2006

A New Model for Understanding Users' IS Security Compliance

Mikko Siponen
University of Oulu, mikko.t.siponen@jyu.fi

Seppo Pahnila
University of Oulu, seppo.pahnila@oulu.fi

Adam M. Mahmood
University of Texas - El Paso, mmahmood@utep.edu

A New Model for Understanding Users' IS Security Compliance

Mikko Siponen
Department of Information Processing Science, University of Oulu, 90014, Oulu, Finland
mikko.siponen@oulu.fi

Seppo Pahnila
Department of Information Processing Science, University of Oulu, 90014, Oulu, Finland
seppo.pahnila@oulu.fi

Adam M. Mahmood
Department of Information and Decision Sciences
University of Texas at El Paso
mmahmood@utep.edu

Abstract

The literature agrees that the major threat to IS security is constituted by careless employees. Therefore, effective IS security requires that users are not only aware of, but also comply with organizations' IS security policies and procedures. To address this important concern, different IS security awareness, education and enforcement approaches 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. This research-in-progress study proposes a new model that contains the factors that explain employees' IS security compliance.

Keywords: IS security compliance, IS security, IS security management.

1. Introduction

The importance of information systems (IS) security has increased as witnessed by the increasing number of IS security incidents that organizations are confronted within the last few years. While in 1997-1999 surveys, 37-50% of the organizations were victims of IS security breaches (Thompson, 1998; Hancock, 1999 p. 188-189), the respective numbers in the years 2001-2003 ranged from 75% to 91% (Bagchi & Udo, 2003, p. 684; Gordon & Loeb, 2002 p. 438-439; Hinde 2002 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 policies (Dhillon & Backhouse, 2001; Siponen, 2005; Villarroel *et al*. 2005). Employees, however, seldom comply with these IS security procedures and techniques, placing the organizations' assets and business in danger (Stanton *et al*. 2005 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, several different information security awareness, education and enforcement approaches have been proposed. Aytes and Connolly (2003) and Siponen (2000) 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 building a theoretical model explaining how employees' compliance with IS security policies and guidelines can be improved. While the present research-in-progress papers do not contain any empirical data at the moment, the testable model we advance can be validated later through an empirical research.

The rest of the paper is organized as follows: the second section reviews previous works regarding IS security awareness, education, and enforcement. The third proposes the research model, fourth discuss the research methodology, while the results of the study are presented in the fifth section.

2. Previous work on IS security behavior

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

Conceptual principles

Kajava and Siponen (1997) stress the role of user training and education in improving the IS security behavior of university students. Furthermore, Sommers and Robinson (2004 p. 379) used humorous videos of their own making to present IS security policy and procedures to university students. While empirical findings on the impact of this strategy are not presented, Sommers and Robinson (2004 p. 380) mention that the students enjoyed the videos. McCoy and Fowler (2004 p. 347) educated university students on IS security principles through mass emailing, newsletter articles and ads, web-based training and posters. For faculty and staff, McCoy and Fowler (2004 p. 347-348) used online training, posters, and articles in newsletters.

Thomson and von Solms (1997) suggest an IS security awareness program for organizations, and target groups for this program. McLean (1992) stresses that employees do not only have to be aware of IS security principles, but need also to learn the IS security procedures. To this end, McLean (1992 p. 180) proposes the use of campaigns and marketing principles to improve IS security behavior. Moorwood (1998) suggests a practical program for training employees in business continuity plans.

Perry (1985, pp. 94-95) offers practical principles for the improvement of IS security behavior: highlighting IS security violations, developing an IS security policy, sending managers to IS security seminars, and getting consultants to evaluate the IS security state of the organization.

Spurling (1998 p. 20) suggests building a company-specific process that fits the culture of the organization in question. He also advocates the use of presentations and training sessions, booklets, newsletters, email, and screen savers in promoting IS security awareness in organizations (Spurling, 1998, p. 25-26). Like Spurling (1998), Parker suggests spreading IS security messages through newsletters, brochures, posters, mugs and screensavers in organizations (Parker, 1998 p. 466). Additionally, sanctions and rewards in annual work

performance reviews are "the mother of all security controls" (Parker, 1998 p. 462). Parker (1998 p. 463) further suggests that employees should pay an IS security deposit as a guarantee against the potential security losses they may inflict. Parker (1998 p. 464) also notes the importance of activating managers in organizations, as they act as role models for their subordinates.

Gaunt (1998), Furnell, Sanders and Warren (1997) and Katsikas (2000) propose information security awareness programs for improving IS security behavior in healthcare contexts.

Furnell (2005 p. 274-275) sees unusable IS security features as an explanation as to why computer users fail to use security features. He illustrates how users can protect themselves by enabling these security features. Furnell *et al*. (2000, 2002) propose the use of IS security training software that helps users to become aware of potential risks and corresponding IS security countermeasures.

Wood (1995) suggests 53 means for ensuring that employees comply with IS security procedures, such as IS security advertisement on coffee mugs and writing IS security articles in the organization's newsletter.

While these approaches by Furnell, Sanders and Warren (1997), Furnell *et al*. (2000, 2002), Furnell (2005), Gaunt (1998), Kajava and Siponen (1997), Katsikas (2000), McLean (1992), McCoy and Fowler (2004), Moorwood (1998), Parker (1998), Perry (1985), Sommers and Robinson (2004), Spurling (1998), Thomson and von Solms (1997), and Wood (1995) propose interesting principles for increasing IS security awareness, none of these are theoretically grounded or offer empirical evidence on the effects of this principles in practice.

Theoretical models without empirical support

Aytes and Connolly (2003) present a testable model aimed at explaining why users engage in behavior that violates IS security policies. They assume that such behavior is related to the perceived probability and desirability of the outcomes of the individuals' choices.

Lee and Lee (2002) propose a model of computer abuse, incorporating the social bonds theory, the theory of planned behavior, the social learning theory and the general deterrence theory. Social bond factors affect the attitude of computer abusers as follows: (1) employees attached to their peers do not want to hurt their peers; (2) highly committed employees do not want to negate their previous efforts; (3) persons viewing computer abuse as illegal are likely to avoid computer crimes (Lee & Lee, 2002 p. 60). Moreover, social learning theory is assumed to have positive effects on the subjective norm, to use the terms of the Theory of Planned Behavior, in the sense that close association with a peer performing computer abuse exposes an employee to computer abuse (Lee & Lee, 2002 p. 60). Their model has not been tested empirically.

Siponen (2000) suggests the use of the theory of planned behavior, the theory of intrinsic motivation, and need-based theories to ensure that employees follow IS security policies and guidelines. Following Siponen, Layton (2005) stresses the need to focus on employees' internalization of the IS security policies. Like Siponen (2000), Layton (2005) also proposes that the reason for employees to follow IS security policies needs to be justified to users. Layton also discusses need-based theories, theories of intrinsic motivation (by Deci) and the Expectancy

theory (by Vroom), as well as theories of ethics. These frameworks by Siponen (2000) and Layton (2005) have not been tested empirically.

Thomson and von Solms (1998) suggest the use of social psychology to improve employees' IS security behavior, without referring to any particular theory. They do not offer testable hypotheses or empirical findings.

To summarize, while the works by Aytes and Connolly (2003), Siponen (2000), Layton (2005), Lee and Lee (2002), and Thomson and von Solms (1997) contribute to the creation of theoretical insights on how employees' IS security compliance can be increased; they do not offer empirical evidence to support these suggestions.

Empirical works grounded upon theories

Stanton *et al*. (2004) created categories of security behavior by interviewing 110 people, and tested the categories through a survey (n=1167). Their categories include malicious users and those employees causing IS security problems due to unintentional lapses on the one hand, or using their knowledge intentionally to protect the organization's assets, on the other hand.

Straub (1990) and Straub and Welke (1998) 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 (Straub 1990 p. 272-273).

Woon *et al*. (2005) 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.

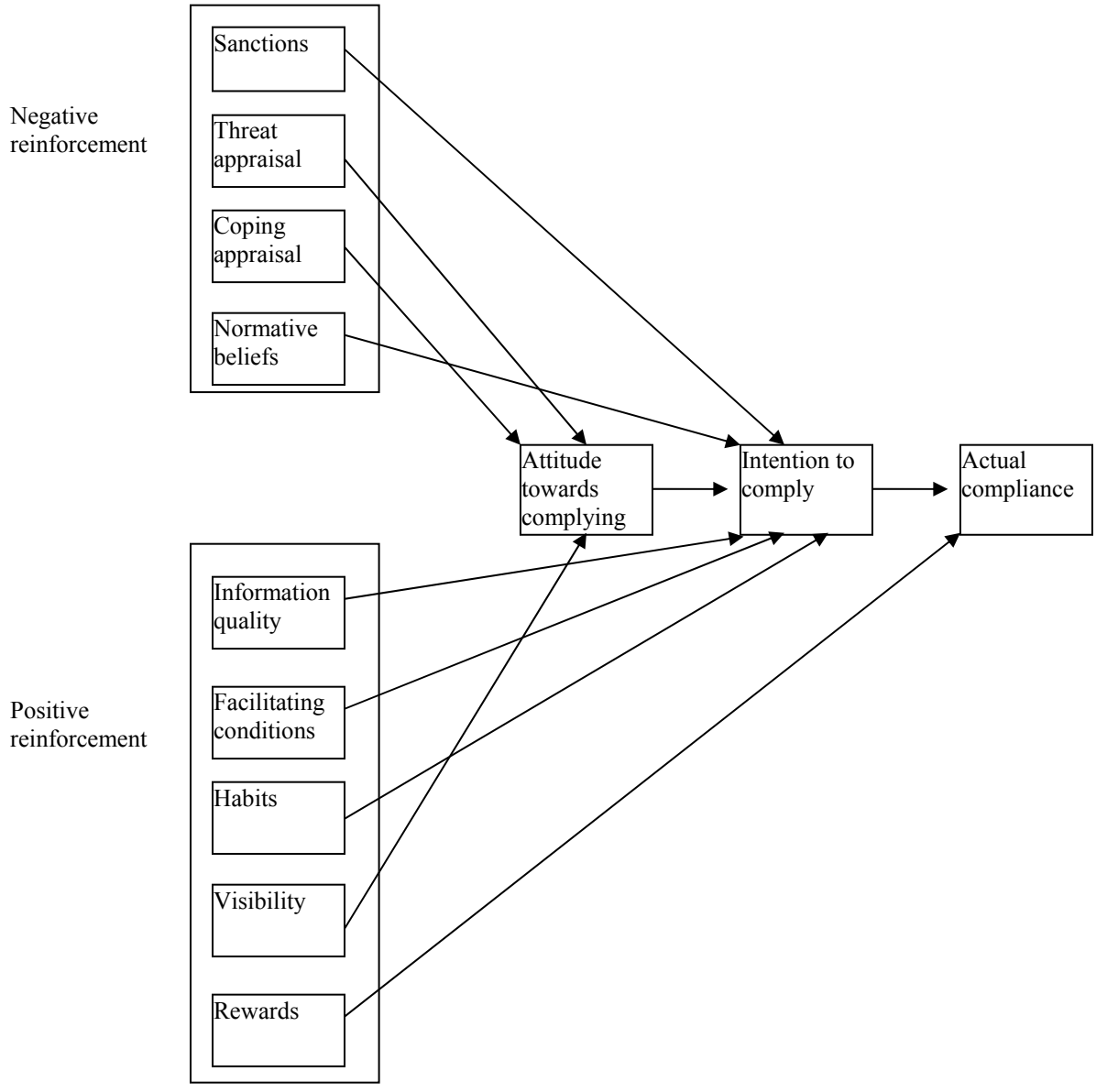
To summarize the findings of the literature review, while 30 IS security awareness, education and enforcement approaches exist, only three approaches incorporate a theoretically and empirically grounded model. Of these three, Woon *et al*. (2005) study wireless network users, while Straub (1990) focuses on deterrence theory, and Stanton *et al*. (2004) have created categories of security behavior. Excluding Straub (1990), these IS security awareness, education and enforcement approaches 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 2) for the study combines General Deterrence Theory, Protection Motivation Theory, the Theory of Reasoned Action, Information Systems Success, and Triandis' behavioral framework 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 the Theory of Reasoned Action (TRA) (Fishbein and Ajzen 1975). Attitude indicates a person's positive or negative feelings toward some stimulus object (Ajzen 1991). According to Ajzen (1991), intentions captured the motivational factors that have 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 entail in a behavior, the more likely the behavior is 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 2. Theoretical model for IS security policy compliance.



Sanctions

Sanctions come from the General Deterrence theory. The General Deterrence Theory suggests that certainty, severity, and celerity of punishment affect people's decision on whether they commit a crime or not (Straub & Welke, 1998). Straub found out that stating penalties for IS security policy non-compliance increases security behavior (Straub, 1990). However, studies by Straub (1990) and Straub and Welke (1998) employ what Higgins et al (2005) call as classical deterrence theory. Hence, these seminal studies (Straub, 1990; Straub & Welke, 1998) do not address other important components of contemporary General Deterrence Theory, namely social disapproval, self-disapproval and Impulsivity (Higgins et al., 2005). This leads to the following hypothesis:

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

Threat appraisal and coping appraisal

According to Woon *et al.* (2005), threat appraisal consists of two dimensions; perceived vulnerability and perceives severity. Woon *et al* (2005 p. 369) utilize the concept of perceived vulnerability in the context of home users, from Rogers (1983), 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 (Woon et al., 2005 p. 369). Like perceived vulnerability, Woon et al (2005) derive this concept from the protection motivation theory by Rippetoe and Rogers (1987). In developing this concept, as an example, they used identity stealing and email eavesdropping through hacking among home wireless users (e.g., having my online identity stolen as a result of wireless hacking is a serious problem for me).

Coping appraisal is a measure consisting of three dimensions: response efficacy, self efficacy, and response cost (Rogers 1983; Woon et al. 2005). Response efficacy relates to the belief in the perceived benefits of the action (Rogers, 1983). 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 (Bandura 1977). 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 (Bandura 1977). 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 (Woon et al. 2005).

We postulate that threat appraisal and copying appraisal are an important factors in explaining employees' attitude towards 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 in this respect. Therefore, we hypothesize:

H2: Threat appraisal affects employees' attitude to comply with IS security policies.

H3: Coping appraisal affects employees' attitude to comply with IS security policies.

Normative beliefs

Normative beliefs reflect normative expectations of peers or colleagues (Fishbein and Ajzen 1975). Aydin (1991) 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 (1992) 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 varying constructs. Larcker and Lessig (1980) 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*. (1983) developed a standard instrument to measure user information satisfaction, based on 39 computer user satisfaction factors suggested by Bailey and Pearson (1983). Wang and Strong (1996) 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*. (2002) 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 (2002) mapped sixteen different dimensions of information quality, based on the study by , e.g., accessibility, completeness, relevancy and timeliness, to four quadrants: sound, dependable, useful and usable, aiming to develop a generalized measure for improving information quality. Lee *et al*. (2002) developed a methodology for assessment and improvement of information quality (AIMQ) in organizations. The AIMQ methodology mapped fifteen different dimensions of information quality. Lee *et al.* (19XX) concluded that AIMQ is useful when identifying IQ problems, prioritizing IQ improvement areas, and monitoring IQ improvements.

Given that information quality relates to user satisfaction with the usefulness of the information (Ives, Olson *et al*. 1983), 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., IS security policy and related activities may be distributed through 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 intention to comply with IS security policies.

Facilitating conditions

According to Triandis (1980), facilitating conditions are objective factors that observers agree 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 (Venkatesh, Morris et al. 2003). 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 have not 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' intention to comply with IS security policies.

Habits

A habit is unconscious or automatic behavior, as opposed to intentions or conscious behavior (Limayem & Hirt, 2003 p. 71; Triandis, 1980). Based on the model by Triandis (1980), habits are found to explain IS usage (Limayem & Hirt, 2003; Cheung & Limayem, 2005). It is argued that the influence of habits on actual behavior increases in the long run, while the influence of behavioral intentions decreases (Limayem & Hirt, 2003 p. 84) in the long run. Hence, Limayem and Hirt (2003 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.

Visibility

In technology acceptance literature, visibility refers to the degree to which one can see others using the system in the organization (Moore & Benbasat 1991). In that sense, visibility is found to explain technology usage. In computer abuse content, Straub (1990) found that the overall visibility of IS security in an organization, with reference to different IS security actions such as monitoring, introducing IS security policies and respective enforcement activities, reduces computer abuse in organizations.

Based on a literature review, we decided to include in our instrument external and internal IS security visibility. Internal IS security visibility refers to the degree to which one can see not only IS security actions, campaigns or advertisements, but also formal or information communications in the organization. External IS security visibility refers to the degree to which one can see IS security measures outside of the organization. Potential sources of external

visibility include news or commercials in media such as newspapers, radio, the Internet or TV. Societal reactions (Finney & Lesieur, 1992) can be seen as one dimension of visibility. According to Finney and Lesieur (1992), such reactions manifest themselves through public outrage through different media, such as TV and newspapers. They are found to be a major factor regarding illegal activities: in general, the weaker the social reactions to a crime, the easier it is to commit.(Finney & Lesieur, 1992 p. 285). A similar relationship is assumed to exist regarding IS security policy non-compliance. For example, negative social reactions towards certain IS security policy violations create IS security visibility, by not only increasing the interest of users, but also increasing the importance placed on IS security at the management level. Such incidents make employees and top managers realize that IS security policy violations by employees may result in serious problems, including negative public image. This, in turn, is assumed to increase employees' and managers' interest in IS security. This leads to the following hypothesis:

H8. Visibility affect employees' attitude toward complying with IS security policies.

Rewards

Rewards can be used as effective means for cultivating interest and increasing motivation and performance (Cameron & Pierce, 2002 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 (p. 24). Considering employees' attitude and intention to actual compliance, we can hypothesize:

H9. Rewards affect employees' actual compliance of the security policies

H11. Employees' attitude towards complying with IS security policies have a significant impact on intention to comply with IS security policies.

H12. Employees' intention to comply with IS security policies have a significant impact actual compliance with IS security policies.

4. Research methodology

The data of the field study will be collected based on the Web questionnaire. To maximize the reliability of the measurements with respect to the constructs of our research, we selected items that have been used in prior research which are modified to suit research context. By using previously validated questions, we have tried to ensure the reliability of the study. According to Straub (1989) and Boudreau et al. (2001), using validated and tested questions will improve the reliability of results. These questions are evaluated by the IT users, security managers, and IT experts aiming to increase content validity (Straub 1989). Considering the feedback, we did some necessary modifications to the questionnaire in order to execute a pilot test. Data collected via responses to the questionnaires designed for the study will be stored in a database for statistical analysis.

The questionnaire for the present research includes items taken from different sources. Habits, for example, are generated from the studies by Triandis (1980) and Limayem and Hirt (2003).

Facilitating conditions are based on the questionnaire items developed by Limayem and Hirt (2003) and Cheung et al. (2000). Normative beliefs are taken from the study by Karahanna and Straub (1999). Visibility are based on the study by Moore and Benbasat (1991). Information quality is measured by using the item scale proposed by Lee et al. (2002). Scale items Sanctions, Rewards, Threat appraisal and Copying appraisal are generated from the literature by Roger and Prentice-Dunn (1997). All the items are measured using seven-point Likert scale (strongly disagree – strongly agree).

5. 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 IS security awareness, education and enforcement approaches 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. This study put forward a new model in order to explain employees' IS security compliance. While empirical research is needed to test the model further, understanding users' psychological and behavioral incentives, their attitude and intention toward complying security policies through the model will increase our understanding about the issue which may have practical value for IS managers, practitioners and researchers.

References

Ajzen, I. (1991). "The Theory of Planned Behavior." *Organizational Behavior and Human Decision Processes* **50**(2): 179-211.

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

Aytes, K. & Connolly, T. (2003), 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.

Bagchi K and Udo G (2003) An analysis of the growth of computer and Internet security breaches. *Communications of AIS* 12, 684–700.

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

Bandura, A. (1977). "Self-Efficacy: Toward a Unifying Theory of Behaviour Change." *Psychological Review* **84**(2): 191-215.

Boudreau, M.-C., D. Gefen, et al. (2001). "Validation in information systems research: A state-of-the-art assessment." *MIS Quarterly* **25**(1): 1-16.

Cameron, J. & Pierce, W., (2002), *Rewards and intrinsic motivation*. Westport, Conn: Bergin & Garvey

Cheung, W., M. K. Chang, et al. (2000). "Prediction of Internet and World Wide Web usage at work: a test of an extended Triandis model." *Decision Support Systems* **30**: 83-100.

Cheung, C.M.K & Limayem, M. (2005), 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, pp. 471-482.

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

Dhillon, G. & Backhouse, J., (2001), Current directions in IS security research: toward socio-organizational perspectives. *Information Systems Journal.* Vol 11, No 2.

Finney, H.C. & Lesieur, H.R., (1992), A Contingency theory of organizational crime. *Research in the Sociology of Organizations,* vol. 1, pp. 255-299.

Fishbein, M. and I. Ajzen (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research.* MA, Addison-Wesley.

Furnell, S. M., Gennatou, M., Dowland, P.S., (2000), Promoting security awareness and training within small organisations. *1st Australian Information Security Management Workshop,* Deakin University, Geelong.

Gaunt, N., (1998), Installing an appropriate IS security policy [in hospitals], *International Journal of Medical Informatics,* Vol. 49, No. 1, pp. 131-134.

Gordon, L.A & Loeb, M.P., (2002), The Economics of Information Security Investment. *ACM Transactions on Information and System Security,* Vol. 5, No. 4, November 2002, Pages 438–457.

Hancock, B., (1999), 1999 CSI/FBI survey: Cyberattacks on the rise. *Computers & Security,* Volume 18, Issue 3, Pages 188-189.

Higgins, G.E., Wilson, A.L., & Fell, B.D. (2005), An Application of Deterrence Theory to Software Piracy. *Journal of Criminal Justice and Popular Culture,* 12 (3), 166-184.

Hinde, S., (2002), Security surveys spring crop. *Computers & Security,* Volume 21, Issue 4, 1 August 2002, Pages 310-321.

Ives, B., M. H. Olson, et al. (1983). "The measurement of user information satisfaction." *Communications of ACM* **26**(10): 785-793.

Kahn, B. K., D. M. Strong, et al. (2002). "Information Quality Benchmarks: Product and Service Performance." *Communication of ACM* **45**(4): 184-192.

Kajava, J. and Siponen, M. T., (1997), 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.

Karahanna, E., D. W. Straub, et al. (1999). "Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs." *MIS Quarterly* **23**(2): 183-213.

Katsikas, S. K., (2000), Health care management and information system security: awareness, training or education, *International Journal of Medical Informatics*, Vol. 60, No. 2, pp. 129-135.

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

Lee, J. & Lee, Y., (2002), A holistic model of computer abuse within organizations. *Information management & computer security,* vol. 10, no. 2, pp. 57-63.

Lee, Y. W., D. M. Strong, et al. (2002). "AIMQ: a methodology for information quality assessment." *Information & Management* **40**: 133-146.

Limayem, M. & Hirt, S.G., (2003), Force of Habit and Information Systems Usage: Theory and Initial Validation. *Journal of Association for Information Systems,* vol. 4, pp. 65-97.

McCoy, C., & Fowler, R.T., (2004), "You are the key to security": establishing a successful security awareness program. In the *proceedings of the SIGUCCS'04*, October 10-13, Baltimore, Maryland, pp. 346-349.

McLean, K., (1992), IS security awareness - selling the cause, in *Proceedings of the IFIP TC11,* Eighth International Conference on IS security, IFIP/Sec '92.

Moore, G.C. and Benbasat, I. (1991), Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. *Information Systems Research,* vol. 2, no. 3, pp. 192-222.

Morwood, G., (1998), Business continuity: awareness and training programmers. *Information Management & Computer Security*, Volume 6 Number 1, pp. 28-32.

Rogers, E. M. (1995). *Diffusion of Innovations.* New York, The Free Press.

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

Siponen, M.T. (2005): Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and organization,* Volume 15, Issue 4, pp. 339-375.

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

Spurling, P. (1995), Promoting security awareness and commitment. *Information Management & Computer Security,* vol. 3, no. 2, pp. 20-26.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). An analysis of end user security behaviors. *Computers & Security,* 24, 124-133

Straub, D. W., (1989), Validating Instruments in MIS Research ", *MIS Quarterly*, June, Vol 13, No 2, pp 147-169.

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

Straub, DW and Welke, RJ "Coping with Systems Risk: Security Planning Models for. Management Decision-Making," *MIS Quarterly* (22:4), 1988, pp. 441-469.

Thompson, D., (1998), 1997 Computer crime and security survey. *Information Management & Computer Security,* vol. 6, no. 2, pp. 78–101.

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

Thomson, M. E. and von Solms, R., (1998), IS security Awareness: educating your users effectively, *Information Management & Computer Security,* Vol. 6, No 4, pp. 167-173.

Triandis, H. C. (1980). Values, Attitudes, and Interpersonal Behavior. *Nebraska Symposium on Motivation 1979,* University of Nebraska Press, Lincoln**:** 195-259.

Venkatesh, V., M. G. Morris, et al. (2003). "User Acceptance of Information Technology: Toward a Unified View." *MIS Quarterly* **27**(3): 425-478

Villarroel, R, Fernández-Medina, E and Piattini, M., (2005), Secure information systems development – a survey and comparison. *Computers & Security* 24(4): 308-321.

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

Woon, I. M. Y., Tan, G.W. & Low, R.T. (2005) A Protection Motivation Theory Approach to Home Wireless Security. Proceedings of the *Twenty-Sixth International Conference on Information Systems*, Las Vegas, pp. 367-380.