Employees' Behavior towards IS Security Policy Compliance

Seppo Pahnila[a], Mikko Siponen[a] and Adam Mahmood[b]
[a]University of Oulu, Department of Information Processing
Science, Linnanmaa, P.O.BOX 3000, FIN-90014 Oulun yliopisto, FINLAND.
E-mail:{Mikko.Siponen, Seppo.Pahnila}@oulu.fi
[b]Department of Information and Decision Sciences, University of Texas at El Paso
E-mail: mmahmood@utep.edu

Abstract

The literature agrees that the major threat to IS security is constituted by careless employees who do not comply with organizations' IS security policies and procedures. To address this concern, different approaches for ensuring employees' IS security policy compliance have been proposed. Prior research on IS security compliance has criticized these extant IS security awareness approaches as lacking theoretically and empirically grounded principles to ensure that employees comply with IS security policies. To fill this gap, this study proposes a theoretical model that contains the factors that explain employees' IS security policy compliance. Data (N=245) from a Finnish company provides empirical support for the model. The results suggest that information quality has a significant effect on actual IS security policy compliance. Employees' attitude, normative beliefs and habits have significant effect on intention to comply with IS security policy. Threat appraisal and facilitating conditions have significant impact on attitude towards complying, while coping appraisal does not have a significant effect on employees' attitude towards complying. Sanctions have insignificant effect on intention to comply with IS security policy and rewards do not have a significant effect on actual compliance with IS security policy.

1. Introduction

The importance of information systems (IS) security has increased as witnessed by the increasing number of IS security incidents that organizations have encountered within the last few years. While in 1997-1999 surveys, 37-50% of the organizations were victims of IS security breaches [46, 17 p. 188-189], the respective numbers in the years 2001-2003 ranged from 75% to 91% [4 p. 684, 16 p. 438-439]; Hinde [21 p. 310].

To cope with increased IS security threats, different security measures have been proposed, from technical protection means (e.g., anti-virus software tools) to different information management standards, secure systems design methods and IS security policies [12, 39, 51]. Employees, however, seldom comply with these IS security procedures and techniques, placing the organizations' assets and business in danger [42 p. 125]. Hence, effective IS security requires that employees are not only aware of, but also comply with the IS security policies and guidelines. To address this crucial IS security concern, different approaches for ensuring employees' IS security policy compliance have been proposed. Aytes and Connolly [3] and Siponen [38] have criticized extant IS security awareness approaches as lacking not only theoretically grounded methods, but also empirical evidence on their effectiveness. This paper addresses these important weaknesses by first building a theoretical model explaining how employees' compliance with IS security policies and guidelines can be improved. Then the model is validated using an empirical study.

The rest of the paper is organized as follows: the second section reviews related research studies. The third section proposes the research model, fourth discusses the data collection procedure. The empirical results of the study are presented in the fifth section. Sixth section discusses the implications of the study for research and practice.

2. Previous work on IS security behavior and compliance

Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07)
0-7695-2755-8/07 $20.00 © 2007 IEEE
1530-1605/07 $20.00 © 2007 IEEE

The previous research studies regarding compliance with IS security policies and guidelines can be divided into three categories: (1) conceptual principles; (2) theoretical models without empirical support; and (3) empirical support grounded upon theories. These studies are discussed next.

Studies belonging to the category of conceptual principles, present different practical principles and suggestions for improving employees' compliance with IS security polices. These principles are not theoretically grounded, and they do not present empirical evidence to support their principles and suggestions. These studies include IS security awareness programs for university context by Kajava and Siponen [25], Sommers and Robinson [40 p. 379] and McCoy and Fowler [31 p. 347] and an IS security awareness programs by Perry [34, pp. 94-95], Spurling [41 p. 20], Parker [33, p. 466] and Thomson and von Solms [47]. These studies also include information security awareness programs for improving IS security policy compliance in healthcare contexts by Gaunt [18] and Furnell, Sanders and Warren [17] and Katsikas [26], McLean's [32 p. 180] IS security campaigns to improve IS security policy compliance. Like Wood's [53] 53 tips for ensuring that employees comply with IS security procedures. Also scholars have suggested that practitioners can educate users through IS security training software [14], [15] and by making IS security features more user friendly [16].

Theoretical models without empirical support contain studies that contribute to the creation of theoretical insights on how employees' IS security policy compliance can be increased. These studies, however, do not offer empirical evidence to support these models or suggestions. These studies include Aytes and Connolly's [3] testable model aimed at explaining why users engage in behavior that violates IS security policies, psychological frameworks by Siponen [38], Thomson and von Solms [47] and Lee and Lee's [28] model of computer abuse, based the social bonds theory, the theory of planned behavior, the social learning theory and the general deterrence theory.

Regarding empirical studies grounded upon theories, Straub [44] and Straub and Welke [45] use the general deterrence theory to investigate whether management investment in IS security measures reduces computer abuse. Weekly hours dedicated to IS security and security in general, dissemination of IS security polices and guidelines, stating penalties for non-compliance, and the use of IS security software were found to be most effective IS security deterrents [44 pp. 272-273].

Woon et al. [54] studied what factors explain the usage of security features among those home PC users that have a wireless network. They found that perceived severity of the IS security threat, effectiveness of response, perceived capability to use the security features (self-efficacy) and the cost of using the security features (response cost) affect home users' decisions on whether or not to use security features..

To summarize the findings of the literature review, while several approaches for ensuring employees' IS security policy compliance exist, only three approaches incorporate a theoretically and empirically grounded model. Of these two approaches, one by Woon et al. [54] study wireless network users, while the other by Straub [44] focuses on deterrence theory. With the exception of the study by Straub [44], these approaches for ensuring employees' IS security policy compliance do not offer an exploratory model or evidence that explains why employees in organizations do not comply with IS security guidelines and what factors affect employees' IS security policy compliance. This study aims to fill this gap.

3. The Research Model

The theoretical model (Figure 1) for the study combines General Deterrence Theory, Protection Motivation Theory, the Theory of Reasoned Action, Information Systems Success, and Triandis' Behavioral Framework [49] and Rewards.

The central factors of our model are: attitude towards compliance, intention to comply and actual compliance with IS security policies. They are based on the widely used and accepted Theory of Reasoned Action (TRA) [13]. Attitude indicates a person's positive or negative feelings toward some stimulus object [1]. According to Ajzen [1], intentions captured the motivational factors that influence a behavior, and they indicate how hard people are willing to try to perform the behavior in question. According to TRA, the stronger the intention to carry out a behavior, the more likely the behavior will be carried out. In our study, the more stronger the intention to comply with IS security policies is, the more likely the individual will actually comply with the policies.

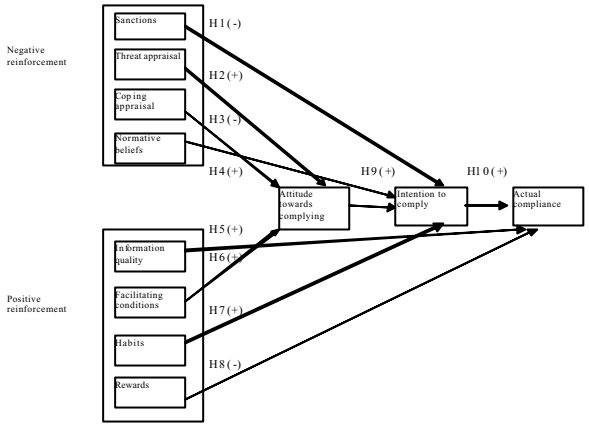

Figure 1. Theoretical model for employees' IS security policy compliance.

Sanctions. Sanctions come from the General Deterrence Theory. This theory suggests that certainty, severity, and celerity of punishment affect people's decision on whether they commit a crime or not [45]. Straub [44] found that stating penalties for IS security policy non-compliance increases security behavior. Studies by Straub [44] and Straub and Welke [45] employ what Higgins et al. [20] call as the classical deterrence theory. These seminal studies [44, 45] do not, however, address two important components of contemporary General Deterrence Theory, namely social disapproval, self-disapproval and impulsivity [18]. This leads to the following hypothesis:

H1. Sanctions affect an employees' intention to comply with IS security policies.

Threat appraisal and coping appraisal. According to Woon et al. [54], threat appraisal consists of two dimensions: perceived vulnerability and perceives severity. Woon et al. [54 p. 369] utilize the concept of perceived vulnerability in the context of home users, from Rogers [36], to refer to one's assessment of the probability that s/he is exposed to a threat. Applying this idea to the question of non-compliance with IS security policies by employees, we use the concept of perceived vulnerability to refer to employees' assessment of whether their organization is confronted by IS security threats. The assumption is that if employees do not see that they are truly confronted by IS security threats, they will hardly comply with IS security guidelines. Perceived severity refers to the consequences to individuals if a security threat occurs [54 p. 369]. Like perceived vulnerability, Woon et al. [54] derive this concept from the protection motivation theory by Rippetoe and Rogers [35]. In developing this concept, as an example, they used identity stealing and email eavesdropping through hacking among home wireless users ..

Coping appraisal is a measure consisting of three dimensions: response efficacy, self efficacy, and response cost [36, 54]. Response efficacy relates to the belief in the perceived benefits of the action [36]. Carrying out action may remove the threat. In our study, it means that complying with security policies is an effective mechanism for detecting a threat. In a computer environment, two sets of controls can be identified: people can control their own beliefs and behavior, and they can control their environment. They want to control different resources such as time, money and/or they want to control information. Self-efficacy emphasizes the individual's ability or judgment of their capabilities to cope with the task ahead [6]. The self-efficacy theory suggests that if organizations can increase employees' self-efficacy, judgment about their abilities to cope successfully with the tasks ahead, this can improve their efficiency [6]. Response costs are the costs, which results from individual's behavior. Results of the recommended behavior may lead to, for example, monetary expense, inconvenience, embarrassment or other negative consequences [54].

We postulate that threat appraisal and copying appraisal are an important factors in explaining employees' attitude toward complying with IS security policies. This assumption is based on the idea that if employees see that non-compliance with IS security policies is perceived to jeopardize IS security, they are more likely to follow the IS security policies. Therefore, we hypothesize:

H2. Threat appraisal affects employees' attitude toward complying with IS security policies.

H3. Coping appraisal affects employees' attitude towards complying with IS security policies.

Normative beliefs reflect normative expectations of peers or colleagues [13]. Aydin [2] suggests that individuals create their behavior based on the interaction with each other. Thus, membership of a social environment or the influence of important people may have a persuasive influence on whether or not to perform a specific behavior. With respect to compliance with IS security policies and guidelines, colleagues' or managers' positive attitudes toward complying with the rules may guide other people's attitudes, leading to positive behavior. Hence, we hypothesize:

H4. Normative beliefs affect employees' intention to comply with IS security policies.

Information quality. DeLone and MacLean [11] have identified six information success features: system quality, use, user satisfaction, individual impact, organizational impact and information quality. Information quality was seen as one key determinant for identifying the factors which may affect the success of information systems. Previous research has developed numerous measures of information quality and identified various constructs. Larcker and Lessig [27] developed a measure consisting of two dimensions: perceived importance of information and perceived usefulness of information. Perceived importance of information identifies factors such as relevance, informativeness, meaningfulness, importance, helpfulness and significance. Perceived usefulness consists of factors such as unambiguity, clarity and readability. Ives et al. [22] developed a standard instrument to measure user information satisfaction, based on 39 computer user satisfaction factors suggested by Bailey and Pearson [5]. Wang and Strong [52] determined 20 information quality dimensions (e.g., value-added, relevancy, accuracy, and ease of understanding) based on data collected from information consumers. Kahn et al. [23] divided information quality into product quality and service quality. While these are considered to have different characteristics, both of them have both tangible and intangible aspects. As a result of the study, Kahn [24] mapped sixteen different dimensions of information quality, accessibility, completeness, relevancy and timeliness, to four quadrants: sound, dependable, useful and usable Lee et al. [29] developed a methodology for assessment and improvement of information quality (AIMQ) in organizations, having fifteen different dimensions of information quality.

Given that information quality relates to user satisfaction with the usefulness of information [22], we suggest that information quality matters to IS security policy compliance. After all, IS security policies are ultimately information spread through different channels (e.g., emails, Intranet or on paper). Therefore, it is expected that the perceived quality and usefulness of the information within IS security policies will explain whether an employee will comply with IS security policies and guidelines. Thus, we hypothesize:

H5. The information quality of the IS security policy affect the actual compliance with IS security policies.

Facilitating conditions. According to Triandis [49], facilitating conditions are objective factors that observers agree to make a task easy to accomplish. The more resources and opportunities individuals believe they possess, the more easier for them to accomplish a task. The existence of a supportive organizational and technical infrastructure is the key to enhancing favorable facilitating conditions [50]. In the context of the present research, it is assumed that facilitating conditions has a positive influence on the intention to comply with IS security policies. If employees lack appropriate facilitating conditions, such as time to get acquainted with security policies, or they do not have easy access to the policies, or they do not get support on how to comply with security policies, they are unlikely to comply with the IS security policies. Hence, we hypothesize:

H6. Facilitating conditions affect employees' attitude towards complying with IS security policies.

Habits. A habit is unconscious or automatic behavior, as opposed to intentions or conscious behavior [30 p. 71, 46]. Based on the model by Triandis [49], habits are found to explain IS usage [30, 10]. It is argued that the influence of habits on actual behavior increases in the long run, while the influence of behavioral intentions decreases [30 p. 84] in the long run. Hence, Limayem and Hirt [30 p. 84] propose that technology use can be made habitual through making it mandatory initially or introducing rewards and other incentives for the use of the technology. Following this lead, we suggest that habitual behavior explains IS security policy non-compliance. Hence, we hypothesize:

H7. Habits affect an employee's intention to comply with IS security policies.

Rewards. Rewards can be used as effective means for cultivating interest and increasing motivation and performance [8 p. 20]. Rewards can be tangible (e.g., money, gold stars, medals, awards) or intangible (praise by peers) - the use of rewards is individual: what may work as reinforcement for one person may not work for another person [8 p. 24]. Considering employees' attitude and intention toward actual compliance, we can hypothesize:

H8. Rewards affect employees' actual compliance of the security policies

H9. Employees' attitude towards complying with IS security policies have a significant impact on intention to comply with IS security policies.

H10. Employees' intention to comply with IS security policies have a significant impact on actual compliance with IS security policies.

4. Research methodology and settings

To maximize measurements reliability with respect to the constructs of our research, we selected items that have been tried and tested by extant research, if and when available. According to Straub [43] and Boudreau et al. [7], using validated and tested questions will improve the reliability of results. Habits are generated from the studies by Triandis [49] and Limayem and Hirt [30]. Facilitating conditions are based on the questionnaire items developed by Limayem and Hirt [30] and Cheung et al. [9]. Normative beliefs are taken from the study by Karahanna and Straub [25]. Information quality is measured by using the item scale proposed by Lee et al. [29]. Sanctions are modified from [20] and Rewards are taken from [8]. Scale items on Threat appraisal and Copying appraisal are generated from Roger and Prentice-Dunn [37]. All the items are measured using seven-point Likert scale (strongly disagree – strongly agree). Since these measures are originally tested in different context (they are not used for policy compliance) and cultures, we saw the need to test the measures in IS security context and in the Finnish culture. Accordingly, the web-based questionnaire was piloted with 15 IT users to increase content validity [43]. Based on their feedback, we improved the readability of the questions.

The data used in the paper were collected in a Finnish company using a web-based questionnaire aiming at testing our research model presented in Fig. 1. The company's businesses include food and groceries, specialty goods, hotels and restaurants, hardware and agriculture, automobiles and service stations. Seven hundred fifty respondents were asked to fill out the web-based questionnaire. Two hundred forty five respondents filled out the questionnaire. Five respondents answered only the demographic questions. Thus, the total sum of reliable responses was 240.

Selection bias is important to consider because it has an effect on the generalizability of the results. Selection bias occurs when the respondents of the study are not "real" or relevant representatives of the sample [3]. As Table 1 show, gender and age groups of the respondents were quite equally distributed. Moreover, respondents covered a wide geographical area. Although these issues are important aspects with respect to minimizing bias [4], it is quite obvious that the selection bias has to be taken into consideration as a limitation in generalizing the results of the study.

5. Data collection

Table 1 summarizes respondents' descriptive statistics. The demographic data shows that the number of male (49.4%) and female (50.6%) are rather equally distributed. Most of the respondents are middle-aged, 38.4% representing the age group 31-40 and 31.4% representing the age group 41-50. The respondents held executive responsibility (46.5%), specialist (11.4%) and managerial (9.0%) positions. In Table 2 is depicted the descriptive data of the model variables.

Table 1. Descriptive statistics of the respondents

Measure	Items	Frequency	Percent
Gender	Male	121	49.4
	Female	124	50.6
Age	<30	27	11
	31-40	94	38.4
	41-50	77	31.4
	>50	47	19.2
Organizational Level	Manager	22	9.0
	Secretary	9	3.7
	Assistant	11	4.5
	Executive	114	46.5
	Specialist	28	11.4
	Planner	10	4.1
	Trainer	3	1.2
	Sales and service	12	4.9
	Others	36	14.7

Table 2. Mean and standard deviation of the variables (N=241).

Variable	Mean	Standard deviation	Min	Max
Actual compliance	1.4681	0.73176	1.00	5.00
Intention to comply	1.3710	0.71790	1.00	5.33

Attitude towards complying	1.5969	0.80136	1.00	6.00
Habits	1.7894	0.86740	1.00	6.00
Facilitating conditions	4.6289	1.51287	1.00	7.00
Normative beliefs	1.4759	0.81135	1.00	5.00
Information quality	2.8540	1.13182	1.00	6.50
Sanctions	3.8871	1.66014	1.00	7.00
Threat appraisal	2.3300	0.94535	1.00	6.00
Coping appraisal	3.0247	1.39409	1.00	7.00
Rewards	5.0385	1.43062	1.67	7.00

Factor analysis is used to reveal the latent structure of the independent variables. The distribution of all the variables of the structure was analyzed, which showed that all the variables included in the structure were normally distributed. The number of factors was extracted using Kaiser's criterion, that is, factors having eigenvalues greater that 1 were accepted in the solution. All eight factors accounted for 72.9% of the total variance. Moreover, Cattle Scree test results were used for the acceptance of the solution. According to the Cattle Scree test, the optimum number of factors can be found at the turning point of the downward curve where the curve first begins to straighten. When the curve is nearly a straight line, the variance is mostly random variance (error variance) [5]. Analyses were executed using the principal component extraction method followed by Varimax rotation. We assessed the convergent validity by using Cronbach's alpha and factor analysis assessing the discriminant validity. All the factor loadings exceeded 0.50. There was no cross-construct loading that exceeded 0.50. Reliability analysis was used to assess the consistency of the factors. According to Hair et al. [19], the widely accepted lower limit for Cronbach's alpha is 0.70. As shown below, Cronbach's alpha has high coefficients. Some variable items were dismissed on the basis of item-to-total correlation because of poor reliability.

Table 3. Factor analysis results.

Factors	Items	Factor loading	Cronbach's alpha
Information quality	infq1	0.785	0.918
	infq2	0.834	
	infq3	0.822	
	infq4	0.760	
	infq5	0.695	
	infq6	0.855	
Normative beliefs	normbel1	0.896	0.899
	normbel2	0.879	
	normbel3	0.711	
	normbel4	0.784	
Sanctions	sanctio1	0.930	0.906
	sanctio2	0.938	
	sanctio3	0.918	
	sanctio4	0.576	
Habits	habit1	0.861	0.931
	habit2	0.846	
	habit3	0.849	
Threat appraisal	thrappr1	0.606	0.729
	thrappr2	0.618	
	thrappr3	0.730	
	thrappr4	0.613	
	thrappr5	0.602	
Copying appraisal	copappr1	0.840	0.798
	copappr2	0.882	
	copappr3	0.758	
Facilitating conditions	facicon1	0.620	0.713
	facicon2	0.758	
	facicon3	0.751	
Rewards	rewards1	0.693	0.733
	rewards2	0.836	
	rewards3	0.813	

We also assessed the intercorrelation among the factors. All the correlation coefficients were less than 0.80, which is normally considered as a critical value [5]. If the correlation coefficient is too high, it may mean that there could be the problem of multicollinearity. According the analysis, it seems that the problem of multicollinearity does not have negative effects on further analyses. In this research, multiple regression analysis is used as an extension of factor analysis, aiming at finding a model that describes the phenomena under study as comprehensively as possible and estimates the compatibility of the research model and the collected research data. The results of regression analysis are shown in Table 4. As Table 4 shows, the first model explains 8.0 percent (R^2 = 0.08) of the variance of the model. Threat appraisal (thrappr ß=0.278, t-value 4.510, p=0.001) and facilitating conditions (facicont ß=-0.201, t-value -3.270, p=0.001) have a significant direct effect on attitude towards complying. Coping appraisal (copappr) does not have a significant effect on attitude towards complying.

In the second multiple regression analysis the model explains 64.9% of the variance. Attitude (atti), normative beliefs (normbel) and habits have a significant effect on intention to comply IS security policies. The effect of sanctions on intention to comply was not significant. This is interesting, recognizing that 40,2 % of the respondents viewed that they will be punished, if they do not follow security policies and guidelines, and 88,2 % of the respondents viewed that they will feel guilty for IS security policy non-compliance, and 61,4% saw that problem for them if their peers found out that they did not follow IS security policies.

In the third regression analysis, the amount of variance explained by the model was 79.3 percent. Intention has a strong significant influence on actual compliance (ß=0.869, t-value 27.977, p=0.001). Also information quality has a significant effect on actual compliance, whereas rewards have no significant effect on actual compliance. This was the case in spite of the fact that 33 % of the respondents indicated that they will be praised (an intangible award), if they comply with IS security policies. The respondents did not, however, receive a tangible reward for compliance.

Table 4. Results of the regression tests. First variable of each test is dependent variable.

Regression test	R^2	F-value	Standardized coefficient ß	t-value	Sig.	Hypothesis result
1. Attitude towards complying	0.080	15.920(*				
thrappr			0.278	4.510	0.000	supported
facicont			-0.201	-3.270	0.001	supported
copappr						not supported
2. Intention to comply	0.649	142.987(*				
attitu			0.537	8.773	0.000	supported
normbel			0.235	4.969	0.000	supported
habits			0.141	2.349	0.020	supported
sanctions						not supported
3. Actual compliance	0.793	452.775(*				
Intent			0.869	27.977	0.000	supported
Infq			0.072	2.330	0.021	supported
rewards						not supported

6. Discussion

We found that information quality has a significant effect on actual IS security policy compliance. Attitude, normative beliefs and habits have significant effect on intention to comply with IS security policies. Threat appraisal and facilitating conditions have significant impact on attitude towards complying, while coping appraisal does not have a significant effect on attitude towards complying. Sanctions do not have a significant effect on intention to comply and rewards do not have a significant effect on actual compliance. These findings offer new insights for practice and research. For practitioners, the findings highlight the role of positive incentives and influence on compliance.

Habits has a significant effect on intention to comply with IS security policies. Following a suggestion by Limayem and Hirt [30 p. 84] regarding technology use, it is important to IS security staff to get their organization's employees into the habit of complying with IS security policies. The other factors, described next, are important in this process. To start with, practitioners need to make sure that guidance and help from superiors and security staff are easily available to employees, if they encounter difficulties in complying with IS security policies (facilitating conditions).

On the basis of our findings, practitioners should realize that positive social pressure (normative belief) towards IS security policy compliance from top management, immediate supervisor, peers and IS security staff is important for ensuring employees' IS security policy compliance. This is consistent with the findings that social environment has an effect on individuals' behavior [2]. To ensure positive social pressure, top management, immediate supervisors and

IS security staff should clearly and explicitly note the importance of complying with IS security polices.

The information quality of the IS security policy also affects the actual compliance with IS security policies. For IS security practitioners, this means that the information security policy should be quickly accessible and it is very important that employees can quickly find the information that they need from IS security polices. Also, the amount of information on IS security policies must be sufficient for employees' needs. For example, IS security policy documents cannot be too long or too short. Our findings also suggest that it should be easy for employees to interpret IS security policies. This means, for instance, that the language used in IS security policy must be easy to understand for employees. It is also important to ensure that the information on IS security policy is perceived relevant to employees' work and information on IS security policy is sufficiently up-to-date for their work.

Threat appraisal has a significant effect on attitude towards complying with IS security policies. It is, therefore, important that employees are made aware of the IS security threats and their severity and celerity for the organization by IS security staff. For example, email messages, seminars, posters, and articles in newsletters can be used to disseminate such information.

Practical wisdom [33] and previous studies in IS security highlight the role of sanctions [44]. According to our findings, sanctions, derived from General Deterrence Theory, do not affect significantly intention to comply with IS security policies.

One possible explanation for rewards' not having significant effect on actual behavior is that there were no tangible award system used in the organization. Therefore, future research is needed to study organizations that use a tangible reward system to facilitate IS security policy compliance. Also, future research is needed to see whether one can generalize these findings across a larger population.

7. Conclusions

Careless employees are a key threat to IS security. Hence, users not only have to be aware, but also comply with organizations' IS security policies and procedures. To address this important concern, different approaches for IS security policy compliance have been suggested. Prior research on IS security compliance has criticized these extant IS security approaches as lacking theoretically and empirically grounded principles to ensure that employees comply with IS security policies. This study synthesized a model in order to explain employees' IS security compliance. The results suggest that information quality has a significant effect on actual IS security policy compliance. Attitude, normative beliefs and habits have significant effect on intention to comply with IS security policies. Threat appraisal and facilitating conditions have significant impact on attitude towards complying, while coping appraisal does not have a significant effect on attitude towards complying. Sanctions do not have a significant effect on intention to comply with IS security policy and rewards do not have a significant effect on actual IS security policy compliance. Future empirical research is needed to test the model further by using a different population.

References

[1] Ajzen, I., "The Theory of Planned Behavior", Organizational Behavior and Human Decision Processes 50,2, 1991, 179-211.

[2] Aydin, C. E. and Rice, R. E., "Social worlds, individual differences, and implementation. Predicting attitudes toward a medical information system", Information & Management 20, 1991, 119-136.

[3] Aytes, K. and Connolly, T., "A Research Model for Investigating Human Behavior Related to Computer Security", Proceedings of the 2003 American Conference On Information Systems, Tampa, FL, August 4-6. 2003.

[4] Bagchi, K. and Udo, G., "An analysis of the growth of computer and Internet security breaches", Communications of AIS 12, 2003, 684–700.

[5] Bailey, J. E. and. Pearson, S. W., "Development of a tool for measuring and analysing computer user satisfaction", Management Science 29, 5, 1983, 530-545.

[6] Bandura, A., "Self-Efficacy: Toward a Unifying Theory of Behaviour Change", Psychological Review 84, 2, 1977, 191-215.

[7] Boudreau, M.-C., Gefen, D. and Straub, D. W., "Validation in information systems research: A state-of-the-art assessment." MIS Quarterly 25, 1, 2001, 1-16.

[8] Cameron, J. and Pierce, W. Rewards and intrinsic motivation. Westport, Conn: Bergin & Garvey, 2002.

[9] Cheung, W., Chang M. K. and Lai, W. S., "Prediction of Internet and World Wide Web usage at work: a test of an extended Triandis model." Decision Support Systems 30, 2000, 83-100.

[10] Cheung, C.M.K. and Limayem, M., "The role of habit in Information Systems continuance: examining the evolving relationship between intention and usage", Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas, 471-482, 2005.

[11] DeLone, W. and MacLean, E., "Information Systems Success: The Quest for the Dependent Variable", Information Systems Research 3, 1, 1992, 60-95.

[12] Dhillon, G. and Backhouse, J., "Current directions in IS security research: toward socio-organizational perspectives", Information Systems Journal. 11, 2, 2001.

[13] Fishbein, M. and Ajzen, I., Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. MA, Addison-Wesley. 1975.

[14] Furnell, S. M., Gennatou, M. and Dowland, P.S., "Promoting security awareness and training within small organizations", Proceedings of the First Australian Information Security Management Workshop, Geelong, Ausralia, 2000.

[15] Furnell, S. M., Gennatou, M. and Dowland P. S., "A prototype tool for IS security awareness and training", International Journal of Logistics Information Management, 15, 5, 2002, 352-357.

[16] Furnell, S. M., "Why users cannot use security", Computers & Security 24, 4, 2005, 274-279.

[17] Furnell, S., Sanders, P. W. and Warren, M. J., "Addressing IS security training and awareness within the European healthcare community", in Proceedings of Medical Informatics Europe '97. 1997.

[18] Gaunt, N., "Installing an appropriate IS security policy in hospitals", International Journal of Medical Informatics, 49, 1, 1998, 131-134.

[19] Hair, J.F.J., Anderson, R.E., Tatham, R.L., and Black, W. C., Multivariate data analysis. 5 ed: Upper Saddle River, New Jersey, Prentice Hall Inc. 1998.

[20] Higgins, G.E., Wilson, A.L. and Fell, B.D., "An Application of Deterrence Theory to Software Piracy", Journal of Criminal Justice and Popular Culture, 12, 3, 2005, 166-184.

[21] Hinde, S., "Security surveys spring crop", Computers & Security, 21, 4, 2002, 310-321.

[22] Ives, B., Olson, M. H. and Baroudi, J. J., "The measurement of user information satisfaction", Communications of ACM, 26, 10, 1983, 785-793.

[23] Kahn, B. K., Strong, D. M. and Wang, R. Y.,et al. "Information Quality Benchmarks: Product and Service Performance", Communication of ACM, 45, 4 2002, 184-192.

[24] Kajava, J. and Siponen, M. T., "Effectively Implemented IS security Awareness - An Example from University Environment", in Proceedings of IFIP-TC 11 (Sec'97/WG 11.1), 13th International Conference on IS security: IS security Management- The Future. 1997.

[25] Karahanna, E., Straub, D. W. and Chervany, N. L, "Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs", MIS Quarterly, 23, 2, 1999, 183-213.

[26] Katsikas, S. K., "Health care management and information system security: awareness, training or education", International Journal of Medical Informatics, 60, 2, 2000, 129-135.

[27] Larcker, D. F. and Lessig, V. P., "Perceived usefulness of information: a psychometric examination", Decision Sciences, 11, 1, 1980, 121-134.

[28] Lee, J. and Lee, Y., "A holistic model of computer abuse within organizations", Information management & computer security, 10, 2, 2002, 57-63.

[29] Lee, Y. W., Strong, D. M., Kahn, B. K. and Wang, B.Y., "AIMQ: a methodology for information quality assessment", Information & Management, 40, 2002, 133-146.

[30] Limayem, M., and Hirt, S.G., "Force of Habit and Information Systems Usage: Theory and Initial Validation", Journal of Association for Information Systems, 4, 2003, 65-97.

[31] McCoy, C. and Fowler, R.T., "You are the key to security": establishing a successful security awareness program. In the proceedings of the SIGUCCS'04, Baltimore, Maryland, October 10-13, 2004, 346-349.

[32] McLean, K., "IS security awareness - selling the cause", in Proceedings of the IFIP TC11, Eighth International Conference on IS security, IFIP/Sec '92. 1992.

[33] Parker, D. B., Fighting Computer Crime: A new Framework for Protecting Information, John Wiley & Sons, USA. 1998.

[34] Perry, W. E., Management Strategies for Computer Security, Butterworth Publishers, USA. 1985.

[35] Rippetoe, S. and Rogers, R. W., "Effects of Components of Protection - Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat", Journal of Personality and Social Psychology, 52, 3, 1987, 596-604.

[36] Rogers, R. W., "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation Theory", in Social Psychophysiology, J. Cacioppo and R. Petty (Eds.), Guilford, New York, 1983.

[37] Rogers, R. W. and Prentice-Dunn, S., "Protection motivation theory", In D. S. Gochman (Ed.), Handbook of Health Behavior Research I: Personal and Social Determinants, New York, NY: Plenum Press, 1997, 113-132.

[38] Siponen, M., "A Conceptual Foundation for Organizational Information Security Awareness", Information Management & Computer Security, 8, 1, 2000, 31-41.

[39] Siponen, M.T., "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods", Information and organization, 15, 4, 2005, 339-375.

[40] Sommers, K. and Robinson, B., "Security awareness training for students at Virginia Commonwealth University", In the proceedings of the SIGUCCS'04, Baltimore, Maryland, October 10-13, 2004, 379-380.

[41] Spurling, P., "Promoting security awareness and commitment", Information Management & Computer Security, 3, 2, 1995, 20-26.

[42] Stanton, J. M., Stam, K. R., Mastrangelo, P. and Jolton, J., "An analysis of end user security behaviors", Computers & Security, 24, 2005, 124-133

[43] Straub, D. W., "Validating Instruments in MIS Research", MIS Quarterly, 13, 2, 1989, 147-169.

[44] Straub, D.W., "Effective IS Security: An Empirical Study", Information Systems Research, 1, 3, 1990, 255-276.

[45] Straub, DW. and Welke, RJ., "Coping with Systems Risk: Security Planning Models for. Management Decision-Making", MIS Quarterly, 22, 4, 1998, 441-469.

[46] Thompson, D., "1997 Computer crime and security survey", Information Management & Computer Security, 6, 2, 1998, 78–101.

[47] Thomson, M.E. and von Solms, R., "An effective IS security awareness program for industry", in proceedings of the WG 11.2 and WG 11.1 of the TC-11 IFIP, 1997.

[48] Thomson, M. E. and von Solms, R., "IS security Awareness: educating your users effectively", Information Management & Computer Security, 6, 4, 1998, 167-173.

[49] Triandis, H. C., "Values, Attitudes, and Interpersonal Behavior", Nebraska Symposium on Motivation 1979, University of Nebraska Press, Lincoln, 1980, 195-259.

[50] Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D., "User Acceptance of Information Technology: Toward a Unified View", MIS Quarterly, 27, 3, 2003, 425-478

[51] Villarroel, R, Fernández-Medina, E. and Piattini, M., "Secure information systems development – a survey and comparison", Computers & Security, 24, 4, 2005, 308-321.

[52] Wang, R. Y. and Strong, D. M., "Beyond Accuracy: What data quality means to data consumers", Journal of Management Information Systems, 12, 4, 1996, 5-34.

[53] Wood, C. C., "Information Security Awareness Raising Methods", Computer Fraud & Security Bulletin, Elsevier Science Publishers, Oxford, England, June 1995, pp 13-15.

[54] Woon, I. M. Y., Tan, G. W. and Low, R. T., "A Protection Motivation Theory Approach to Home Wireless Security", Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas, 2005, 367-380.