PACIS 2007 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2007

Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study

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

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

Adam Mahmood
University of Texas,USA, mmahmood@utep.edu

87. Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study

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

Mikko Siponen
University of Oulu, Finland
mikko.siponen@oulu.fi

Adam Mahmood
University of Texas,USA
mmahmood@utep.edu

Abstract

It is widely agreed that a key threat to information security is caused by careless employees who do not adhere to the information security policies of their organizations. In order to ensure that employees comply with the organization's information security procedures, a number of information security policy compliance measures have been proposed in the past. Prior research has, however, criticized these measures as lacking theoretically and empirically grounded principles. To fill this gap in research, the present study advances a novel model that explains employees' adherence to information security policies. This model modifies and combines the Protection Motivation Theory, the General Deterrence Theory, the Theory of Reasoned Action, the Innovation Diffusion Theory and Rewards. In order to empirically validate this model, we collected data (N=917) from four different companies. The findings show that direct paths from threat appraisal, self-efficacy, normative beliefs, and visibility to the intention to comply with IS security policies were significant. Response efficacy, on the other hand, did not have a significant effect on the intention to comply with IS security policies. Sanctions have a significant effect on actual compliance with IS security policies, whereas rewards did not have a significant effect on actual compliance with the IS security policies. Finally, the intention to comply with IS security policies has a significant effect on actual compliance with the IS security policies.

Keywords: information security compliance, protection motivation theory, general deterrence theory.

Introduction

Information security incidents that organizations have confronted within the last few years have increased. While in 1997-1999 surveys, 37-50% of the organizations were victims of information security breaches (Thompson, 1997), the same 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).

In order to cope with increased information security threats, not only different technical protection means (e.g., anti-virus software tools) but also information security policies (Dhillon & Backhouse, 2001; Siponen, 2005; Villarroel *et al*. 2005) have been suggested in the literature. Employees in organizations, unfortunately, seldom comply with these information security techniques and policies, placing their organization's assets and interests in serious jeopardy (Stanton *et al*. 2005 p. 125). Effective information security, therefore, requires that employees comply with information security (IS) policies and guidelines. In order to address this crucial information security concern, several IS security policy compliance measures, often referred to as information security awareness, education, and enforcement approaches, have been proposed in the information security literature. Aytes and

Connolly (2003), Pahnila et al. (2007), Puhakainen (2006), Siponen (2000) and Siponen et al. (2007) have criticized existing information security awareness approaches as lacking not only theoretically grounded methods, but also there is no empirical evidence on their effectiveness. These studies show that while 30 information security awareness, education and enforcement approaches exist, only four approaches incorporate a theoretically and empirically grounded model. Of these four, Woon *et al*. (2005) studied wireless network users, while Straub (1990) and Straub and Welke (1998) focused on classical deterrence theory, and Aytes and Connolly (2004) apply the Rational Choice Model. Thus, with the exception of the studies by Straub (1990), Straub and Welke (1998), and Aytes and Connolly (2004), the existing information security awareness, education and enforcement approaches do not offer a theoretical model combined with evidence that explains why employees in organizations do not comply with information security guidelines, nor do they consider what factors affect employees' information security policy compliance. This paper fills this gap in research by first building a new theoretical model, derived from the Protection Motivation Theory, the General Deterrence Theory, the Theory of Reasoned Action, The Innovation Diffusion Theory and Rewards, aimed at explaining how employees' compliance with information security policies and guidelines can be improved. The model is then empirically validated using a quantitative survey.

The results of this study are of relevance to researchers and practitioners. Since the existing studies on information security policy compliance present only anecdotal information as to which factors explain employees' adherence to information security policies (with the three exceptions; see Aytes & Connolly, 2004; Straub, 1990; Straub & Welke, 1998; Woon *et al*. (2005), is it of the utmost importance to study this matter. This information is also useful for practitioners who want to obtain empirically validated information as to how they can improve their employees' adherence to information security policies, and in the process, enhance the security of their organization's information.

The second section of the paper proposes the research model and third part discusses the research methodology. The empirical findings are presented in the fourth section. The fifth section discusses the implications of the study for practice.

The Research Model to Explain Employees' Adherence to IS security policies

In this section, we present the theoretical model (Fig 1) which is derived from the Protection Motivation Theory, the Theory of Reasoned Action, the Innovation Diffusion Theory, the General Deterrence Theory and Rewards. We next we discuss each element of the theoretical model in detail.

Normative beliefs means expectations of colleagues, peers and superiors, which may have a persuasive influence on whether or not an employee will adhere to a specific behavior norm (Ajzen, 1991). In the context of IS security policy compliance, we suggest, based on the idea of normative beliefs, that the behavior of managers, IS security staff and peers will have a persuasive effect on employees' IS security policy compliance. Hence, we hypothesize:
H1: Normative beliefs affect employees' intention to comply with information security policies.

Threat appraisal

Threat appraisal consists of two dimensions: perceived vulnerability and perceived severity. Perceived vulnerability means conditional probability that a negative event will take place if no measures are taken to counter it (Rippetoe and Rogers, 1987). In the context of our study, the negative event is any information security threat. Therefore also in the context of our study, perceived vulnerability refers to employees' perceived assessment of whether their organization is vulnerable to information security threats, and the immediacy of such threats if no measures are undertaken to counter them.

In turn, perceived severity encompasses both psychological and physical harm the threat can cause (Rippetoe and Rogers, 1987). In the context of our study, it means potential negative consequences caused by information security breaches for the organization.

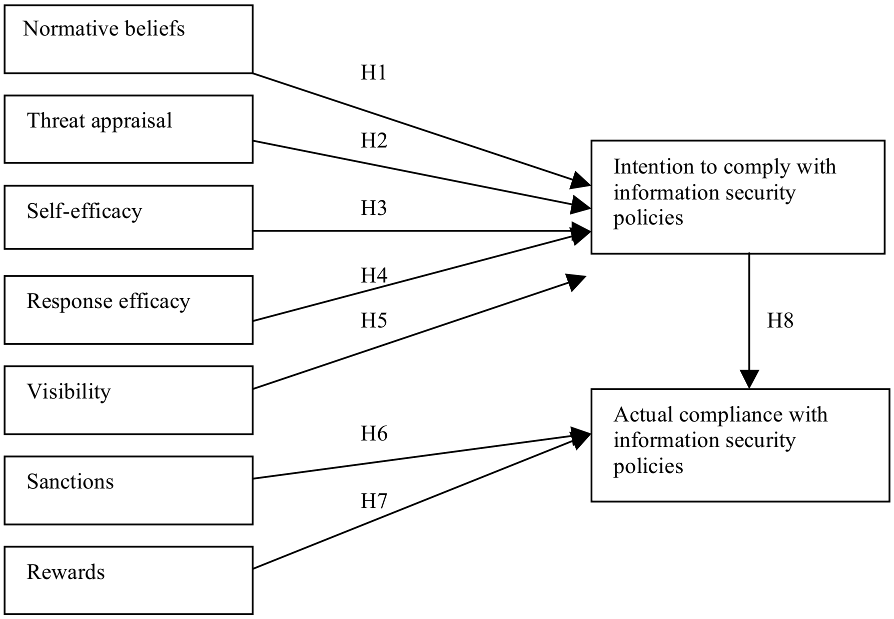
Normative beliefs
Threat appraisal
Self-efficacy
Response efficacy
Visibility
Sanctions
Rewards
H1
H2
H3
H4
H5
H6
H7
H8
Intention to comply with information security policies
Actual compliance with information security policies

Figure 2. The research model explaining compliance with information security policies.

Here our assumption is that if an organization's employees do not realize that they are really confronted by information security threats (threat appraisal) and if they do not feel that these threats can cause consequences with a destructive impact for the organization (perceived severity), they will not comply with information security policies. Therefore, we hypothesize:

H2: Threat appraisal affects employees' intention to comply with information security policies.

Self-efficacy and response efficacy

Response efficacy and self-efficacy come from a coping appraisal, which is a component of the Protection Motivation Theory (Rogers 1983; Rogers and Prentice-Dunn, 1997). Response efficacy relates to the belief in the perceived benefits of coping action (Rogers, 1983). That is, carrying out the coping action removes the threat. In our study, it means that adherence to information security policies is an effective mechanism for detecting an information security threat. Self-efficacy emphasizes the individual's ability or judgment of their capabilities to perform the coping response actions (Bandura 1977). To place self-efficacy theory in the context of our study, it refers to the situation whereby workers' beliefs on whether they can apply and adhere to IS security policies will lead to compliance with these policies. Maddux and Rogers (1982) found in their study that self-efficacy was the most powerful predictor of intention. Therefore, we hypothesize:

H3: Self-efficacy affects employees' intention to comply with information security

policies.

H4: Response efficacy affects employees' intention to comply with information security policies.

Visibility. In technology acceptance literature, visibility refers to the degree to which one can see others using the system (Moore and Benbasat, 1991). In the computer abuse context, it refers to the overall visibility of IS security in an organization which, through different IS security actions (enforcement of IS security policies), reduces computer abuse within the organization (Straub, 1990). In our study, visibility represents environmental information which has persuasive effect on the cognitive process. Accordingly, IS security visibility refers to the degree to which one can see not only IS security actions, campaigns, advertisements, and formal or informal information communications within the organization, but also security measures outside the organization via media. Hence, we hypothesize:

H5: Visibility affects employees' intention to comply with information security policies.

Sanctions. The concept of deterrence has been a key focus of criminological theories for more than thirty years. A leading theory in the field is the General Deterrence Theory, originally developed for controlling criminal behaviour (Higgins et al. 2005). Traditionally, the classical deterrence theory suggests that certainty, severity, and celerity of punishment, affect people's decision on whether to commit a crime or not (Higgins et al. 2005). Certainty means that an individual believes that his or her criminal behavior will be detected, while severity means that it will be harshly punished. In turn, celerity signifies that the detection will occur at once. Straub (1990) found that stating penalties for information security policy non-compliance increases proper information security behavior. However, studies by Straub (1990) and Straub and Welke (1998) employ what Higgins et al. (2005) call the classical deterrence theory. Therefore, these seminal studies by Straub (1990, Straub and Welke 1998) do not address three important components of contemporary General Deterrence Theory: social disapproval, self-disapproval and impulsivity. Social disapproval refers to the degree to which family members, friends and co-workers disapprove of an action. Self-disapproval refers to an individual's feeling of shame, guilt, and embarrassment about an action, while impulsivity means low self-control, that is, the inability of an individual to resist a temptation toward criminal behavior when an opportunity for it exists. This leads to the following hypothesis:

H6. Sanctions affect employees' actual compliance with information security policies.

Rewards. Rewards can be used as effective means for cultivating interest and increasing motivation and performance (Cameron and Pierce 2002 p. 20). Rewards can be tangible (e.g., money, gold stars, medals, and 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 (Cameron and Pierce 2002 p. 24). Considering employees' attitudes and intentions toward actual compliance, we can hypothesize:

H7. Rewards affect employees' actual compliance of the security policies

Intention

Intention to comply with information security policies and actual compliance with information security policies are based on 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 capture the motivational factors that have an influence on 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 commit oneself to a form of behavior, the more likely the behavior will be carried out. According to our model, the stronger the intention to comply with information security policies is, the more likely the individual will actually comply with the information security policies. Rogers and Prentice-Dunn (1997) suggest that the intentions are the most applicable measure of protection motivation. Previous research on technology acceptance, for instance, shows that intentions are good predictors of actual behavior (e.g., Venkatesh et al., 2003), which is adherence to information security policies in the context of our study. In our study, behavioral intention is an indicator of the effects of persuasion related to information security policies. Thus, we can hypothesize:

H8. Employees' intention to comply with information security policies has a significant impact on actual compliance with information security policies.

Research methodology

According to Straub (1989) and Boudreau et al. (2001), using validated and tested questions will improve the reliability of constructs and results. Accordingly, we used items that have been tried and tested by previous studies, when available (Table 1).

Table 1. Summary of research constructs.

Construct	Theoretical background	Measures modified from
Intention to comply	The Theory of Reasoned Action	Agarwal and Prasad (1998) Moon and Kim (2001)
Actual compliance	The Theory of Reasoned Action	Limayem and Hirt (2003), Heijden (2003)
Normative belief	The Theory of Reasoned Action	Karahanna, Straub and Chervany (1999)
Threat appraisal and copying appraisal	Protection Motivation theory	Roger and Prentice-Dunn (1997)
Visibility	Innovation Diffusion Theory	Moore and Benbasat (1991), Straub (1990)
Sanctions	The General Deterrence Theory	Higgins, Wilson and Fell (2005)
Rewards	Rewards	Cameron and Pierce (2002)

All the items are measured using a standard seven-point Likert scale (strongly disagree – strongly agree). Since the measures presented in table 2 are not previously tested in the context of information security policy compliance, the present research tests these measures in that context. Hence, the questions were pilot tested using 15 people. Based on their feedback, the readability factor of the questions was improved. The data was collected from four Finnish companies. A total 3130 respondents were asked to fill out the web-based questionnaire. Taking into consideration missing data and invalid responses, we had a total of 917 reliable responses. Thus, the response rate of the survey was 29.3 %, which can be deemed to be acceptable. One company did not include in their questionnaire the measure "years in service", as shown in Table 2.

In this study, the data analysis was conducted using SPSS 14.0 and AMOS 6.0 structural equation modeling software (SEM). The use of a SEM should be based on theory and on the researcher's clear view of the suggested model, since SEMs do not include sophisticated methods for model specification. AMOS is a tool based on covariance which can be used for confirmatory factor analysis.

As mentioned earlier, the content validity of the instrument was ensured by using experts and practitioners who assessed the used items. Convergent validity was ensured by assessing the factor loadings and by calculating variance extracted. We conducted a single confirmatory factor analysis for each of the constructs. As Table 3 shows, nearly all the model items loaded well, exceeding the 0.50 (Hair et al. 1998). There were two items which where slightly below 0.50, but they are acceptable, exceeding the threshold 0.40. Divergent validity was assessed by computing the correlations between constructs. Correlations between all pairs of constructs were below the threshold value of 0.90. Variance extracted from all the constructs exceeded 0.5 (Hair et al. 2006). Internal consistency reliability among the items was assessed by calculating Cronbach's alpha. As Table 3 shows, Cronbach's alpha exceeded the suggested value of 0.60 for all constructs. Hence, according to results it seems that the reliability and validity of the constructs in the model are acceptable.

Results

The number of males (56.1%) and females (43.9%) are fairly equally distributed. Most of the respondents are middle-aged, 31.3% representing the age group 31-40 and 30.0% representing the age group 41-50 (Table 2).

Table 2. Descriptive statistics of the respondents

	Frequency	Percent
Gender (N=917)		
Male	514	56.1
Female	403	43.9
Age (N=919)		
<30	135	14.7
31-40	288	31.4
41-50	276	30.0
>50	220	23.9
Years in service in the existing company (N=670)		
<5	202	30.1
5-10	155	23.1
>10	313	46.8

Most respondents have long working experience. Over forty six percent of the respondents (46.7 %) have served in their company for more than ten years. Quite often selection bias, which simply means that the respondents of a study are not relevant representatives of the sample, limits the generalizability of the results (Hair, 1998). In our study, gender and age groups of the respondents were fairly equally distributed, and they covered a wide geographical area. While these issues are important to minimizing bias (Hair, 1998), nevertheless the selection bias has to be mentioned as a potential limitation in generalizing the results of the present study.

Table 3. Mean and standard deviation of the constructs.

Construct	Mean	Standard deviation	Min	Max
Actual compliance	6.16	0.98	1	7
Intention to comply	6.35	0.88	1	7
Normative beliefs	6.29	0.97	1	7
Threat appraisal	5.72	0.99	1	7
Response efficacy	4.75	1.43	1	7
Self-efficacy	5.89	1.02	1	7
Visibility	4.55	0.82	1	7
Sanctions	3.80	1.58	1	7
Rewards	2.67	1.44	1	7

Table 4. Convergent validity and internal consistency and reliability

Construct	Items	Factor loading	Variance extracted	Cronbach's alpha
Actual compliance	Actcomp1	0.65	0.81	0.84
	Actcomp2	0.88		
	Actcomp3	0.89		
Intention to comply	Intcomp1	0.71	0.80	0.85
	Intcomp2	0.86		
	Intcomp3	0.84		
Normative beliefs	Normbel1	0.80	0.77	0.87
	Normbel2	0.92		
	Normbel3	0.73		
	Normbel4	0.70		
Threat appraisal	Thrappr1	0.54	0.62	0.76
	Thrappr2	0.65		
	Thrappr3	0.60		
	Thrappr4	0.61		
	Thrappr5	0.70		
	Thrappr6	Dropped		
Response efficacy	Respeffi1	0.73	0.75	0.80
	Respeffi2	0.88		
	Respeffi3	0.66		
Self-efficacy	Selfeffi1	Dropped	0.85	0.83
	Selfeffi2	0.89		
	Selfeffi3	0.80		
Visibility	Visibi1	0.54	0.54	0.61
	Visibi2	0.45		
	Visibi3	0.56		
	Visibi4	0.59		
Sanctions	Sanctio1	0.91	0.83	0.90
	Sanctio2	0.96		
	Sanctio3	0.89		
	Sanctio4	Dropped		
	Sanctio5	0.59		
	Sanctio6	Dropped		
Rewards	Reward1	0.46	0.74	0.77

Reward2	0.91
Reward3	0.84

The model was estimated using the maximum likelihood method. The fitness of the model was tested using the goodness-of-fit statistics, which indicate the degree of compatibility between the proposed model and the observed covariances and correlations. The fit indices chosen for this study are based on the literature, and represent two different fit characteristics: absolute fit and comparative fit. The chi-square test (χ^2) with degrees of freedom, p-value and sample size is commonly used as an absolute model fit criteria (Hoyle, 1995; Schumacker & Lomax, 1996). The root-mean-square residual index (RMSEA) is used to assess the error due to simplification of the hypothesized model. The Tucker-Lewis Index (TLI) and Comparative Fit Index (CFI) are recommended for comparing the hypothesized model to the independent model (Hoyle, 1995; Schumacker & Lomax, 1996). The fit indices indicate that the research model provides a good fit with the data. The recommended fit criteria and the result of our analysis are presented in Table 5.

Table 5. Fit criteria.

Model		Criteria
χ^2	12.717	
df	6	
p	0.048	
TLI	0.980	>0.9
CFI	0.997	>0.9
RMSEA	0.035	<0.05

The findings indicate that the direct paths from threat appraisal, self-efficacy, normative beliefs and visibility to the intention to comply with IS security policies were significant. Response efficacy, in turn, does not have a significant effect on intention to comply with IS security policies (see table 6). Sanctions have significant effect on actual compliance with the policies, whereas rewards did not have a significant effect on actual compliance. Intention to comply with IS security policies has a significant effect on actual compliance with IS security policies. The model accounts for 72 % ($R^2 = 0.72$) of the variance in intention to comply. Standardized beta weight (ß) from intention to comply with IS security policies to actual compliance with IS security policies was 0.40; $p \leq 0.05$.

Table 6. Summary of hypotheses

Hypothesis	Support
Intcomp → Actcomp	Supported
Thrappr → Intcomp	Supported
Respeffi → Intcomp	Not supported
Selfeffi → Intcomp	Supported
Normbel → Intcomp	Supported
Visibi → Intcomp	Supported
Sanctio → Actcomp	Supported
Reward → Actcomp	Not supported

Concluding discussion

The literature agrees that the major threat to information security is constituted by careless employees who do not comply with organizations' information security policies and procedures. Hence, employees not only have to be aware of, but will also have to comply with organizations' information security policies and procedures. To address this important concern, different information security awareness, education and enforcement approaches have been proposed. Prior research on information security policy compliance has criticized these extant information security policy compliance approaches as lacking theoretically grounded and empirically validated principles to ensure that employees comply with information security policies. In order to address these two problems in the literature, the present research put forth a novel model in order to explain employees' information security compliance. The model combined the Protection Motivation Theory, the General Deterrence Theory, the Theory of Reasoned Action, The Innovation Diffusion Theory and Rewards. The proposed model was then empirically validated using data (N=917) collected from four companies.

The findings of the present research indicated that the direct paths from threat appraisal, self-efficacy, normative beliefs and visibility to intention to comply with IS security policies were significant. Response efficacy, on the other hand, did not have a significant effect on intention to comply with IS security policies. Sanctions also had a significant effect on actual compliance with IS security policies whereas rewards did not have a significant effect on actual compliance with them. Finally, intention to comply with IS security policies had a significant effect on actual compliance.

The findings regarding threat appraisal suggest that employees should be made aware of the information security threats and their severity and celerity for the organization by information security staff. To be more precise, our findings regarding threat appraisal suggest that information security personnel of an organization should emphasize to the employees that not only are information security breaches becoming increasingly serious for the organization, but also their severity with regard to conducting the normal business of the organization is increasing.

Self-efficacy, as stated earlier, refers to the employees' beliefs about whether they can apply and adhere to information security policies. The present research empirically showed that self-efficacy had a significant impact on intention to comply with information security policies. The respondents do not see that the existence of security staff or IS security policies as such keep the IS security breaches down. Instead, what is required, according to the results of our study, is the respondents' own actions in complying with IS security policies. This finding also stresses the perceived relevance of information security policies. If information security policies are not perceived as being relevant and sufficiently up-to-date for their work by employees, they do not adhere to them. Yet, the finding also suggests that it is important to ensure that, throughinformation security education, for example, employees really can use information security measures.

Our results show that response efficacy does not have a significant effect on intention to comply with information security policies. Sanctions have a significant impact on actual compliance with information security policies. This is consistent with previous findings on IS security that highlight the role of sanctions (Hoffer & Straub, 1989). This finding regarding sanctions means in practice that practitioners need to state the sanctions for information security policy non-compliance in a visible manner. In particular, it is important to get employees to believe that their non-compliance with information security policies will be detected and severe legal sanctions will take place. The findings suggest that the detection must occur quickly. Also, on the basis of our findings regarding sanctions (social disapproval) and normative beliefs, information security practitioners should realize that social pressure towards information security policy compliance from top management, immediate supervisor, peers and information security staff is important for ensuring employees' information security policy compliance. This is consistent with the findings that the social environment has an effect on an individual's behavior (Ajzen, 1991). To ensure such social pressure, top management, immediate supervisors and information security staff should explicitly make clear the importance of complying with information security policies to their employees. This finding has implications for the information security education strategy of organizations. In the light of our findings, organizations should pay special attention to educating top management, immediate supervisors and information security staff in order that they can spread the word on the importance of adhering to information security policies, and in that way, create social pressure towards information security policy compliance. This is definitely good news for large corporations who may have difficulty in educating all their employees for practical reasons.

Our results suggest that visibility has a significant effect on intention to comply with IS security policies. For practitioners, this means that IS security must be advocated in the organization through education and campaigns in a visible manner. In other words, here the importance is on the visibility, not the exact means by which the security matters are advocated in organizations. External IS security visibility also has an impact on the cognitive process of PMT. Potential sources of external visibility include news or commercials in media such as newspapers, radio, the Internet or TV. For practitioners, this means that IS security incidents reported in the media should be made visible to employees and these should be discussed in organizations.

One possible explanation for rewards not having a significant effect on actual behavior is that there may not be a tangible award system used in the organization. It is also possible that our respondents did not receive any form of appreciation or positive acknowledgement for complying with IS security policies from their organizations. Future research is needed to study organizations that use both tangible and intangible reward systems to facilitate adherence to IS security policy compliance.

Finally, intention to comply with information security policies had a significant impact on actual compliance with information security policies. This is consistent with the literature in the area of technology acceptance: the intention to use a form of technology is shown to correlate with the actual use of that technology (Venkatesh et al., 2003).

References

Agarwal, R. and J. Prasad. "Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology." *Information Systems Research,* 1998, **9:**2, pp. 204-215.

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

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.

Aytes, K. and Connolly, T. "Computer and Risky Computing Practices: A Rational Choice Perspective", *Journal of Organizational and End User Computing*, 16:2, 2004, pp. 22-40.

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

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

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, pp. 1-16.

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

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

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

Gordon, L & Loeb, M. The economics of information security investment. *ACM Transactions on Information and System Security*, 2002, 5:4, pp. 438-457.

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

Hair, J.F.J., Black,W.C., Babin, B.J. Anderson, R.E., Tatham, R.L. *Multivariate data analysis*. 6th ed. Pearson Prentice Hall, 2006.

Heijden, H. V. D. "Factors influencing the usage of websites: the case of a generic portal in The Netherlands." *Information & Management,* 2003, 40, pp. 541-549.

Hoffer, J. A. and D. W. Straub. "The 9 to 5 Underground: Are you Policing Computer Crimes." *Sloan Management Review*, 1989, 30:4, pp. 35-43.

Hoyle, R.H. *Structural Equation Model. Concepts, Issues, and Applications*, H. R. Hoyle (ed.), SAGE publications, Inc, 1995.

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*, 2005, 12:3, pp. 166-184.

Hinde, S. "Security surveys spring crop", *Computers & Security*, 2002, 21:4, pp. 310-321.

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*, 1999, 23:2, pp. 183-213.

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

Moon, J.-W. and Y.-G. Kim. "Extending the TAM for a World-Wide-Web context." *Information & Management*, 2001, 38, pp. 217-230.

Moore, G.C. and Benbasat, I. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation". *Information Systems Research*, 1991, 2:3, pp. 191-222.

Pahnila, S., Siponen, M., Mahmood, A. "Employees' Behavior Towards IS Security Policy Compliance". *Proceedings of 2007 Hawaii International Conference on System Sciences*, 2007.

Puhakainen, P. *A design theory for information security awareness*. Unpublished Ph.D. Thesis, Oulu, Finland, 2006.

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*, 1987, 52:3, pp. 596-604.

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.

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, pp. 113-132.

Schumacker, R.E. and R.G. Lomax, *A Beginner's Guide to Structural Equation Modeling*, Mahwah, New Jersey: Lawrence Erlbaum Associates, 1996, pp. 288.

Siponen, M. “A Conceptual Foundation for Organizational Information Security Awareness”, *Information Management & Computer Security*, 2000, 8:1, pp. 31-41.

Siponen, M.T. “Analysis of modern information security development approaches: towards the next generation of social and adaptable ISS methods”, *Information and organization*, 2005, 15:4, pp. 339-375.

Siponen, M. T., Pahnila, S., Mahmood, A. Adherence to Information Security Policies: An Empirical Study. *Proceedings of the IFIP SEC2007, Sandton, Gauteng, South Africa*, 2007.

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

Straub, D. W. “Validating Instruments in MIS Research", *MIS Quarterly*, 1989, 13:2, pp. 147-169.

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

Straub, D.W. and Welke, R.J. "Coping with Systems Risk: Security Planning Models for. Management Decision-Making", *MIS Quarterly*, 1998, 22:4, pp. 441-469.

Thompson, D. “1997 Computer crime and security survey”, *Information Management & Computer Security*, 1998, 6:2, pp. 78–101.

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

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

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, pp. 367-380.