**)	0.329			
H5d: SV → SA ↑ MSP	No Interaction	SV → SA (β = 0.316/5.274**) MSP → SA (β = 0.415/6.669**)	0.272	0.036	20.497**	Supported
	Interaction	SV → SA (β = 0.310/4.997**) MSP → SA (β = 0.411/6.230**) SV x MSP → SA (β = 0.209/3.257**)	0.308			

Note: SV: Security Visibility, SA: Security Awareness, SP: Security Policy, SEdu: Security Education, MSP: Management Security Participation

exposures. While our study does not delineate the focus of individuals' attention for each security factor, we submit that security education, policy, visibility and management participation are appropriate and important antecedents of awareness.

In addition to the direct effects of our constructs on security awareness, we hypothesized five moderation effects. Four of the moderation effects were significant. Security education did not moderate the relationship between visibility and awareness (H4c) while security policy is a significant moderator of this relationship (H4b). The moderation effect of H4b suggests a security policy strengthens the relationship between visibility and awareness. A security policy is a tangible document emphasizing information security. As such, it appears to augment the importance of security visibility to the formation of awareness. Similarly, management security participation strengthens the effect of visibility on awareness (H5d). We suggest management participation may tap into the 'distinctiveness' attribute of a stimulus and thereby provoke greater attention. That is, a manager's participation is likely to garner greater attention by an employee due to his/her status compared to another employee's participation. Hence, managers' participation is likely to reinforce the association between security visibility and awareness.

The value of influential others in the workplace to motivate security awareness, and thus compliance behavior, represents an actionable outcome for security practice. Not only does management participation directly influence employees' security awareness, it also reinforces two other direct effects in addition to H5d discussed above. Management participation augments the influence of security education (H5b) and security policy (H5c) on respondents' security awareness. When managers are observed engaging in information security the effect of other relationships on awareness become stronger. This suggests organizational members higher in status and influence should be regarded as valuable components of employees' security-related experiences. They aid in the heightening of security awareness. These members are likely to impact employees' perceptual and cognitive processes during exposure to security efforts and activities, with the effect of strengthening awareness.

Despite large investments in information security, security incidents continue to grow and organizations are allocating more resources toward advanced security systems, often requiring compliance behavior to minimize information security threats and incidents.[59] Bandura[15] purports the failure to perform a modeled behavior may result from several factors including irrelevant observations, inadequate memory representations and failure to retain knowledge, among others. Thus, when a behavior is performed, it is likely that prior observations were relevant, memory sufficiently represented the stimulus and knowledge was retained. In other words, the individual has the necessary awareness to motivate behavior. Research notes that when security campaigns offer weak content and ad hoc initiatives sustainable behavioral change is not produced[59]; awareness is low. We suggest when employees' information security experiences are relevant and their memory retains the security focus of the experience and produces security knowledge, then the awareness that motivates compliance results. Interestingly, individuals do not enact all they learn but are more likely to perform behaviors that result in outcomes they value.[15] Hence, it would be useful for information security researchers to study the value propositions associated with compliant security behavior.

Our study falls into the category of basic information security research[14] and is motivated by the desire to study security issues with outcomes relevant for security practice. We apply SLT to the security compliance issue to emphasize an effective, actionable way to improve compliance behavior by focusing on employees' security awareness. Our study does not explicate the cognitive or perceptual mechanisms by which awareness is achieved, nor does it pursue how employees retain and replicate modeled security behaviors. We entrust these inquiries to future security research. Our overall objective is to emphasize that understanding *how* to motivate security compliance proceeds from first identifying *what* information security efforts, currently in practice, capture employees' attention and create awareness. Additionally, our model is not comprehensive of all employees' security-related experiences and observations. For example, past research finds computer monitoring contributes to awareness[60] as well as a positive attitude toward security compliance.[61] Future research should include and examine the effects of other typical security experiences and exposures in the workplace.

Implications for research and practice

Organizations may rely primarily on technical and physical tools to address information security management,[37] without understanding the role of non-technical means to create awareness and induce compliance. Prior information security research endorses awareness as fundamental to security compliance and SLT maintains attention is the first stage in the process for motivating behavior. Our study leads us to conclude the identification of the security stimuli capturing the attentional processes of employees is a critical first step in security compliance. Information security compliance behavior is an ongoing problem that requires fresh approaches to improve the information security effect rate and security practice.[14] We suggest a research focus on security stimuli and the attributes attracting and holding employees' and attention will yield relevant and actionable insights for information security practice.

However, employees' attentional processes are complex. Attention is a set of processes in which the brain selects elements of incoming sensory information for higher level processing.[62] At a basic level, attention consists of observing and noticing; however, selective focusing implies individual variation related to stimulus attributes that are processed further. Selective focusing in observational learning indicates difficulty in clarifying why, when and how individuals' security observations are symbolically coded, organized, and rehearsed. While challenging, such research would have positive impact on information security practice.

The rise of damaging information security events by organizational insiders, whether intentional or not, confirms the need for research examining the cognitive processing of security stimuli by employees. How do employees take in and process different types of security experiences? What are the attributes of security stimuli that capture employees' security focus? Without a full understanding of employee compliance motivations, the immediate reaction to security incidents may include additional resource allocation to technology or process improvements rather than people-oriented initiatives. While the implementation of improved security processes and technology will continue, employees will also continue in their role as the weakest link. Huge strides in information security are possible when researchers clarify how to strengthen the employee link to compliance. Our study implies the activation of attentional processes through stimulating employees' sensory and arousal levels (i.e. perception and cognition of security stimuli) is a valid pursuit.

Limitations

Our study has several limitations that should be addressed in future research. First, this study is limited by the analysis of employees' perceptions rather than actual behavior. However, information security awareness is a perception that would be salient among employees in most organizations due to the serious consequences of information security failure. While there are limitations to behavioral intentions as a proxy for actual behavior, this does not undermine our objective of identifying determinants of awareness. Future researchers could use controlled lab experiments to measure compliance intentions and actual behavior.

Additionally, while our model explains 58 percent of the variance in security awareness, the identification of other important antecedents of awareness would be valuable. This would increase the understanding of what constitutes effective organizational security experiences. Because we use cross-sectional data, our study presents a snapshot of employee perceptions and intentions that may differ over time and location. Additional research in this area might follow a longitudinal approach and gather data from a variety of countries to increase generalizability.

Conclusion

Our research model demonstrates employees' information security awareness arises from both explicit and subjective security-related experiences in the workplace. However, not all security experiences are likely to contribute to security awareness. Our respondents identified several factors positively contributing to their information security awareness including education, policy, security visibility and management participation. Interestingly, managerial security participation has the strongest relationship to employees' awareness and it also strengthens the links of other organizational factors with security awareness. For the benefit of information security practice, we encourage future research that drills-down to the attribute-level of employees' workplace security observations and experiences to discover *what* captures employees' attention and *why*.

References

1. IDC. Worldwide Semiannual Security Spending Guide; 2016.
2. Cybersecurity Ventures. Q3 Cybersecurity Market Report; 2015.
3. Hwang I, Cha O. Examining technostress creators and role stress as potential threats to employees' information security compliance. Comput Hum Behav. 2018;81:282–93. doi:10.1016/j.chb.2017.12.022.
4. Loch K, Carr H, Warkentin M. Threats to information systems: today's reality, yesterday's understanding. MIS Q. 1992;16 (2):173–86. doi:10.2307/249574.
5. Lowry P, Moody G. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. Inform Syst J. 2015;25:433–63. doi:10.1111/isj.12043.
6. Verizon. Verizon 2016 Data Breach Investigations Report; 2016.
7. Van Niekerk J, Von Solms R. Information security culture: a management perspective. Comput Secur. 2010;29:476–86. doi:10.1016/j.cose.2009.10.005.
8. West R. The psychology of security. Commun ACM. 2008;51 (4):34–40. doi:10.1145/1330311.
9. Siponen M. A conceptual foundation for organizational information security awareness. Inf Manage Comput Secur. 2000;8 (1):31–41. doi:10.1108/09685220010371394.
10. Dinev T, Hu Q. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. J Assoc Inf Syst. 2007;8:386–408.
11. Hanus B, Windsor J, Wu Y. Definition and multidimensionality of security awareness: close encounters of the second order. SIGMIS Database. 2018;49(18):103–33. doi:10.1145/3210530.3210538.
12. Chen X, Chen L, Wu D. Factors that influence employees' security policy compliance: an awareness-motivation-capability perspective. J Comput Inform Syst. 2018;58(4):312–24. doi:10.1080/08874417.2016.1258679.
13. Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 2010;34(3):523–48. doi:10.2307/25750690.
14. Siponen M, Baskerville R. Intervention effect rates as a path to research relevance: information systems security example. J Assoc Inf Syst. 2018;19(4):247–65. doi:10.17705/1jais.00491.
15. Bandura A. Social learning theory. New York (NY): General Learning Press; 1977.
16. Bandura A. Observational learning. In: Byrne JH, editor. Learning and memory. 2nd ed. New York (NY): Macmillan Reference USA; 2004. p. 482–484.
17. Newhouse W, Keith S, Scribner B, Witte G National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST Special Publication 800–181; 2017 [accessed 2019 Feb 14]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
18. Rogers E. Diffusion of innovations. New York (NY): The Free Press; 1995.
19. D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inform Syst Res. 2009;20(1):79–98. doi:10.1287/isre.1070.0160.
20. Rhee HS, Ryu YU, Kim CT. Unrealistic optimism on information security management. Comput Secur. 2012;31(2):221–32. doi:10.1016/j.cose.2011.12.001.
21. Pahnila S, Siponen M, Mahmood A Employees' behavior towards IS security policy compliance. 40th Annual Hawaii International Conference on System Sciences; New York (NY); 2007.
22. Baker WH, Walla Ce L. Is information security under control? Investigating quality in information security management. IEEE Secur Priv. 2007;5(1):36–44. doi:10.1109/MSP.2007.11.
23. Kritzinger E, Smith E. Information security management: an information security retrieval and awareness model for industry. Comput Secur. 2008;27(5–6):224–31. doi:10.1016/j.cose.2008.05.006.
24. Anderson JR. Cognitive psychology and its implications, 6th ed. New York (NY): Worth Publishers; 2004.
25. Posey C, Roberts T, Lowry P. The impact of organizational commitment on insiders' motivation to protect organizational information assets. J Manage Inform Syst. 2015;32(4):179–214. doi:10.1080/07421222.2015.1138374.
26. Chen Y, Ramamurthy K, Wen KW. Impacts of comprehensive information security programs on security culture. J Comput Inform Syst. 2015;55(3):11–19. doi:10.1080/08874417.2015.11645767.
27. Straub DW. R. Coping with systems risk: security planning models for management decision making. MIS Q. 1998;22(4):441–64. doi:10.2307/249551.
28. Tsohou A, Kar Yda M, Kokolakis S. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. Compt Secur. 2015;52:128–41. doi:10.1016/j.cose.2015.04.006.
29. Nesheim T, G Ressgård LJ. Knowledge sharing in a complex organization: antecedents and safety effects. Safety Sci. 2014;62:28–36. doi:10.1016/j.ssci.2013.07.018.
30. Kwok L, Longl Ey D. Information security management and modeling. Inf Manage Comput Secur. 1999;7(1):30–40. doi:10.1108/09685229910255179.
31. Von Solms R. Information security management: why standards are important. Inf Manage Comput Secur. 1999;7(1):50–58. doi:10.1108/09685229910255223.
32. Hwang I, Kim D. The effect of organizational information security environment on the compliance intention of employee. J Inform Syst. 2016;25(2):51–77. doi:10.5859/KAIS.2016.25.2.51.
33. Puhakainen P, Siponen M. Improving employees' compliance through information systems security training: an action research study. MIS Q. 2010;34(4):757–78. doi:10.2307/25750704.

34. Steinbart P, Raschke R, Gal G, Dilla W. Information security professionals' perceptions about the relationship between the information security and internal audit functions. J Inform Syst. 2013;27(2):65–86. doi:10.2308/isys-50510.
35. Da Veiga A, Eloff J. A framework and assessment instrument for information security culture. Comput Secur. 2010;29(2):196–207. doi:10.1016/j.cose.2009.09.002.
36. Lee SM, Lee SG, Yoo S. An integrative model of computer abuse based on social control and general deterrence theories. Inform Manage. 2004;41(6):707–18. doi:10.1016/j.im.2003.08.008.
37. Kim SH, Kim GA. A firm's environmental determinants impacting the information security management and the moderating effects of regulatory influence. J Korean Oper Res Manage Sci. 2012;37(3):79–94. doi:10.7737/JKORMS.2012.37.3.079.
38. Dhillon G. Principles of information systems security: Text and cases. Hoboken (NJ): Wiley; 2007. 97–129.
39. Venkatesh V, Morris M, Davis G, Davis F. User acceptance of information technology: toward a unified view. MIS Q. 2003;27(3):425–78. doi:10.2307/30036540.
40. Vroom C, Von Solms R. Towards information security behavioral compliance. Comput Secur. 2004;23(3):191–98. doi:10.1016/j.cose.2004.01.012.
41. Kim SH, Kim GA, French MA. Relationships between need-pull/technology-push and information security management and the moderating role of regulatory pressure. Inf Technol Manage. 2015;16(3):173–92. doi:10.1007/s10799-015-0217-5.
42. Sambamurthy V, Zmud R Managing IT for success: the empowering business partnership. Working paper. Washington (DC): Financial Executives Research Foundation; 1992.
43. Liang H, Saraf N, Hu Q, Xue Y. Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. MIS Q. 2007;31(1):59–87. doi:10.2307/25148781.
44. Guhr N, Lebeck B, Breitner M. The impact of leadership on employees' intended information security behavior: an examination of the full-range leadership theory. Inform Syst J. 2019;29:340–62. doi:10.1111/isj.12202.
45. Hsu C, Lee JN, Straub D. Institutional influences on information systems security innovations. Inform Syst Res. 2012;23(3):918–39. doi:10.1287/isre.1110.0393.
46. Dutta A, McCrohan K. Management's role in information security in a cyber economy. Calif Manage Rev. 2002;45(1):67–87. doi:10.2307/41166154.
47. Ajzen I. The theory of planned behavior. Organ Behav Hum Dec. 1991;50:179–211. doi:10.1016/0749-5978(91)90020-T.
48. Vance A, Siponen M, Pahnila S. Motivating IS security compliance: insights from habit and protection motivation theory. Inform Manage. 2012;49(3):190–98. doi:10.1016/j.im.2012.04.002.
49. Nelson K, Cooprider J. The contribution of shared knowledge to IS group performance. MIS Q. 1996;20(4):409–32. doi:10.2307/249562.
50. Safa N, Von Solms R, Furnell S. Information security policy compliance model in organizations. Comput Secur. 2016;56:70–82. doi:10.1016/j.cose.2015.10.006.
51. Meng A, Lee SY. The value of IT to firms in a developing country in the catch-up process: an empirical comparison of China and the United States. Decis Support Syst. 2007;43(3):737–45. doi:10.1016/j.dss.2006.12.007.
52. Kankanhalli A, Teo H, Tan B, Wei K. An integrative study of information systems security effectiveness. Int J Inf Manage. 2003;23(2):139–54. doi:10.1016/S0268-4012(02)00105-6.
53. Herath T, Rao H. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decis Support Syst. 2009;47(2):154–65. doi:10.1016/j.dss.2009.02.005.
54. Bentler P. Comparative fit indexes in structural models. Psychol Bull. 1990;107(2):238–46. doi:10.1037/0033-2909.107.2.238.
55. Browne M, Cudeck R. Alternative ways of assessing model fit. Sage Focus Ed. 1993;155:136–136.
56. Nunnally J. Psychometric theory. 2nd ed. New York (NY): McGraw-Hill; 1978.
57. Fornell C, Larcker D. Evaluating structural equation models with unobservable variables and measurement error. J Marketing Res. 1981;18(1):39–50. doi:10.1177/002224378101800104.
58. Carte TA, Russell CJ. In pursuit of moderation: nine common errors and their solutions. MIS Q. 2003;27(3):479–501. doi:10.2307/30036541.
59. Hwang I, Kim D, Kim T, Kim S. Why not comply with information security? An empirical approach for the causes of non-compliance. Online Inform Rev. 2017;41(1):2–18. doi:10.1108/OIR-11-2015-0358.
60. Vance A, Lowry PB, Eggett D. Using accountability to reduce access policy violations in information systems. J Manage Inform Syst. 2013;29(4):263–90. doi:10.2753/MIS0742-1222290410.
61. D'Arcy J, Lowry P. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Inform Syst J. 2019;29:43–69. doi:10.1111/isj.12173.
62. Tononi G, Koch C. The neural correlates of consciousness, an update. Ann N Y Acad Sci. 2008;1124:239–61. doi:10.1196/annals.1440.004.