# Internalization of Information Security Policy and Information Security Practice: A Comparison with Compliance

Minjung Park
School of Business,
Ewha Womans University
mjpark67@ewhain.net

Sangmi Chai
School of Business,
Ewha Womans University
smchai@ewha.ac.kr

## Abstract

*Most recent information security incidents have been caused by employees' poor managements rather than technology defects. Accordingly, organizations try to improve their information security by demanding that employees conform to information security policies. Previous studies examined the effect of organization's enforcement-based systems, using penalties and rewards, on employees' comply with information security policies. It found there is a lack of autonomy and sustainability if conformity depended on external environmental factors. To confirm, following social influence theory, that employees' information security practices can be better performed if they go beyond compliance and are internalized, we developed an instrument that measures employees' attitudes on information security policies and conducted a pilot test. The results show that information security practices are performed better by the higher internalization group than by the compliance group, proving the greater effectiveness of internalization in improving both employees' and organizations' information security.*

## 1. Introduction

Recently, there has been an increase in the number of cases where organizations' information security incidents are caused by their employees' carelessness or negligence and mistakes—not by problems of technology [25]. Past incidents related to information security occurred primarily through hacking and illegal network intrusion into PCs, which can be solved and prevented via information security technologies such as anti-virus software [17]. As the number of information security related incidents caused by employees is on the rise, there is a growing need to approach the user's perspective, rather than just through technology, to devise solutions for preventing incidents. In short, as the number of incidents caused by employees not conscientiously performing information security practices as required by the organization have increased, the organization's information security has been greatly influenced by employees' willingness and attitudes [7]. In addition, Chen et al. [9] emphasized that individuals, not technology, are the main agents of information security.

Most studies on information security policies have focused on identifying whether punishments and rewards based on compulsion significantly increase employees' intention to comply with information security policies [18,32] or their awareness of information security through education and training [14,26]. Forcing employees to comply with information security policies based on these external environmental factors does not lead to continuous improvements in their intent to comply [21]. However, employees' continuous intent to comply with policies has a significant impact on their information security practices [33]. Moreover, forcing employees to comply with information security policies has little chance of improving organizations' information security because of the lack of employees' autonomy and because such coercion cannot, alone, improve their awareness of information security. Forcing employees to comply with information security policies will negatively affect organizations' information security environments and fail to motivate employees' information security practices.

According to Kelman [23], attitudes move from compliance to identification and then internalization depending on an individual's acceptance of social influences. Behaviors expressed differently at each stage influence an individual's intent to conform to specific values and norms. Therefore, employees' conformity to an information security policy, influenced by environmental effects and an acceptance of social influences, changes over time. This study asks the following research question: If employees internalize information security policies, will their intent to conform to them gradually increase and

URI: http://hdl.handle.net/10125/50484
ISBN: 978-0-9981331-1-9

finally lead to a level of information security practice higher than that achieved by employees whose attitude is merely one of compliance?

Employees internalize values and norms based on their voluntary cooperation; this increases their intent to continuously conform to whichever norm is the subject of internalization [28]. Therefore, employees' internalization of information security policies becomes the foundation not only for improving employees' awareness of information security but also for increasing the organization's information security. This study develops an instrument to examine the difference between employees' internalization of and compliance with information security policies and verifies the instrument's validity and reliability.

Results of this study provide a foundation for devising solutions to the weaknesses in employees' compliance with information security practice and for inspiring information security practice consistently based on employee autonomy.

## 2. Theoretical background

### 2.1. Social influence theory

According to social influence theory, changes in attitudes that occur as an individual conforms to values and norms by accepting social influences are behavioral processes that affect each other rather and are not strictly separable [20]. Acceptance of social influences changes behavior and attitudes through three processes: compliance, identification, and internalization. According to Kelman [23], compliance occurs when an individual accepts social influences in an attempt to receive a certain reward or avoid punishment. Identification happens when an individual perceives the importance of an issue and then shows a willingness to conform. Internalization takes place when an organization's value systems and norms coincide with those of the individual via the admission of social influences. The existence of a value subjectively perceived as useful for solving problems is a motivation to internalize [23,24]. Values congruence, whereby employees have beliefs or values consistent with the organization's goals and values, promotes employees' internalization [5]. When internalization occurs, employees change their behaviors by increasing their intent to conform, thereby experiencing a sense of achievement, which reinforces their continuous voluntary internalization activity [23,24]. This study compares between compliance and internalization to describe their effect on changes in an individual's attitude via social influence.

Andrighetto et al. [2] suggested that, as individuals internalize behaviors based on ethical autonomy, they are conforming without regard to their own self-interest. Therefore, the positive effects of norms in an organization are greater when employees internalize norms such as regulations than when they perceive and comply with norms as a means of pursuing their own interests [3]. Moreover, individuals' internalization tends to strengthen when they are free from external environmental factors. Accordingly, norms are maintained consistently through autonomy rather than through dependence on external rewards and punishment [4].

Ryan & Connell [28] described compliance and identification as low levels of internalization—attitudes at stages preceding internalization, as individuals accept social influences. They compared between the effects of two types of behavior motivation, achievement behaviors, and prosocial behaviors, and suggested that an individual's internal willingness to derive pleasure and satisfaction is a factor that triggers internalization. They also explained that compliance with rules and norms, where an individual accepts social influence, is an imperfect stage of internalization. Chirico and Salvato [10] explored the factors affecting the internalization of knowledge acquisition, a specific goal of organizational members, and emphasized the importance of social ties and interaction among members. They considered senses of trust and familiarity as forms of social capital and found that interactions and conflicts among people are the major issues affecting individuals' internalization.

### 2.2. Attitudes on information security policy

An information security policy offers a direction for information security within an organization and is a document that describes the proper use of information system resources to prevent the misuse of the information system by employees; it is the most important control measure for an organization's information security [13,19]. Herath and Rao [18] examined the major reasons for employees' intention to comply with information security policies, focusing on various internal and external environmental factors. They confirmed the importance of social influence within an organization for policy conformance. Specifically, they suggested that external environmental factors such as rewards, punishments, and peer evaluations as well as intrinsic motivations such as an employees' perception of the efficiency of security rules influence compliance with information security policies. In addition, superiors' and managers' attitudes on information security and the organizational supports available for information security also influence employees' compliance with information security policies [12]. Meanwhile, internal factors such

as employees' expertise in information security, ability to implement technologies, and interests also improve the intent to comply with information security policies [26]. Most studies on employees' conformity with information security policies have concentrated on compliance, as they have focused on how employees' attitudes on information security policies are conditioned by external environmental factors such as sanctions, rewards, and evaluations. However, Cram et al. [11] conducted a meta-analysis of research on compliance with organizations' information security policies and found that punishment and rewards did not greatly improve employees' intentions to comply and that their norms and beliefs had a strong relationship with information security practice competence. The authors concluded that employees' internalization is necessary for improving the organizations' information security, considering that employees' attitudes on information security policies are influenced more strongly by internal factors such as individuals' values and attitudes than by external factors such as rewards and punishment.

Individuals' internalization of rules and norms, going beyond the controlled external environment, can facilitate a high degree of conformity [2]. Internalization promotes strong compliance, but, since internalization is easily motivated when individuals are free from external environmental factors such as rewards, punishment, and sanctions, it cannot occur when behaviors are forced by external factors [24]. Although dividing employees' attitudes on information security policies into "compliance" and "internalization" strictly is difficult, attitudes on conformity with an organization's information security policies can be improved during the internalization stage.

The internalization of values and norms is differentiated from the form in which an individual's state of mind is endogenous to a certain subject among many others in that it is chosen under external effects [15]. According to prospect theory, an individual who internalizes a goal, instead of reaching a goal endogenously, could be more active in achieving goals [6]. This is based on the loss aversion, where individuals are generally more sensitive to losses than gains. Therefore individuals determine that among various alternatives, it chosen by them has a higher value than the others considering their effort and investment, which leads to a lower probability of abandonment [1,22]. Thus, employees require internalization to sustain their conformity to information security policies and maintain a safe organizational information security environment in a long term.

With internalization of regulations or rules, behaviors could show continuous and autonomous conformity toward them. For example, a driver stops at a red light automatically when he or she is internalized with traffic regulations. When people internalize a goal, they show a long-term effort to achieve it. A person with an internalized goal for stop smoking; for example, recovering health, could be more successful to maintain nonsmoking status longer time than a person to stop smoking for complying with a regulation or a penalty; for example, parental guide for banning smoking for their adolescent children. Based on these examples, we can extend internalization of organizational members in information security practices. If employees comply with organizational information security polices in compliance status, they abide by codes and protocols based on psychological calculations regarding rewards or penalties expected from compliance or violation. If the amount of damages they can expected from violations are smaller than benefits from compliance, they would choose violation rather than compliance. However, if employees are in internalization status, they place the purpose of their behavioral choices on information security itself so that they have tendency to show more autonomous and prolonged conformity towards protocols.

## 2.3. Information security practice behavior

Information security practices are activities that protect the organization from various threats related to information breaches and are classified as information management based on the adoption of security technology and employees' awareness of security [27]. Their technology management aspects include frequent updates of anti-virus software and systems, the deleting of browsing histories and cookies, and individual-level tasks such as refraining from accessing suspicious websites and opening suspicious emails [8,16]. Employees' information security practices are required to maximize the efficient use of procedures related to security technologies; these require investments of time and effort in the minimization of mistakes [29]. Information security practices are influenced by attitudes to and awareness of information security [31]. Therefore, improving the factors affecting employees' information security practices improves information security at both the individual and organizational levels. This study attempts to identify employees' information security behaviors, which vary depending on their attitudes to information security policies.

## 3. Research method & data analysis

### 3.1. Instrument development

This study aims to determine how information security practices differ between employees who internalize of information security policies and those who comply with them. Previous studies have focused on employees' compliance with information security policies. This study goes further by developing an instrument with which to measure employees' internalized of attitudes on those policies. In addition, to increase the effect of the comparison between complied and internalized of attitudes, questions used in previous instruments used to measure compliance with information security policies were complemented with new items. Previous questionnaires lacked a consideration of internal factors that can affect individuals' conformity behavior such as internal values and beliefs. Most of the studies assessed employees' compliance with information security policies only through external factors such as superiors' evaluations, rewards, and punishment. The recent increase in the number of information security incidents has made the information security practices required by organizations more specific, and advances in information protection software has made the technology-related policies to which organizational members must conform more detailed. To overcome the limitations of previous instruments, this study develops questions about individuals' compliance with and internalization of information security policies and performance of information security practices.

The instrument developed included a total of 11 items excepted for demographic questionnaires. Based on questions about changes in individuals' attitudes used by Kelman [23], a group of questions classified as "Attitudes on Information Security Policy" were developed to measure individuals' compliance with and internalization of information security policies. In addition, a series of questions classified as "Information Security Practice Behavior" were developed to examine individuals' information security practices as required by their organizations. All questions were measured using a seven-point Likert scale.

### 3.2. Data collection

To ensure the validity and reliability of the developed instrument and examine the difference in information security practices between employees' compliance and internalization of information security policies, a pilot test was conducted with 125 participants.

An analysis was carried out on 102 sets of valid data, excluding inappropriately answered questionnaires. The survey was conducted on workers in the fields of construction, education, and finance. The characteristics of the respondents are shown in Table 1.

**Table 1. Descriptive statistics of the respondents**

| | **Frequency (%)** |
|---|---|
| ***Gender*** | |
| Male | 63 (61.8) |
| Female | 39 (38.2) |
| ***Age*** | |
| 20 – 29 | 42 (41.2) |
| 30 – 39 | 55 (53.9) |
| 40 – 49 | 4 (3.9) |
| 50 – 59 | 1 (1.0) |
| ***Industry*** | |
| Construction | 35 (34.3) |
| Education | 23 (22.5) |
| Finance | 15 (14.8) |
| Others | 29 (28.4) |
| ***Total*** | 102 (100.0) |

### 3.3. Measurement validation

Table 2 shows the instrument developed in this study and the average responses of each question by conducting a pilot test.

An exploratory factor analysis was conducted to verify the validity and reliability of the constructs listed in Table 2. The analysis results showed that all of them are appropriate, as shown in Table 3, verifying that the data are suitable for factor analysis. First, principal component analysis was used to confirm the validity of the factor loading, and factor analysis was carried out using Varimax. As can be seen in Table 3, the value of each load factor is greater than 0.6, indicating that the scale has good construct validity.

**Table 2. Developed measurement questions**

| Construct | Measurement Indicator | Mean |
|---|---|---|
| ***Attitudes on Information Security Policy*** | **Compliance** | |
| | Q1. Complying with the organization's information security policy could decrease my work efficiency. | 3.26 |
| | Q2. If I comply with the information security policy, the organization should give me rewards accordingly. | 3.42 |
| | Q3. Even though accessing to the intranet from out of office is prohibited, I will try to access it for urgent matters. | 4.56 |
| | Q4. I think my organization enforces to me to comply with information security policy more than it is needed. | 3.69 |
| | **Internalization** | |
| | Q5. I think information security policy is needed for all organizations. | 2.21 |
| | Q6. I will comply with the information security policy to improve the organization's information security. | 2.49 |
| | Q7. I contribute to the organization by complying with its information security policy. | 2.60 |
| ***Information Security Practice Behavior*** | Q8. I immediately report to the system administrator in case of a virus infection or on receiving suspicious emails. | 3.30 |
| | Q9. I do not share my PC with co-workers even though it is needed for work convenience. | 4.46 |
| | Q10. I use different passwords for the intranet and websites separately. | 3.71 |
| | Q11. I do not use software and files that I am not allowed to take outside even for urgent matters. | 4.07 |

All communalities, which indicate the explanation ratios by extracted factors, exceeded 0.5, verifying the validity of the collected responses. In addition, Kaiser–Meyer–Olkin (KMO) and Bartlett tests were conducted to verify the adequacy of the factor analysis. In general, KMO shows the degree to which correlations between variables are explained by other variables. A low value means that the composition of variables is not adequate for factor analysis; when the value is closer to 1 and above 0.5, the data are determined to be adequate for factor analysis. In Bartlett's sphericity test, when the significance probability is lower than 0.05, the data are deemed suitable for factor analysis [30]. The reliability and validity of the measurement items developed for the study were confirmed (*KMO=.677, Bartlett p-value .000).*

This study employed the Cronbach coefficient (Cronbach's α), the most commonly used method of reliability analysis. The results show that the Cronbach's α of the internalization of and compliance with information security policy and information security practice behavior are 0.847, 0.744, and 0.793 respectively. All of them are above 0.7, indicating that this scaled questionnaire has good reliability [34].

**Table 3. Exploratory factor analysis results**

| Construct | No. | Factor Analysis | | | | Reliability |
|---|---|---|---|---|---|---|
| | | Principal component analysis with Varimax rotation(EFA) | | | Communalities | Cronbach's α |
| | | Internalization | Compliance | Information Security Practice Behavior | | |
| **Internalization** | Q5 | .681 | -.046 | .407 | .551 | 0.847 |
| | Q6 | .872 | -.066 | .276 | .795 | |
| | Q7 | .904 | .021 | .230 | .827 | |
| **Compliance** | Q1 | -.212 | .656 | .194 | .512 | 0.744 |
| | Q2 | -.331 | .683 | .080 | .687 | |
| | Q3 | .055 | .666 | -.200 | .786 | |
| | Q4 | -.491 | .764 | .467 | .569 | |
| **Information Security Practice Behavior** | Q8 | .021 | .168 | .761 | .643 | ` 0.793 |
| | Q9 | -.099 | .033 | .658 | .623 | |
| | Q10 | -.038 | .086 | .757 | .536 | |
| | Q11 | -.183 | .012 | .819 | .582 | |
| KMO | | | | | 0.677 | |
| Bartlett | | $x^2$ | | | 293.524 | |
| | | *df* | | | 55 | |
| | | *Sig.* | | | ***< 0.001*** | |

## 3.4. Results

An independent samples T-test (see Table 4) was performed to examine the difference in information security practice between employees' compliance with and internalization of information security policies based on the developed measurement. The analysis showed that the mean of information security practice when information security policies were internalized was 4.45, statistically significantly higher than the mean value (3.67) of the group with a compliance attitude *(p=0.002).* The study results thus confirmed that the difference between employees' compliance with and internalization of information security policies has a significant effect on information security practices: Employees' information security practice increases when they internalize information security policies and is higher than for those who only ensure compliance.

**Table 4. T - test results**

| x | Information Security Practice Behavior | | *t* | *Sig.* |
|---|---|---|---|---|
| | **Mean** | **S.D** | | |
| **Compliance** | 3.67 | 1.07 | - 3. 213 | ***.002*** |
| **Internalization** | 4.45 | 1.14 | | |

$^{**}p < 0.01$

## 4. Discussion

### 4.1. Theoretical implications

This study has several theoretical implications for information security. First, we applied concepts drawn from social influence theory and adapted them to measure employees' attitudes on information security policies. Prior research using social influence theory has focused on certain ethical norms and values. However, this study suggests the need to apply social influence to regulations and information security policy. Internalization is accompanied by autonomy and persistence, which are important for efficient behaviors. Secondly, this study demonstrates the need to expand information security-related regulations and disciplines by empirically verifying the effects of employees' internalization on information security policies. The instrument developed in this study can be used as the foundation for expanding the scope of research on employees' intention to conformity with information security policies. Previously developed instruments have limitations because they do not reflect the recent information security environments and do not consider employees' distinctiveness in organizations. However, this study includes for recent organizations' information security environments (e.g., blocking employees' access to intranet outside office or forbidding bring out official documents to outside). Finally, this study also overcomes limitations of the prior literature which mainly focused on extrinsic factors such as sanctions and rewards affects to employees' conformity with information security policy by discussing intrinsic factors. As a result, this study shows, now we have to consider employees' awareness and values of information security for identifying their motivations and attitudes on information security.

### 4.2. Practical implications

As organizational information security breaches have increased in recent years, the importance of finding ways of increasing employees' conformity with information security policies has also increased. The results of this study show that employees' internalization of information security policies is a major factor in enhancing both individual information security practices and organizations' information security environments. Finally, this study suggests future directions that firms could take to establish effective strategies in information security. It means firms have to consider how can inspire employees' awareness of information security when they establish firms' information security policy which can enhance their internalization of its policy. It is important because inspiring the intent to internalize of employees' information security policy can advance employees' continuous and autonomous conformity with it. In a long-term perspective, it can save firms' operation costs stems from enforcement-based systems (imposing penalties or rewards through monitoring employees' information security behaviors all the time). Developed instrument in this study also can be used for evaluating employees' attitudes on information security policy in their organizations in internalization perspectives.

### 4.3. Limitations and future research

The measurement was developed and used to conduct a pilot test on approximately 100 people, in this study, should be complemented and revised. We have a plan to enhance the elaboration of the questionnaires in the future. As this study found that employees' internalization of information security policies has a positive effect on information security practice, further research should focus on identifying factors that promote and undermine employees' internalization, based on developed and complemented instruments. Such a future research will provide a direction for establishing an organizational environment that can improve employees' internalization of information security policies and thus serve as a foundation for strengthening information security at both individual and organization.

## 5. Conclusions

This study developed an instrument with which to compare practices driven by employees' compliance with information security policies with those driven by internalization and verified its reliability and validity. The results found that the questionnaires developed were all suitable for measuring the employees' internalization of, and compliance with, information security policies, and that when their attitudes on information security policies were internalized, the level of information security practice was higher than when the policies were just complied with. Therefore, this study suggests that organizations should devise solutions to inspire employees' internalization of information security policies. This is because it is impossible to fundamentally improve the employees' and organizations' information security when employees' are enforced to conform to information security policies by external environmental factors, as the attitude of compliance lacks sustainability and autonomy. As previous studies found that the congruence between values or goals toward a subject is the main cause of internalization. When employees' have a value system that is similar to the goals of organizations' information security policy, internalization is accomplished and its effect is maximized, improving the employees' and organizations' information security. Therefore, this study proposes organizations have to establish information security policy considering employees' attitudes and the appropriate ways of requiring their conformity of information security policy.

## References


[1] Abdellaoui, M., H. Bleichrodt, and C. Paraschiv, "Loss Aversion under Prospect Theory: A Parameter-Free Measurement," Management Science, Publisher, Location, 2007, pp. 1659-1674

[2] Andrighetto, G., D. Villatoro, R. Conte, and J. Sabater Mir, "Simulating the Relative Effects of Punishment and Sanction in the Achievement of Cooperation," Proceedings of 8th European Workshop on Multi-Agent Systems, 2010.

[3] Andrighetto, Giulia, Daniel Villatoro, and Rosaria Conte. "Norm internalization in artificial societies." *Ai Communications* 23.4 2010, pp. 325-339.

[4] Aronfreed, J., Conduct and Conscience: The Socialization of Internalized Control over Behavior, Elsevier, Location, 2013.

[5] Bagozzi, R. P., and U. M. Dholakia, "Intentional Social Action in Virtual Communities," Journal of Interactive Marketing, Publisher, Location, 2002, pp. 2-21.

[6] Bargh, J. A., P. M. Gollwitzer, A. Lee-Chai, K. Barndollar, and R. Trötschel, "The Automated Will: Nonconscious Activation and Pursuit of Behavioral Goals," Journal of Personality and Social Psychology Publisher, Location, 2001, p. 1014.

[7] Bulgurcu, B., H. Cavusoglu, and I. Benbasat, I, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," MIS Quarterly, Publisher, Location, 2010, pp. 523-548.

[8] Chai, S., S. Bagchi-Sen, C. Morrell, H. R. Rao, and S. Upadhyaya, "Role of Perceived Importance of Information Security: An Exploratory Study of Middle School Children's Information Security Behavior," Issues in Informing Science and Information Technology, Pulisher, Location,2006, pp. 127-135.

[9] Chen, C. C., B. Dawn Medlin, and R. Shaw, "A Cross-Cultural Investigation of Situational Information Security Awareness Programs," Information Management & Computer Security, Publisher, Location, 2008, pp. 360-376.

[10] Chirico, F., C. and Salvato, "Knowledge Internalization and Product Development in Family Firms: When Relational and Affective Factors Matter," Entrepreneurship Theory and Practice, Publisher, Location, 2016, pp. 201-229.

[11] Cram, W. A., J. Proudfoot, and J. D'Arcy, "Seeing the Forest and the Trees: A Meta-Analysis of Information Security Policy Compliance Literature," Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.

[12] D'Arcy, J., and G. Greene, "Security Culture and the Employment Relationship as Drivers of Employees' Security Compliance," Information Management & Computer Security, Publisher, Location, 2014, pp. 474-489.

[13] D'Arcy, J., and A. Hovav, "Deterring Internal Information Systems Misuse," Communications of the ACM, Publisher, Location, 2007, pp. 113-117.

[14] D'Arcy, J., A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research, Publisher, Location, 2009, pp. 79-98.

[15] Gintis, H., "The Hitchhiker's Guide to Altruism: Gene-Culture Coevolution, and the Internalization of Norms," Journal of Theoretical Biology, Publisher, Location, 2003, pp. 407-418.

[16] Gross, R., and A. Acquisti, "Information Revelation and Privacy in Online Social Networks," Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society: ACM, Publisher, Location, 2005, pp. 71-80.

[17] Harrington, S. J., "A Test of a Person--Issue Contingent Model of Ethical Decision Making in Organizations,Journal of Business Ethics, Publisher, Location, 1997, pp. 363-375.

[18] Herath, T., and H. R. Rao, "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," Decision Support Systems, Publisher, Location, 2009, pp. 154-165.

[19] Höne, K., and J. H. P. Eloff, "Information Security Policy—What Do International Information Security Standards Say?" Computers & Security, Publisher, Location, 2002, pp. 402-409.
[20] Horne, C., "Explaining Norm Enforcement," Rationality and Society, Publisher, Location, 2007, pp. 139-170.
[21] Hu, Q., T. Dinev, P. Hart, and D. Cooke, D. "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," Decision Sciences, Publisher, Location, 2012, pp. 615-660.
[22] Kahneman, D., A. and Tversky,"Prospect Theory: An Analysis of Decision under Risk," Econometrica: Journal of the Econometric Society, Publisher, Location, 1979, pp. 263-291.
[23] Kelman, H. C., "Compliance, Identification, and Internalization Three Processes of Attitude Change," Journal of Conflict Resolution, Publisher, Location, 1958, pp. 51-60.
[24] O'Reilly, C. A., and J. Chatman, "Organizational Commitment and Psychological Attachment: The Effects of Compliance, Identification, and Internalization on Prosocial Behavior," Journal of Applied Psychology, Publisher, Location,1986, p. 492.
[25] Pahnila, S., M. Siponen, and A. Mahmood, "Employees' Behavior Towards IS Security Policy Compliance," System Sciences, 2007. HICSS 2007. 40Th Annual Hawaii International Conference on: IEEE, Publisher, Location2007, pp. 156b-156b.
[26] Puhakainen, P., and M. Siponen, "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," Mis Quarterly, Publisher, Location, 2010, pp. 757-778.
[27] Rhee, H.-S., C. Kim, and Y. U. Ryu, "Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior," Computers & Security, Publisher, Location, 2009, pp. 816-826.
[28] Ryan, R. M., and J. P. Connell, "Perceived Locus of Causality and Internalization: Examining Reasons for Acting in Two Domains," Journal of Personality and Social Psychology, Publisher, Location, 1989, p. 749.
[29] Siponen, M. T., "A Conceptual Foundation for Organizational Information Security Awareness," Information Management & Computer Security, Publisher, Location, 2000, pp. 31-41.
[30] Tabachnick, B. G., L. S. Fidell, and S. J. Osterlind, Using Multivariate Statistics,Publisher, Location, 2001.
[31] Thomson, M. E., and R. von Solms, "Information Security Awareness: Educating Your Users Effectively," Information Management & Computer Security, Publisher, Location,1998, pp. 167-173.
[32] Vance, A., M. Siponen, and S. Pahnila, "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," Information & Management, Publisher, Location, 2012, pp. 190-198.
[33] Warkentin, M., A. C., J. Shropshire, and W. D. Barnett, "Continuance of Protective Security Behavior: A Longitudinal Study," Decision Support Systems, Publisher, Location, 2016, pp. 25-35.
[34] Cortina, Jose M. "What is coefficient alpha? An examination of theory and applications." Journal of applied psychology, 1993, pp. 98