sustainability

MDPI

Article

Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing

Myeonggil Choi

Department of Business Administration, Chung-Ang University, 84 Heukseok-ro, Dongjak-gu, Seoul 06974, Korea; mgchoi@cau.ac.kr; Tel.: +82-2-820-5454; Fax: +82-2-815-7001

Academic Editors: James Park and Han-Chieh Chao
Received: 21 March 2016; Accepted: 28 June 2016; Published: 7 July 2016

Abstract: Information security has been predicted as a barrier for future sustainable computing. Regarding information security of secure sustainable computing, the role of information security managers has received attention. In particular, transformational leadership by information security managers should be stressed for persuading, directing, and controlling management and employees. This study shows that the transformational leadership (in forms such as idealized influence, individualized consideration, and inspirational motivation) of information security managers can improve the effectiveness of information security. The enforcement and relevance of information security policies could be mediating effects on the effectiveness of information security. This study collects data from governmental and public institutions in Korea. This study suggests the need for leadership education programs, and indicates that job training for information security managers should be conducted regularly.

Keywords: sustainable computing; information security manager; transformational leadership; relevance of information security policy; enforcement of information security policy; information security effectiveness

1. Introduction

Many national governments have been utilizing information and communication technology (ICT) to improve public services, for effective communication and interactions with their constituents, and in administrative organizations [1,2]. Sustainable computing services are driving sustainability beyond simply energy use and product considerations [3], and deal with the loss of control by individuals, businesses, and governments [3]. Sustainable computing services can be defined as effective and reliable processes for delivering sustainable IT services [4]. Sustainable computing services consider managing performance and doing what is necessary to keep the service operating smoothly, including ensuring constant security, providing systems recovery planning, and keeping versions current [5]. Essentially, sustainable computing provides secure computing services to users. Security can be considered the dividing line between non-sustainable and sustainable computing service [3]. Any system is considered unsustainable if it cannot protect data or ensure a required computing quality [3]. Information security has been regarded as a serious issue, especially in e-government contexts [6]. Organizations attempting to protect information must consider controls on internal stakeholders [7]: a large number of information security breaches are due to poor user compliance with information security protocols [8]. The violation of information security harms private organizations by causing financial losses and reputation damage [9]; in the public sector, the violation of information security can lead to serious, complex financial, political, and economic losses; reputation damage; and the loss of public trust in e-government and government organizations that adopt e-government methods.

Thus, to prevent cybercrime, it is natural for e-governments to seek advanced security management processes and continuous information security innovation.

Many governments have attempted to overcome the barriers to information systems security (ISS) within their organizations for sustainable computing [10]. ISS has become an important focus of e-governments since the late 1990s; ISS issues have received attention [11]. ISS is defined as secure systems and policies for protecting an organization's information resources from disclosure to unauthorized persons who attempt to access those information resources [12]. Burney [13] and Rohmeyer [14] argued that the combination of information security management and information programs could improve the effectiveness of ISS. They described the critical duties of information security managers in establishing information security programs. Burney argued that information security managers can be information mediators between the general management department and the technical department [12]. Rohmeyer investigated the major constructs of information security manager skills and information security program maturity within organizational information security. Pohmeyer argued that the effectiveness of the organization can be improved by skilled information security managers [13]. As mentioned in previous studies, the role of information security managers is central to directing e-government ISS efforts, and to encouraging employees to comply with ISS policies.

Research has concluded that for maintaining information security within an organization, information security managers must specify appropriate information security policies and motivate their employees to follow them [11,15–17]. Although information security managers cannot directly enforce ISS policy compliance, they must constantly encourage and motivate all members to comply with information security policies, including monitoring and warning those organizational members who violate security policy. Sometimes, information security managers must also persuade top managers to invest in people, budgets, and technological security controls for ISS [18]. The leadership of the information security manager could encourage employee compliance with ISS and improve the alertness of top managers, thus improving the effectiveness of ISS. The leadership of the information security manager could improve the effectiveness of ISS in e-governments.

This study attempts to evaluate the factors that affect ISS effectiveness from the perspective of information security manager leadership for secure sustainable computing. Accordingly, this study attempts to elucidate the interplay of information security manager leadership and ISS effectiveness.

Using advanced information and communications infrastructure, the Korean government has actively promoted e-government as a way to improve national competitiveness [19]. The Korean e-government model has been found to be one of the most successful models [20]. To ensure public trust and confidence in e-government, the Korean government has invested budgets, human resources, and legislative attention in developing, implementing, and imitating advanced ISS and have treated continuous ISS innovation as necessary [21]. However, individual Korean government agencies' information security systems still have problems, including a lack of manpower, budget limitations, and ill-defined roles and scopes regarding information security [21]. In the development of e-governments worldwide, information security manager leadership issues could have theoretical and practical implications for the development of other countries' e-governments.

2. Literature Review and Hypotheses

2.1. Research Background

ISS research has adopted four perspectives, namely, functionalist, radical humanist, radical structuralist, and interpretive. The functionalist perspective has been a major research theme in information security research [22]. Hu et al. [23] and Knapp et al. [24] argued the importance of both top management's role and information security policy when investigating ISS using social role theory. According to this theory, managers are expected to model the manager's role behavior expected by the organization to achieve goals and outcomes in most daily activities [25]. Regarding social role theory,

most researchers have focused on the role of top management. Hu et al. [23] and Knapp et al. [24] showed the importance of top management in influencing employee behavior, resulting in compliance with information security policies.

Many studies have suggested the need for formal research on the relationship between leadership and ISS effectiveness [13,26]; however, studies of these and related areas are limited to a small number of academic studies. Interest groups, such as the Computer Security Institute (CSI), and industry publications such as Information Security Magazine and CSO Magazine have conducted various surveys. Rohmeyer [14] investigated the major constructs of information security effectiveness, information security manager skills, and information security program maturity within organizational information security. High effectiveness in information security management has been shown to be positively related to the leadership and qualifications of information security managers [14,27,28]. Rohmeyer argued that organizations that hire skilled information security managers are expected to be more effective at information security [14]. A skilled information security manager is one with higher skills and qualifications; the required skills of an information security manager can be summarized as technical, administrative, bureaucratic, and technocratic [14].

Many studies have described the role of information security managers in establishing information security programs. Burney [13] and Kim and Choi [27] have described the essential roles and responsibilities of ISS managers. Burney stressed the leadership activities of information security managers in establishing information security measures. Burney also described the important roles of information security managers as information mediators between technical and general management departments. Wylder [29] described the roles of the information security manager in establishing the information security program. When the information security program reaches maturity, the security manager's skills (technical, administrative, bureaucratic, and technocratic) are required. Luftman [30] described the role of the information security manager from the perspective of IT governance. Information security managers are involved in making decisions and obtaining IT resources in the context of information security tasks.

This study adopts a human behavior approach and an institutional approach to improving ISS effectiveness. Unlike previous studies, which focus on the technological controls for ISS effectiveness, Chaudhry et al. proposed a human behavior and institutional approach as a development framework for enterprise ISS [31]. The framework consists of four main pillars, namely, security policy, security awareness, access control, and top-level management support (which has a foundation of corporate governance). This study also considers information security policy as an important part of information security in an organization, and investigates it as a meditating effect on ISS effectiveness. The purpose of transformational leadership of an information manager is improving employee awareness of information security in organizations. Top-level management support and corporate governance are also essential factors in supporting the activities of the information security manager, information security policy [31], and ISS effectiveness [32].

In the information security realm, deterrents are defined as administrative tools that can include information security policies that describe the secure use of information systems [33]. The controls of administrative deterrents have been validated as effective in reducing IS [34] and computer abuses (such as software piracy [35,36]) and violation of information security policies [33,37,38]. Wiant [39] also regarded information security policies as deterrent measures, and noted that the effectiveness of information security policy can be maintained when computer abuse incidents and their seriousness are monitored and reported. The theory of general deterrence states that policy can prevent potential abusive acts by presenting the threat of sanctions and unpleasant consequences [34,40].

2.2. Transformational Leadership

The relationship between information security managers and other employees, regardless of their position in the organization, can be treated as the relationship between leaders and followers. To urge employees within the organization to maintain information security, information security managers

should persuade, inspire, and motivate their employees. Information security managers do not have any direct controls by which to order, monitor, or punish other employees. To effectively lead other employees in complying with information security policies, information security managers should display leadership via implementation of information security policy. Here, the authors review the related components leadership.

In the past 100 years, leadership has been defined in terms of the behaviors, traits, role relationships, interaction patterns, and occupations of someone in an administrative position. There is a fundamental and highly controversial issue in the field of leadership, namely, "what we do know and what we should know about leadership and leaders" [41]. A wide variety of views on leadership involve the question of whether to judge leadership as a transmission process or a specialized role [42].

Burns [43] and Bass [44] suggested the need to shift the emphasis of leadership studies from mainly examining transactional models grounded on "how leaders and followers make an exchange with each other to models that might expand transactional leadership and were labeled charismatic, transformational, inspirational, and visionary". Both transactional and transformational leadership are originally embedded in the dyadic paradigm, the theory of which retains the relationship of the leader subordinate dyad, as described above. Unlike traditional leadership models that describe leader behavior in terms of providing direction, support, reinforcement behaviors, goals, and leader-follower exchange relationships (or indeed being based on "economic cost-benefit assumptions" [44]), new leadership models highlight "symbolic leader behavior; visionary, inspirational messages; emotional feelings; ideological and moral values; individualized attention; and intellectual stimulation". Emerging from these studies, transformational leadership theories have been the most frequently researched theories over the past 20 years [45,46]. Transformational leadership has been redefined as the mutual commitment to the objectives and mission/vision of the work unit [47].

The theory of transformational leadership indicates that such leaders have reinforced their higher-order values and elevated followers' aspirations such that the followers can identify their mission/vision, work more effectively and efficiently, and work to do their part beyond base expectations and mere transactions [44,48]. Transformational leadership appeals to the moral values of followers in an attempt to raise their consciousness with regard to ethical issues and mobilize their energy and resources to reform institutions.

Judge and Piccolo [49] state that transformational leadership is positively related to leadership effectiveness and to several significant organizational outcomes across many different types of organizations, levels of analyses, situations, and cultures using a series of meta-analytic studies. Many researchers have studied different processes using transformational leadership effects that are eventually realized in the form of performance outcomes [41]. These processes involve follower formation of identification; satisfaction; commitment; perceived fairness [50,51]; job characteristics such as identity, significance, variety, feedback, and autonomy [52]; trust in the leader [53]; and how followers feel about themselves and their group in terms of cohesion, potency, and efficacy [54,55].

New theories of transformational leadership are more concerned with goal attainment in pragmatic task objectives by followers, groups, and organizations than with the moral elevation of followers. Jansen and Crossan [56] state that it is necessary to consider interactions between leaders and followers, rather than the leaders' unreciprocated behaviors. Kahai and colleagues showed that transformational leadership reduces the incidence of social loafing (a "counterproductive" behavior) [57]. Transformational leadership not only reduces the impact of counterproductive behaviors but also improves the performance of individuals and groups, because transformational leaders have the ability to gather followers committed to collective goals, rather than simply to satisfying the followers' personal goals.

Social role theory is a perspective in sociology in which socially defined categories or roles (such as mother, manager, teacher, group member, and team members) have distinct expectations associated with them; correct leader behaviors are required to achieve organization goals and outcomes in most daily activities [25].

Kark et al. [58] suggested that transformational leadership has an impact on both social identification within the work unit and personal identification with the leader. Leadership research on social identity formation has also focused heavily on what constitutes prototypicality, which has shown that followers can be closer to those leaders who are exemplars of the groups the followers want to join or to which they already belong [58]. Lord and Brown [59] presented a model that studies two specific ways in which leaders can influence the manner in which followers choose to behave, in terms of the motivations they have regulated through actions and behaviors. The idea of a working self-concept brings up issues of identity [60].

Transformational leadership by information security managers is expected to improve ISS effectiveness. Although ISS managers can inspire employees to comply with ISS, information security managers do not have direct means for influencing employees. Information security policy is an important mediator in influence among employees.

Researchers have suggested that transformational leadership behaviors include four components: inspirational motivation, idealized influence, individualized consideration, and intellectual stimulation. The first two components are similar to the concept of "charisma" [44,61]. Inspirational motivation includes the demonstration of enthusiasm and optimism, presentation and creation of symbols and emotional arguments, and an attractive vision of the future. Thus, the author hypothesizes that:

(H-1a) The inspirational motivation of transformational leadership affects the relevance of information security policy.

(H-1b) The inspirational motivation of transformational leadership affects the enforcement of information security policy.

Support for (H-1a) and (H-1b) would indicate that the inspirational motivation of transformational leadership has an indirect influence on the relevance of information security policy and the enforcement of information policy, because of its direct influence on the maturity of the information security policy.

Idealized influence involves behaviors such as setting a personal example, demonstrating high ethical standards, and making sacrifices for the benefit of the group. Thus, the author hypothesizes that:

(H-2a) The idealized influence of transformational leadership affects the relevance of information security policy.

(H-2b) The idealized influence of transformational leadership affects the enforcement of information security policy.

Support for (H-2a) and (H-2b) would indicate that the idealized influence of transformational leadership has an indirect influence on the relevance of information security policy and the enforcement of information policy, because of its direct influence on the maturity of the information security policy.

The third component, individualized consideration, contains coaching, encouraging, and providing support to followers. Thus, the author hypothesizes that:

(H-3a) The individualized consideration of transformational leadership affects the relevance of information security policy.

(H-3b) The individualized consideration of transformational leadership affects the enforcement of information security policy.

Support for (H-3a) and (H-3b) would indicate that the individualized consideration of transformational leadership has an indirect influence on the relevance of information security policy and the enforcement of information policy, because of its direct influence on the maturity of the information security policy.

The fourth component, intellectual stimulation, includes behaviors that challenge followers to view problems from new perspectives. Previous studies have demonstrated that these transformational behaviors are related to high employee performance [49] and high leadership effectiveness [62]. Thus, the author hypothesizes that:

(H-4a) The intellectual stimulation of transformational leadership affects the relevance of information security policy.

(H-4b) The intellectual stimulation of transformational leadership affects the enforcement of information security policy.

Support for (H-4a) and (H-4b) would indicate that the intellectual stimulation of transformational leadership has an indirect influence on the relevance of information security policy and the enforcement of information policy, because of its direct influence on the maturity of the information security policy.

2.3. Relevance and Enforcement of Information Security Policies

Several authors have investigated the role of information security policies [24,63–65]. Kemp [63] noted that management should support information security policies if they are to be effective. Thomson and von Solms [64] argued that the effectiveness of information security policies is improved for employees that adopt them in practical cases.

To improve the effectiveness of information security, information security policies should be established as a control for effective deterrence efforts. After the establishment of information security policies, information security managers should manage information security policy properly and stress that policy violation will be punished accordingly. Based on the established policy, information security managers should conduct appropriate monitoring and surveillance programs of employee activities, so as to enforce policy. Information security managers should observe all of the identified violations to deter potential violators. Finally, the organization's management should ensure the deployment of preventive controls that proactively help minimize security incidents [34].

Knapp et al. considered the influences of information security policies on the effectiveness of information security, and divided the concept of information security policy into policy relevance and enforcement [65]. Knapp et al. utilized a qualitative research approach that closely observes grounded theory, which attempts to derive theory from corpus data [66]. Knapp et al. [24] also argued that the enforcement of information security policy would improve the effectiveness of information security. Enforcement is the most important information security policy issue. To improve information security, an organization attempts to include all desired goals. The content of information security policies will be rendered useless if not enforced.

We expect that the enforcement of information security policies will influence the effectiveness of information security. Thus, we hypothesize that:

(H-5) The enforcement of information security policies improves the effectiveness of ISS.

To achieve sustainability of information security policies, information security managers should ensure their relevance, which includes the four aspects described here. Information security policies should reflect changes in technology. Policies should periodically (and correctly) be updated on a regular basis. Review and update processes for updating information security policies should exist [65]. The relevance of information security policies will improve the effectiveness of ISS. To improve the effectiveness of information systems, the enforcement of information security policies should be sustained [34,65]. To improve enforcement, the organization can sanction employees who violate the rules of information security policy, enforce the rules of information security by sanctioning those employees who violate them, and educate security offenders. Management needs to ensure that users are educated and informed on proper IS use. Information security managers should stress that policy violations will be punished accordingly. With policies in place, the managers can ensure that appropriate employee activity monitoring and surveillance programs are utilized to enforce policy. Information security managers should then follow-up with all identified violations to help deter potential abusers. Management should ensure that the implementation of preventive mechanisms using security software proactively helps minimize security incidents. An organization might consider termination of employees who repeatedly violate information security policies [65].

In this study, we expect the relevance of information security policies to influence the effectiveness of information security. Thus, we hypothesize that:

(H-6) The relevance of information security policy improves the effectiveness of ISS.

2.4. ISS Effectiveness

The definition of ISS effectiveness includes the extent to which objectives and goals of an ISS program are achieved, the secure operation of information programs, and the protection of information. ISS effectiveness includes the overall functions of ISS.

ISS effectiveness is influenced by the ways in which security content is addressed in the policy, and how content is communicated to users [67]. ISS effectiveness can be enhanced by security items specified in security policies [68], organizational factors [65], and security measures [69].

Information security measures (such as tools, methods, procedures, and controls) and raising awareness [69] can increase ISS effectiveness. Among information security measures, ISS effectiveness is also influenced by preventive efforts, such as the protection of data, software, hardware, and computer services [70]. Among organizational behaviors, the effectiveness of ISS is impacted by several factors, including policy relevance, user training, policy enforcement [65], and top management [71]. Among hybrid factors, efforts such as hours spent on deterrence and prevention in a week, dedication to data security, notification to users of penalties, and the utilization and violation of security software [34] can also influence ISS effectiveness. Table 1 summarizes research background.

Table 1. Research background.

Research Area	Study Content	Reference
ISS research	Importance of the top management role and information security policy. social role theory, focus on manager's role	Hu et al. [23], Knapp et al. [24], Eagly et al. [25]
	Research on the relationship between leadership and ISS effectiveness	Burney [13], Long [26]
	Information security effectiveness is positively related with the leadership of information security managers	Rohmeyer [14], Kim and Choi [27], Kim et al. [28]
	Role of information security managers in establishing information security programs	Burney [13], Kim and Choi [27], Wylder [29]
	Information security policy as a deterrent measure	Wiant [39]
Transformational leadership	Emphasis on leadership from transactional model	Burns [43], Bass [44], Judge and Piccolo [49], Kark et al. [58]
	Theory of transformational leadership	Bass [44], Avolio [48]
	Interactions between leaders and followers	Jansen and Crossan [56]
Relevance and enforcement of information security Policy	Enforcement of information security policy	Knapp et al. [24], Kemp [63], Thomson and von Solms [64], Knapp et al. [65]
	Relevance of information security policy	Straub [34], Knapp et al. [65]
ISS effectiveness	ISS effectiveness	Knapp et al. [65], Karyda et al. [68], Hagen et al. [69], Straub [71]

3. Methodology

3.1. Measurement Construct

This study uses the research model presented in Figure 1. The variables are measured based on previously validated items, and are then further modified as required. Some of the items have been developed by the authors. The measurement of all variables utilizes a five-point Likert scale, where 1 denotes "strongly disagree" and 5 denotes "strongly agree".

The three items that measure idealized influence are taken from Viator [72] and Podsakoff et al. [73]. The three items that measure intellectual stimulation are taken from Ke and Wei [74], and Podsakoff et al. [73]. The three items of individualized consideration are based on those used by Viator [72] and Ke and Wei [74]. To measure inspirational motivation, three variables taken from Viator [72] and Ke and Wei [74] are used. Four items taken from Knapp et al. [65] are used as measures of the relevance of information security policy. To measure the enforcement of information security policies, four items from Knapp et al. [65] are used. Four items from Hagen et al. [69] are used to measure ISS effectiveness. The items of questionnaire in this study are described in the Appendix.

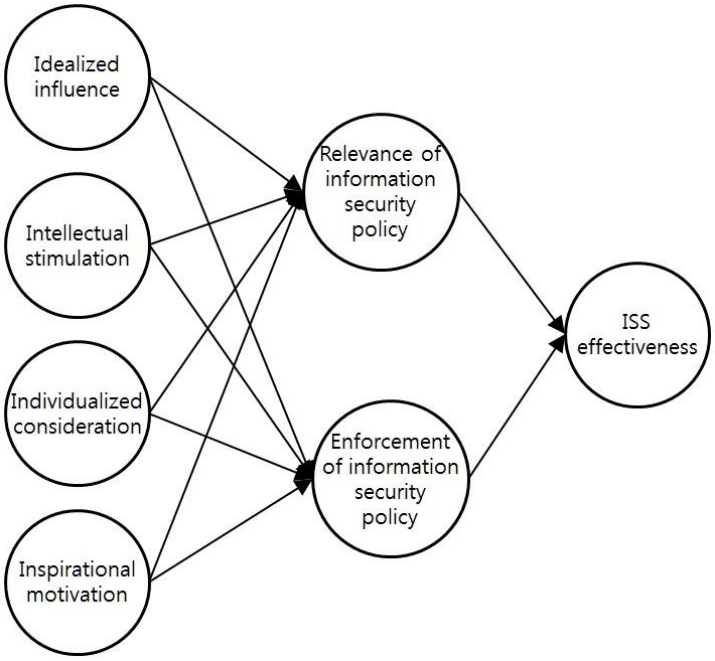

Figure 1. Research model.

3.2. Data Collection

To confirm the validity of the questionnaire, the questionnaire was sent to three information security managers in government and five professors researching information security management by email and phone. These experts gave comments on some of items in the questionnaire (and corrected them for clarity) and the predicted results. Based on their feedback, the authors corrected several items in the questionnaire. After validation, the authors conducted a pilot test. Five researchers were asked to participate in the pilot test. They responded to the questionnaire from the perspective of information security managers and indicated that some of the terms needed to be clarified. Based on their feedback, we modified the questionnaire.

Questionnaires were presented as opinion surveys on information security management to information security managers from approximately 35 Korean central government agencies, 17 local-autonomy governments, and 103 government-owned enterprises. We sent mail to the information security managers in these organizations, asked for the help of an acquaintance in a

government agency, and asked them to fill out the questionnaire. The author chose the surveyed enterprises based on only summary reports of evaluating information security available to the public. To effectively reflect the responses of information security managers, the author sent two or three questionnaires to very large government-owned enterprises such as electricity companies, energy companies, transportation companies, and water management companies. The number of information security managers in these enterprises is known to be greater than 10. Of the 200 paper questionnaires sent, we received 190 back and analyzed the 180 that had valid responses. The valid response rate was 90%.

The results from the 180 respondents are reported in Table 2. The age of most respondents was between 41 and 50 years. Of the respondents, approximately 60% had worked for less than five years at their corresponding positions, and 96.6% were regular employees.

Table 2. Demographic characteristics.

Item	Variable	Frequency	Percentage (%)
Gender	Male	117	65.0
	Female	63	35.0
Age	Under 20 years	1	0.6
	21–30 years	6	3.3
	31–40 years	72	40.0
	41–50 years	62	34.4
	Above 51 years	39	21.7
Years working	Less than 1 year	16	8.9
	1–5 years	11	6.1
	5–10 years	47	26.1
	10–15 years	19	10.6
	More than 15 years	65	36.1
Years working as ISS manager	Less than 1 year	38	21.1
	1–5 years	73	40.6
	5–10 years	13	7.2
	10–15 years	15	8.3
	More than 15 years	41	22.8
IS organization	Yes	98	54.4
	No	82	45.6
Budget scale	Less than 0.1 billion	5	2.8
	0.1–1 billion	44	24.4
	1–5 billion	78	43.3
	5–10 billion	12	6.7
	More than 10 billion	41	22.8
Number of ISS managers	1–5	87	48.3
	5–10	41	22.8
	10–15	23	12.8
	More than 15	29	16.1
Years working in IT field	Less than 1 year	11	6.1
	1–5 years	33	18.3
	5–10 years	22	12.2
	10–15 years	41	22.8
	More than 15 years	73	40.6
Education	High School Diploma	2	1.1
	Junior College	16	8.9
	Bachelor's	97	53.9
	Master's or above	65	36.1

Table 2. *Cont.*

Item	Variable	Frequency	Percentage (%)
Certificate numbers	0	9	5.0
	1	67	37.2
	2	35	19.4
	3	16	8.9
	4	16	8.9
	More than 5	37	20.6
Training or education days per year	0	4	2.2
	1–5	34	18.9
	5–10	76	42.2
	More than 10	66	36.7
Number of conferences attended in a year	0	30	16.7
	1	60	33.3
	2	34	18.9
	3	15	8.3
	4	4	2.2
	More than 5	37	20.6

4. Analysis of Results

The research model is validated using structural equation modeling, which allows analysis of the relationships (and their strengths) between constructs. Reflecting growing use in management studies [75], partial least squares (PLS) is used as the estimation procedure. PLS combines factor analysis with linear regression and does not require large sample sizes; it makes only minimal assumptions about the goal of variance explanation, and makes no assumptions regarding the underlying distribution of data [76]. Smart PLS 2.0 and SPSS 18.0 software packages are used for data analysis.

Reliability can be defined as the overall internal consistency of the results. A standardized approach was taken to improve reliability. Construction of a well-defined survey instrument and consistent administration of the survey improved reliability. In this study, multiple items were developed to measure the statements, which describe the relationships between constructs. Reliability analysis was conducted using SPSS, using the calculation of Cronbach's alpha. The majority of individuals correctly used Cronbach's alpha as the measure of internal consistency. Cronbach's alpha reliability coefficient normally ranges between 0 and 1. The closer Cronbach's alpha coefficient is to 1.0, the greater the internal consistency of the items in the scale. Table 3 shows the reliability of each construct and indicates that Cronbach's alpha values are greater than 0.7, which means that the measurement of the constructs maintained internal consistency.

Exploratory factor analysis is conducted using principle component analysis and varimax orthogonal factor rotation utilizing SPSS. The purposes of exploratory factor analysis are determining the number of fundamental influences underling the domain of variables, measuring the extent to which each construct is associated with the factors, and acquiring information about their nature by observing which factors influence performance on which variables. Table 4 lists the results of the exploratory factor analysis.

Validity represents effectiveness when producing accurate results and conclusions. Internal validity indicates the overall integrity of the experiment. External validity indicates the ability to generalize the findings of the study to the general population (i.e., beyond the limited sample). Threat sources to validity can be statistical or constructs. Statistical threats are related to concerns of whether the observed results were due to chance or, in fact, they can be attributed to some effect of the independent variable. Construct validity is related to the concept of whether or not the operational definitions are valid measures of the various constructs. Construct validity includes empirical and theoretical support for the interpretation of the construct. There are two kinds of approaches in

construct validity. First, convergent validity represents the degree to which a measure is correlated with other measures that it is theoretically predicted to correlate with. Second, discriminant validity represents the extent to which the operational definitions do not correlate with other operational definitions that, theoretically, it should not correlate with.

Table 3. Validity and reliability of reflective constructs.

Construct	Indicator	Item Loading	Mean	SD	*T*-Value	AVE	Composite Reliability	R Square	Cronbach's Alpha
Idealized influence	Ideal_Influ_1	0.91	4.07	0.83	51.75	0.80	0.92		0.87
	Ideal_Influ_2	0.91	3.88	0.87	54.11				
	Ideal_Influ_3	0.85	3.94	0.87	27.35				
Intellectual stimulation	Intel_Sti1	0.85	3.84	0.98	19.86	0.74	0.90		0.83
	Intel_Sti2	0.93	3.69	0.95	58.21				
	Intel_Sti3	0.81	3.95	1.10	14.46				
Individualized consideration	Indiv_Con1	0.81	4.39	0.75	22.42	0.70	0.87		0.79
	Indiv_Con2	0.84	4.12	0.76	28.82				
	Indiv_Con3	0.86	4.42	0.62	33.53				
Inspirational motivation	Inst_Moti1	0.71	3.64	0.91	9.39	0.64	0.84		0.72
	Inst_Moti2	0.88	4.17	0.77	47.51				
	Inst_Moti3	0.80	4.11	0.71	19.71				
Policy enforcement	Pol_Emf1	0.82	4.34	0.64	26.59	0.67	0.89	0.39	0.84
	Pol_Emf2	0.81	4.22	0.68	23.51				
	Pol_Emf3	0.86	4.32	0.70	35.56				
	Pol_Emf4	0.79	4.17	0.75	25.67				
Policy relevance	Pol_Rel1	0.88	4.01	0.78	47.05	0.72	0.88	0.28	0.80
	Pol_Rel2	0.89	3.94	0.84	48.49				
	Pol_Rel3	0.77	3.89	0.84	17.28				
ISS effectiveness	ISS_Effect1	0.87	4.26	0.67	35.28	0.74	0.92	0.56	0.88
	ISS_Effect2	0.89	4.27	0.72	52.43				
	ISS_Effect3	0.81	4.36	0.70	20.51				
	ISS_Effect4	0.86	4.17	0.74	45.49				

Table 4. Exploratory factor analysis.

Indicator	Component						
	1	2	3	4	5	6	7
Pol_Emf2	0.799	0.115	0.120	0.084	0.087	0.141	0.153
Pol_Emf3	0.766	0.189	0.203	0.148	0.158	0.088	0.149
Pol_Emf1	0.752	0.252	0.084	0.085	0.100	0.249	−0.027
Pol_Emf4	0.530	0.377	0.139	−0.067	0.192	0.153	0.375
ISS_Effect4	0.166	0.816	0.130	0.099	0.134	0.126	0.107
ISS_Effect3	0.233	0.772	0.183	0.098	0.298	0.115	0.079
ISS_Effect2	0.220	0.713	0.249	0.057	0.226	0.219	0.148
ISS_Effect1	0.390	0.563	0.172	0.064	0.358	0.113	0.317
Ideal_Influ_3	0.193	0.138	0.840	0.211	0.144	0.132	0.051
Ideal_Influ_2	0.117	0.176	0.813	0.107	0.124	0.030	0.173
Ideal_Influ_1	0.142	0.215	0.792	0.123	0.181	0.217	0.136
Intel_Sti1	0.125	0.117	0.172	0.856	0.048	0.146	0.174
Intel_Sti2	0.001	0.126	0.193	0.801	0.069	0.277	−0.081
Intel_Sti3	0.159	−0.026	0.058	0.765	0.114	0.050	0.343
Pol_Rel1	0.201	0.184	0.146	0.067	0.837	0.158	0.022
Pol_Rel2	0.263	0.233	0.116	0.068	0.788	0.150	0.055
Pol_Rel3	−0.065	0.264	0.205	0.117	0.667	0.007	0.284
Indiv_Con3	0.158	0.157	0.029	0.198	0.061	0.809	0.151
Indiv_Con2	0.329	0.168	0.195	0.126	0.189	0.665	0.109
Indiv_Con1	0.204	0.121	0.265	0.210	0.150	0.596	0.319
Inst_Moti1	0.237	0.098	0.167	0.149	0.126	0.051	0.735
Inst_Moti3	0.234	0.226	0.088	0.115	0.073	0.381	0.646
Inst_Moti2	−0.114	0.145	0.136	0.275	0.103	0.386	0.560

Convergent validity was evaluated using that composite reliability (CR) and average variance extracted (AVE) values for all constructs that are greater than the required validity thresholds. Convergent validity is considered valid if the composite reliability and AVE values are greater than 0.7 and 0.5, respectively [76]. Table 3 indicates that all of the measures satisfy all of the thresholds, and thus, convergent validity is satisfied. To satisfy discriminant validity, the square root of the AVE values must exceed the correlation coefficients between the construct and the other constructs in the model [76]. Table 5 indicates that the square roots of the AVE values exceeded the correlation coefficients, thereby verifying discriminant validity. The fact that convergent validity and discriminant validity were satisfied means that all of measurements maintain internal consistency.

Table 5. Discriminant validity and correlation of latent variable scores.

Construct	Idealized Influence	ISS Effectiveness	Individualized Consideration	Intellectual Stimulation	Inspirational Motivation	Policy Enforcement	Policy Relevance
Idealized influence	0.894						
ISS effectiveness	0.525	0.858					
Individualized consideration	0.473	0.540	0.836				
Intellectual stimulation	0.403	0.315	0.482	0.863			
Inspirational motivation	0.427	0.514	0.592	0.459	0.800		
Policy enforcement	0.453	0.656	0.564	0.303	0.499	0.819	
Policy relevance	0.453	0.631	0.427	0.285	0.404	0.468	0.848

The effects proposed in the model and their significance values are estimated using PLS. Table 6 lists the results of the structural model PLS regressions. The bootstrap method was used to evaluate the path (bootstrap resampling number = 500). The proportion of the ISS effectiveness, the dependent variable that is predicted from the independent variables and meditate variables, is 58%.

Table 6. Testing results of structural model.

Path	B	*T* Statistics
Idealized influence → Policy relevance (H-1a)	0.292	2.753 ***
Idealized influence → Policy enforcement (H-1b)	0.211	3.278 ***
Intellectual stimulation → Policy relevance (H-2a)	−0.002	0.027 ^{NS}
Intellectual stimulation → Policy enforcement (H-2b)	−0.058	0.955 ^{NS}
Individualized consideration → Policy relevance (H-3a)	0.191	2.418 **
Individualized consideration → Policy enforcement (H-3b)	0.361	4.235 ***
Inspirational motivation → Policy relevance (H-4a)	0.168	2.113 **
Inspirational motivation → Policy enforcement (H-4b)	0.222	3.039 ***
Policy relevance → ISS effectiveness (H-5)	0.415	4.784 ***
Policy enforcement → ISS effectiveness (H-6)	0.462	5.121 ***

** $p < 0.05$; *** $p < 0.01$; ^{NS} not significant.

We tested the suggested research model and further investigated the mediating effects of information security policy on ISS effectiveness in the other models. In the first model (Figure 2), all of the constructs are included, and direct and indirect paths to effectiveness (and the effects of the control variable on ISS effectiveness) are tested. Hypothesis 1a, which states that idealized influence is positively associated with policy relevance, is supported ($\beta = 0.292$, $p < 0.01$). This result shows that the strong idealized influence of the information security manager is associated with an improvement in information security relevance. Hypothesis 1b, which states that idealized influence is positively

associated with policy enforcement, is supported (β = 0.211, $p < 0.01$). This result means that the strong idealized influence of the information security manager can increase the level of enforcement of information security policy.

Hypothesis 2a, which states that intellectual stimulation of the information security manager is positively associated with policy relevance, is not supported. This result shows that intellectual stimulation of the information security manager cannot increase the degree of policy relevance. Hypothesis 2b, which states that intellectual stimulation of the information security manager is positively associated with policy enforcement, is also not supported. This result shows that intellectual stimulation of the information security manager cannot increase the level of enforcement of information security policy.

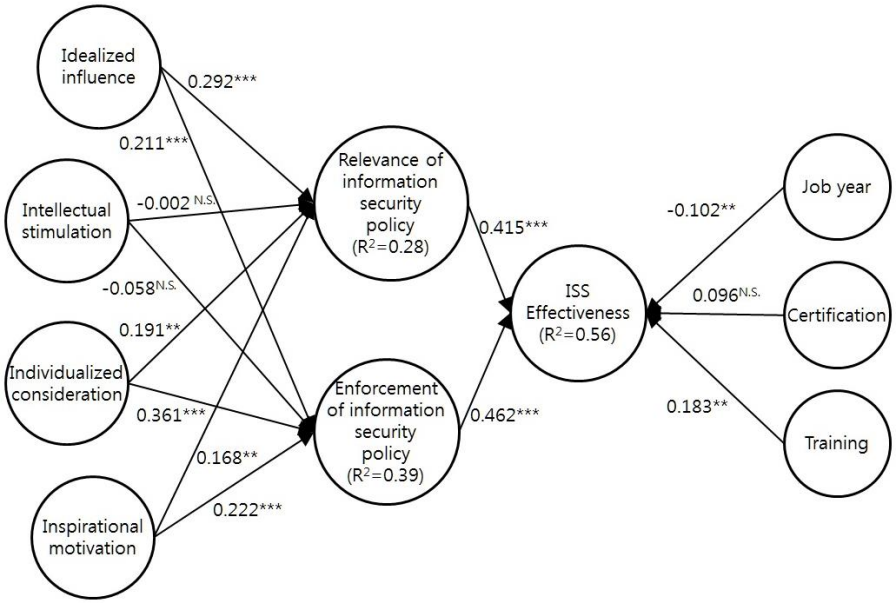

Figure 2. Results of research model. ** $p < 0.05$; *** $p < 0.01$; ^{NS} not significant.

Hypothesis 3a, which states that individualized consideration of the information security manager is positively associated with policy relevance, is supported (β = 0.191, $p < 0.05$). This result means that individual care by the information security manager for employees can increase the degree of policy relevance. Hypothesis 3b, which states that individualized consideration of the information security manager is positively associated with policy enforcement, is supported (β = 0.361, $p < 0.01$). This result shows that individual care of the information security manager can increase the degree of enforcement of information security policy.

Hypothesis 4a, which states that inspirational motivation of the information security manager's leadership is positively associated with policy relevance, is supported (β = 0.168, $p < 0.05$). This result means that motivation due to the information security manager's leadership can increase the degree of policy relevance. Hypothesis 4b, which states that inspirational motivation of the information security manager's leadership is positively associated with enforcement of information security policy, is supported (β = 0.222, $p < 0.01$). This result shows that inspirational motivation by the information security manager regarding information security can increase the degree of enforcement of information security policy.

Hypothesis 5, which states that the relevance of information security policy is positively associated with ISS effectiveness, is supported (β = 0.318, $p < 0.01$). This result means that the relevance of information security policy positively influences ISS effectiveness. Hypothesis 6, which states that the enforcement of information security policy is positively associated with ISS effectiveness, is supported

($\beta = 0.515$, $p < 0.01$). This result shows that the relevance of the information security policy positively influences ISS effectiveness.

As Table 7 indicates, the number of years on the job and training frequency within one year are associated with ISS effectiveness. This shows that education and training of information security managers has influenced the ISS effectiveness [14]. Interestingly, the number of years on job is negatively associated with ISS effectiveness. The relation between the number of years on job of information security managers and ISS effectiveness is needed to be further investigated because other theoretical evidences do not mention the relationship.

Table 7. Results of control variables that influerences ISS effectiveness.

Control Variables	B	*T* Statistics
Job year	−0.102	2.344 **
Certification	0.096	1.452 ^{NS}
Frequency of Training	0.183	2.024 **

** $p < 0.05$; *** $p < 0.01$; ^{NS} not significant.

In addition, the mediation effects of the relevance and enforcement of information security policy are statistically tested. This analysis of the mediation effect explains the relationships between the independent and dependent variables. The mediating effects of the relevance and enforcement are tested using logic developed by Baron and Kenny [77], which suggests that a variable can be considered a mediator when it satisfies the following three conditions:

(1) The path between the independent and mediating variables (path a) is significant.
(2) The path between the meditating and dependent variables (path b) is significant.
(3) When paths a and b are controlled, the correlation in path c (from independent to dependent variables) is no longer statistically significant, and thus, can be eliminated.

As Figure 3 shows, the direct paths from idealized influence, individualized consideration, and inspirational motivation to ISS effectiveness are significant; however, the direct path from intellectual stimulation to ISS effectiveness is not significant. Therefore, intellectual stimulation of the information security manager is excluded from the subsequent mediational analysis.

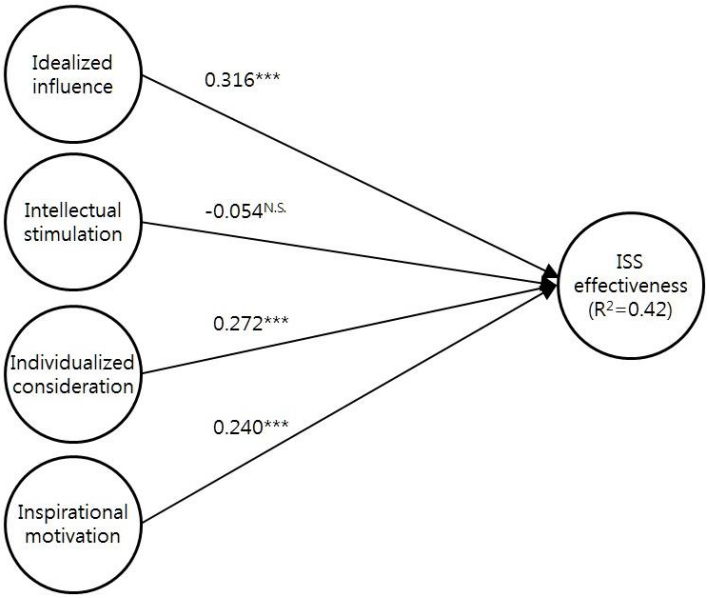

Figure 3. Direct effect model. ** $p < 0.05$; *** $p < 0.01$; ^{NS} not significant.

By introducing information policy relevance as a mediator of the paths between the three independent variables and ISS effectiveness, we observe weak partial mediating effects. The strength of each relationship between ISS effectiveness and idealized influence, individualized care, and inspirational motivation is reduced, thus indicating a partial mediating effect of information security relevance (Figure 4). In other words, idealized influence, individualized consideration, and inspirational motivation are related to ISS effectiveness via the relevance of information security.

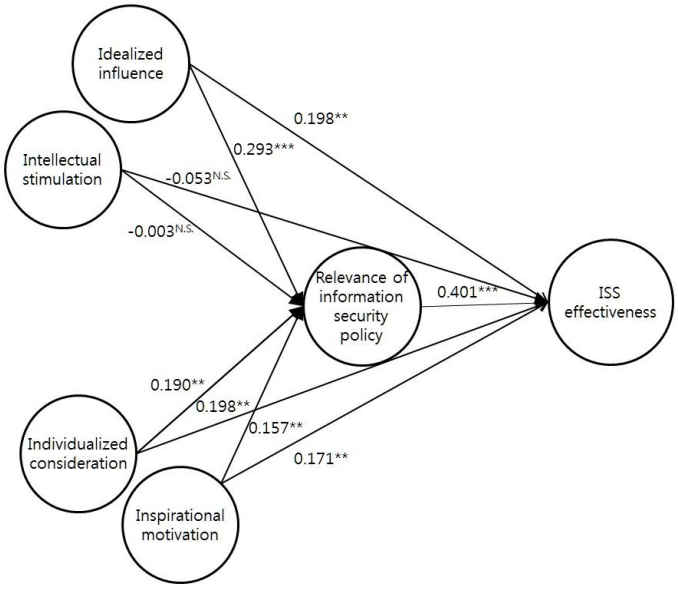

Figure 4. Results of policy relevance meditation effect. ** $p < 0.05$; *** $p < 0.01$; ^{NS} not significant.

The same procedure is conducted to test the meditating effect of information security policy enforcement on each relationship between ISS effectiveness and idealized influence, individual consideration, and inspirational motivation. The relationship between individual consideration and ISS effectiveness is eliminated, thus indicating a complete mediating effect of the enforcement of information security policy on the effects of individualized consideration of the information security manager (Figure 5). This result shows that individual consideration is related to ISS effectiveness via the enforcement of information security policy. Thus, the enforcement and relevance of information security policy contribute to a better explanation of ISS effectiveness.

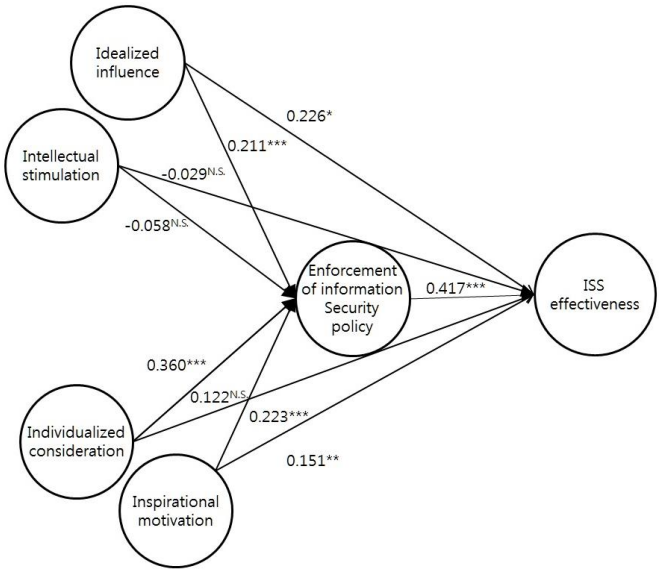

Figure 5. Results of policy enforcement meditation effects. ** $p < 0.05$; *** $p < 0.01$; ^{NS} not significant.

For practicing managers, who try to diagnose the status of ISS effectiveness in their organizations, checklist approaches could be used. Many checklists such as ISO 27001 and parsimonious framework by Ma et al., can be utilized for information security in organizations [78].

5. Conclusions and Discussion

This study showed that transformational leadership by information security managers can improve the effectiveness of ISS used by e-governments. The transformational leadership of information security managers can take a central role in maintaining secure sustainable computing. The results of the study extend and support those of previous studies, which argue that essential skills and the essential role of the information security manager are required for effective information security programs. This study suggests three important results regarding the leadership of information security managers. First, the transformational leadership of information security managers can improve ISS effectiveness. Whereas most previous studies focused on the technical aspects of information security management, this study focused on behavioral characteristics. Although studies into how the leadership of the IT manager can improve the performance of organizations have been performed [14,27,28], this study focused on the transformational leadership of IS managers. The importance of transformational leadership by the information security manager is based on the fact that individuals in organizations have many reasons not to comply with ISS policies. The transformational leadership of IS managers can persuade, assist, and direct employees in complying with ISS policies, thereby improving the effectiveness of IS. Most organizations have tried to provide technological education and training for IS mangers. Education and training for transformational leadership by IS managers should also be established. Organizations should hire IS managers who have the appropriate transformational leadership skills, so as to increase the level of ISS effectiveness.

Second, the relevance and enforcement of information security policy can be mediators between the transformational leadership of information security managers and ISS effectiveness. This study also showed that IS policy should be managed reflecting the changes of information technology environment and the IS policy should be enforced with a certainty and severity. Although most of organizations have established IS policy, they would not regular and consistent update processes, and they have difficulty in punishing the violators committing IS policy [24]. This study showed that the consistent and severe IS policy can improve the maturity of ISS. As the previous study mention, only both the information security governance and top management support can support information security policy [79]. The information security managers, therefore, try to obtain the support of top management level.

Third, this study showed that the education and training positively affect ISS effectiveness in organizations. As the previous study asserts that the adequate IS skills and qualifications have improved the maturity of IS program [78], education and training of information security manager can improve ISS effectiveness. As environments of information technology change rapidly, information security managers need to learn current skills and knowledge. This finding shows that the education and training for IS manager should be provided in a regular period. The author suggests that organizations have to provide mandatory training and education with information security manager at least over 40 h in a year.

This study suggests the effects of information security managers' transformational leadership. Specifically, this study suggests the importance of the leadership of information security managers in e-governments, thus contributing to theoretical research into improving ISS effectiveness in e-governments. E-governments have difficulty considering the transformational leadership of IS managers. Governmental agencies are more centralized, more formalized, and more departmentalized; government organizations result in a form of bureaucratic control (i.e., a greater degree of hierarchy, more centralized decision-making structures, formalized rules, and more functional departments) [80]. As this study indicates, e-governments should try to hire IS managers who have high technical skills and transformational leadership, resulting in improving the maturity of ISS. Additional studies on

the roles of IS managers should be further explored, because many studies show that individuals' behaviors can lead to improved ISS effectiveness.

In summary, the results of this study suggest that leadership education programs and job training for information security managers should be developed and conducted, and that information security policy should be reviewed and updated to improve ISS effectiveness.

This study mainly surveys participants on transformational leadership in public areas. The authors assert that the roles of IS managers in public areas are limited because of their organizational natures. We expect that the private areas demand stronger transformational leadership by IS mangers, in that the culture of efficiency and competiveness in private areas is considered more important than that in public areas [81]. We further investigate the transformational leadership of IS managers in private areas. Because previous studies have indicated that the skill of IS managers in private areas can improve ISS effectiveness, transformational leadership by IS managers could improve the maturity of ISS programs.

Conflicts of Interest: The author declares no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ICT	Information and Communication Technology
ISS	Information Systems Security
CSI	Computer Security Institute
PLS	Partial Least Squares
AVE	Average Variance Extracted

Appendix. Questionnaire Items

– Idealized influence

- I lead employees by promoting information security, rather than by simply describing the importance of information security. (A modified item from Ralph E. Viator and Podsakoff et al. [72,73])
- Regarding information security, I provide a good model for employees. (A modified item from Ralph E. Viator and Podsakoff et al. [72,73])
- I lead employees in information security by following best practices of information security management. (A modified item from Ralph E. Viator and Podsakoff et al. [72,73])

– Intellectual stimulation

- I challenge employees to think about information security policy in new ways. (A modified item from Ke and Wei [74])
- I have stimulated employees to rethink the way they observe the rules of information security. (A modified item from Ralph E. Viator [72])
- I have challenged employees to consider information security as an effective tool to improve the productivity of their tasks. (A new item based on Ke and Wei [74])

– Individualized consideration

- I conduct information activities while considering the feelings of employees. (A modified item from Ralph E. Viator [72])
- I set up appropriate information security learning opportunities for employees. (A modified item from Ke and Wei [74])
- I provide easy information security systems for use by employees with less knowledge of IT. (A new item based on Ke and Wei [74])

– Inspirational motivation

  - I paint an interesting picture of the future of information security. (A modified item from Ralph E. Viator and Podsakoff et al. [72,73])
  - I have a clear understanding of information security as an organizational vision for achievement. (A modified item from Ralph E. Viator and Podsakoff et al. [72,73])
  - I inspire employees based on their plans for the future. (A validated item from Ralph E. Viator [72])

– The relevance of information security policy (Validated items from Knapp et al. [24])

  - Information security policy is updated on a consistent, periodic basis.
  - Information security policy is updated when technology changes require it.
  - An established information security policy review and update process exists.
  - Information security policy is properly updated on a regular basis.

– The enforcement of information security policy

  - Employees caught violating important security policies are appropriately corrected. (A validated item from Knapp et al. [24])
  - Employees violating information security rules are corrected based on sanctions in the organization's policy. (A modified item from Knapp et al. [24])
  - Repeat security offenders are appropriately disciplined. (A modified item from Knapp et al. [24])
  - Severe sanction (such as termination) is considered for employees who repeatedly break security rules. (A modified item from Knapp et al. [24])

– ISS effectiveness

  - The organization provides effective information security controls for software and hardware. (A modified item from Hagen et al. [69])
  - The organization's information security controls can effectively protect data. (A modified item from Hagen et al. [69])
  - The organization's information security controls can effectively provide information services. (A modified item from Hagen et al. [69])
  - The information security program achieves most of its goals. (A modified item from Hagen et al. [69])

References

1. Irani, Z.; Love, P.E.; Montazemi, A. E-Government: Past, present and future. *Eur. J. Inf. Syst.* **2007**, *16*, 103–105. [CrossRef]
2. Zheng, D.; Chen, J.; Huang, L.; Zhang, C. E-Government Adoption in Public Administration Organizations: Integrating Institutional Theory Perspective and Resource-Based View. *Eur. J. Inf. Syst.* **2013**, *22*, 221–234. [CrossRef]
3. Harmon, R.R.; Auseklis, N. Sustainable IT Services: Assessing the Impact of Green Computing Practices. In Proceedings of the Portland International Conference on Management of Engineering & Technology, Portland, OR, USA, 2–6 August 2009.
4. Müller, G.; Sonehara, N.; Echizen, I.; Wohlgemuth, S. Sustainable Cloud Computing. *Bus. Inf. Syst. Eng.* **2011**, *3*, 129–131. [CrossRef]
5. Clifford, A. Sustainable IT. Available online: http://it.toolbox.com/blogs/minimalit/sustainable-it-30157 (accessed on 9 June 2009).
6. Coursey, D.; Norris, D.F. Models of E-Government: Are They Correct? An Empirical Assessment. *Public Adm. Rev.* **2008**, *68*, 523–536. [CrossRef]

7. Alge, B.J.; Ballinger, G.A.; Tangirala, S.; Oakley, J.L. Information Privacy in Organizations: Empowering Creative and Extrarole Performance. *J. Appl. Psychol.* **2006**, *91*, 221–232. [CrossRef] [PubMed]
8. Stanton, J.M.; Stam, K.R.; Mastrangelo, P.; Jolton, J. Analysis of End User Security Behaviors. *Comput. Secur.* **2005**, *24*, 124–133. [CrossRef]
9. Feng, N.; Wang, H.J.; Li, M.Q. A Security Risk Analysis Model for Information Systems: Causal Relationships of Risk Factors and Vulnerability Propagation Analysis. *Inf. Sci.* **2014**, *256*, 57–73. [CrossRef]
10. Choi, M.; Lee, C.H. Information Security Management as a Bridge in Cloud Systems from Private to Public Organizations. *Sustainability* **2015**, *7*, 12032–12051. [CrossRef]
11. Boss, S.R.; Kirsch, L.J.; Angermeier, I.; Shingler, R.A.; Boss, R.W. If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. *Eur. J. Inf. Syst.* **2009**, *18*, 151–164. [CrossRef]
12. Hill, L.B.; Pemberton, J.M. Information Security: An Overview and Resource Guide for Information Managers. *Rec. Manag. Q.* **1995**, *29*, 14–24.
13. Burney, C. *Roles and Responsibilities of the Information Systems Security Officer*; Auerbach Publication, CRC Press LLC: New York, NY, USA, 2003.
14. Rohmeyer, P. An Evaluation of Information Security Management Effectiveness. Ph.D. Thesis, Stevens Institute of Technology, Hoboken, NJ, USA, September 2006.
15. 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*, 523–548.
16. Posey, C.; Roberts, T.L.; Lowry, P.B.; Bennett, R.J.; Courtney, J.F. Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors. *MIS Q.* **2013**, *37*, 1189–1210.
17. Wall, J.D.; Palvia, P.; Lowry, P.B. Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy. *J. Inf. Priv. Secur.* **2013**, *9*, 52–79. [CrossRef]
18. Westphal, J.D.; Clement, M.B. Sociopolitical Dynamics in Relations between Top Managers and Security Analysts: Favor Rendering, Reciprocity, and Analyst Stock Recommendations. *Acad. Manag. J.* **2008**, *51*, 873–897. [CrossRef]
19. Sun, P.L.; Ku, C.Y.; Shih, D.H. An Implementation Framework for E-Government 2.0. *Telemat. Inform.* **2015**, *32*, 504–520. [CrossRef]
20. UNPOG. *E-Government of Korea: Best Practices*; Ministry of Public Administration and Security, National Information Society Agency: Seoul, Korea, 2009.
21. Ryu, S.H.; Jeong, D.R.; Jung, H.K. Ways to Establish Public Authorities Information Security Governance Utilizing E-Government Information Security Management System (G-ISMS). *Korea Inst. Inf. Commun. Eng.* **2013**, *17*, 769–774. [CrossRef]
22. Dhillon, G.; Backhouse, J. Current Directions in IS Security Research: Towards Socio-Organizational Perspectives. *Inf. Syst. J.* **2001**, *11*, 127–153. [CrossRef]
23. Hu, Q.; Dinev, T.; Hart, P.; Cooke, D. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decis. Sci.* **2012**, *43*, 615–660. [CrossRef]
24. Knapp, K.J.; Marshall, T.E.; Kelly Rainer, R.; Nelson Ford, F. Information Security: Management's Effect on Culture and Policy. *Inf. Manag. Comput. Secur.* **2006**, *14*, 24–36. [CrossRef]
25. Eagly, A.H.; Wood, W.; Diekman, A.B. Social Role Theory of Sex Differences and Similarities: A Current Appraisal. In *The Developmental Social Psychology of Gender*; Eckes, T., Trautner, H.M., Eds.; Psychology Press: New York, NY, USA, 2000; Volume 5, pp. 123–174.
26. Long, C.L. A Socio-Technical Perspective on Information Security Knowledge and Attitudes. Ph.D. Thesis, The University of Texas at Austin, Austin, TX, USA, September 1999.
27. Kim, S.; Choi, M. Educational Requirement Analysis for Information Security Professionals in Korea. *J. Inf. Syst. Educ.* **2002**, *13*, 237–248.
28. Kim, H.; Han, Y.; Choi, M.; Kim, S. Curriculum Design and Evaluation for E-Commerce Security Education Using AHP. *IEICE Trans. Inf. Syst.* **2007**, *90*, 668–675. [CrossRef]
29. Wylder, J. *The Life Cycle of Security Managers*; Auerbach Publication, CRC Press LLC: New York, NY, USA, 2001.
30. Luftman, J. *Managing the Information Technology Resource: Leadership in the Information Age*; Prentice Hall: Upper Saddle River, NJ, USA, 2003.

31. Chaudhry, P.E.; Chaudhry, S.S.; Reese, R.; Jones, D.S. *Enterprise Information Systems Security: A Conceptual Framework*; Møller, C., Chaudhry, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2012.
32. Moulton, R.; Coles, R.S. Applying Information Security Governance. *Comput. Secur.* **2003**, *22*, 580–584. [CrossRef]
33. Straub, D.W.; Nance, W.D. Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Q.* **1990**, *14*, 45–60. [CrossRef]
34. Straub, D.W. Effective IS security: An empirical study. *Inf. Syst. Res.* **1990**, *1*, 255–276. [CrossRef]
35. Gopal, R.D.; Sanders, G.L. Preventive and Deterrent Controls for Software Piracy. *J. Manag. Inf. Syst.* **1997**, *13*, 29–47. [CrossRef]
36. Peace, A.G.; Galletta, D.F.; Thong, J.Y. Software Piracy in the Workplace: A Model and Empirical Test. *J. Manag. Inf. Syst.* **2003**, *20*, 153–177.
37. Siponen, M.; Vance, A. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Q.* **2010**, *34*, 487–502.
38. Hu, Q.; Xu, Z.; Dinev, T.; Ling, H. Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Commun. ACM* **2011**, *54*, 54–60. [CrossRef]
39. Wiant, T.L. Information Security Policy's Impact on Reporting Security Incidents. *Comput. Secur.* **2005**, *24*, 448–459. [CrossRef]
40. Parker, D.B. *Computer Security Management*; Reston Publication, Prentice-Hall: Reston, VA, USA, 1981.
41. Avolio, B.J.; Walumbwa, F.O.; Weber, T.J. Leadership: Current Theories, Research, and Future Directions. *Annu. Rev. Psychol.* **2009**, *60*, 421–449. [CrossRef] [PubMed]
42. Yukl, G. *Leadership in Organizations*; Prentice-Hall: Upper Saddle River, NJ, USA, 2010.
43. Burns, J.M. *Leadership*; Harper & Row: New York, NY, USA, 1978.
44. Bass, B.M. *Leadership and Performance beyond Expectations*; Free Press: Collier Macmillan, NY, USA, 1985.
45. Avolio, B.J. *Leadership Development in Balance: Made/Born*; Psychology Press: Mahwah, NJ, USA, 2005.
46. Lowe, K.B.; Gardner, W.L. Ten Years of the Leadership Quarterly: Contributions and Challenges for the Future. *Leadersh. Q.* **2000**, *11*, 459–514. [CrossRef]
47. Graen, G.B.; Uhl-Bien, M. Relationship-Based Approach to Leadership: Development of Leader-Member Exchange (LMX) Theory of Leadership over 25 Years: Applying a Multi-Level Multi-Domain Perspective. *Leadersh. Q.* **1995**, *6*, 219–247. [CrossRef]
48. Avolio, B.J. *Full Leadership Development: Building the Vital Forces in Organizations*; Sage Publication: Thousand Oaks, CA, USA, 1999.
49. Judge, T.A.; Piccolo, R.F. Transformational and Transactional Leadership: A Meta-Analytic Test of Their Relative Validity. *J. Appl. Psychol.* **2004**, *89*, 755–768. [CrossRef] [PubMed]
50. Walumbwa, F.O.; Avolio, B.J.; Gardner, W.L.; Wernsing, T.S.; Peterson, S.J. Authentic Leadership: Development and Analysis of a Multidimensional Theory-Based Measure. *J. Manag.* **2008**, *34*, 89–126.
51. Liao, H.; Chuang, A. Transforming Service Employees and Climate: A Multilevel, Multisource Examination of Transformational Leadership in Building Long-Term Service Relationships. *J. Appl. Psychol.* **2007**, *92*, 1006–1019. [CrossRef] [PubMed]
52. Piccolo, R.F.; Colquitt, J.A. Transformational Leadership and Job Behaviors: The Mediating Role of Core Job Characteristics. *Acad. Manag. J.* **2006**, *49*, 327–340. [CrossRef]
53. Wang, H.; Law, K.S.; Hackett, R.D.; Wang, D.; Chen, Z.X. Leader-Member Exchange as a Mediator of the Relationship between Transformational Leadership and Followers' Performance and Organizational Citizenship Behavior. *Acad. Manag. J.* **2005**, *48*, 420–432.
54. Bass, B.M.; Avolio, B.J.; Jung, D.I.; Berson, Y. Predicting Unit Performance by Assessing Transformational and Transactional Leadership. *J. Appl. Psychol.* **2003**, *85*, 207–218. [CrossRef]
55. Schaubroeck, J.; Lam, S.S.; Cha, S.E. Embracing Transformational Leadership: Team Values and the Impact of Leader Behavior on Team Performance. *J. Appl. Psychol.* **2007**, *92*, 1020–1030. [CrossRef] [PubMed]
56. Jansen, J.J.; Vera, D.; Crossan, M. Strategic Leadership for Exploration and Exploitation: The Moderating Role of Environmental Dynamism. *Leadersh. Q.* **2009**, *20*, 5–18. [CrossRef]
57. Kahai, S.S.; Sosik, J.J.; Avolio, B.J. Effects of Leadership Style, Anonymity, and Rewards on Creativity-Relevant Processes and Outcomes in an Electronic Meeting System Context. *Leadersh. Q.* **2003**, *14*, 499–524. [CrossRef]
58. Kark, R.; Shamir, B.; Chen, G. The Two Faces of Transformational Leadership: Empowerment and Dependency. *J. Appl. Psychol.* **2003**, *88*, 246–255. [CrossRef] [PubMed]

59. Lord, R.G.; Brown, D.J. Leadership, Values, and Subordinate Self-Concepts. *Leadersh. Q.* **2001**, *12*, 133–152. [CrossRef]
60. Lord, R.G.; Brown, D.J. *Leadership Processes and Follower Self-Identity*; Psychology Press: Mahwah, NJ, USA, 2004.
61. Avolio, B.J.; Bass, B.M.; Jung, D.I. Re-Examining the Components of Transformational and Transactional Leadership Using the Multifactor Leadership. *J. Occup. Organ. Psychol.* **1999**, *72*, 441–462. [CrossRef]
62. Lowe, K.B.; Kroeck, K.G.; Sivasubramaniam, N. Effective Correlation of Transformational and Transactional Leadership: A Meta-Analytical Review. *Leadersh. Q.* **1996**, *7*, 385–425. [CrossRef]
63. Kemp, M. Beyond Trust: Security Policies and Defence in Depth. *Netw. Secur.* **2005**, *2005*, 14–16. [CrossRef]
64. Thomson, K.L.; von Solms, R. Towards an Information Security Competence Maturity Model. *Comput. Fraud Secur.* **2006**, *2006*, 11–15. [CrossRef]
65. Knapp, K.J.; Marshall, T.E.; Rainer, R.K., Jr.; Ford, F.N. Information Security Effectiveness: Conceptualization and Validation of a Theory. *Int. J. Inf. Secur. Priv.* **2007**, *1*, 37–60. [CrossRef]
66. Glaser, B.G.; Strauss, A.L. *The Discovery of Grounded Research: Strategies for Qualitative Research*; Aldine Transaction: New Brunswick, NJ, USA; London, UK, 1967.
67. Hone, K.; Eloff, J.H.P. Information Security Policy—What Do International Security Standards Say? *Comput. Secur.* **2002**, *21*, 402–409. [CrossRef]
68. Karyda, M.; Kiountouzis, E.; Kokolakis, S. Information Systems Security Policies: A Contextual Perspective. *Comput. Secur.* **2005**, *24*, 246–260. [CrossRef]
69. Hagen, J.M.; Albrechtsen, E.; Hovden, J. Implementation and Effectiveness of Organizational Information Security Measures. *Inf. Manag. Secur.* **2008**, *16*, 377–397.
70. Kankanhalli, A.; Teo, H.H.; Tan, B.C.; Wei, K.K. An Integrative Study of Information Systems Security Effectiveness. *Int. J. Inf. Manag.* **2003**, *23*, 139–154. [CrossRef]
71. Straub, D.W. Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Q.* **1998**, *22*, 441–469. [CrossRef]
72. Viator, R.E. The Relevance of Transformational Leadership to Nontraditional Accounting Services: Information Systems Assurance and Business Consulting. *J. Inf. Syst.* **2001**, *15*, 99–125. [CrossRef]
73. Podsakoff, P.M.; MacKenzie, S.B.; Moorman, R.H.; Fetter, R. Transformational Leader Behavior and Their Effects on Followers' Trust in Leader, Satisfaction, and Organizational Citizenship Behaviors. *Leadersh. Q.* **1990**, *1*, 107–142. [CrossRef]
74. Ke, W.; Wei, K.K. Organizational Culture and Leadership in ERP Implementation. *Decis. Support Syst.* **2008**, *45*, 208–218. [CrossRef]
75. Pavlou, P.A.; Fygenson, M. Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. *MIS Q.* **2006**, *30*, 115–143.
76. Chin, W.W. Issues and Opinion on Structural Equation Modeling. *MIS Q.* **1998**, *22*, 7–16.
77. Baron, R.M.; Kenny, D.A. The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations. *J. Personal. Soc. Psychol.* **1986**, *51*, 1173–1182. [CrossRef]
78. Ma, Q.; Johnston, A.C.; Pearson, J.M. Information Security Management Objectives and Practices: A Parsimonious Framework. *Inf. Manag. Comput. Secur.* **2008**, *16*, 251–270. [CrossRef]
79. Von Solms, B.; von Solms, R. The 10 deadly sins of information security management. *Comput. Secur.* **2004**, *23*, 371–376. [CrossRef]
80. Frumkin, P.; Galaskiewicz, J. Institutional Isomorphism and Public Sector Organizations. *J. Public Adm. Res. Theory* **2004**, *14*, 283–307. [CrossRef]
81. Al-Mailam, F.F. Transactional versus Transformational Style of Leadership—Employee Perception of Leadership Efficacy in Public and Private Hospitals in Kuwait. *Qual. Manag. Health Care* **2004**, *13*, 278–284. [CrossRef] [PubMed]