# Employees' Adherence to Information Security Policies: An Empirical Study

Mikko Siponen[1], Seppo Pahnila[1], and Adam Mahmood[2]
1 Department of Information Processing Science, The University of Oulu, Finland, {mikko.siponen, seppo.pahnila}@oulu.fi
2 Department of Information and Decision Sciences, University of Texas at El Paso, mmahmood@utep.edu

**Abstract**. The key threat to information security is constituted by careless employees who do not comply with information security policies. To ensure that employees comply with organizations' information security procedures, a number of information security policy compliance measures have been proposed in the past. Prior research has criticized these measures as lacking theoretically and empirically grounded principles to ensure that employees comply with information security policies. To fill this gap in research, this paper advances a new model that explains employees' adherence to information security policies. In this model, we extend the Protection Motivation Theory (PMT) by integrating the General Deterrence Theory (GDT) and the Theory of Reasoned Action (TRA) with PMT. To test this model, we collected data (N = 917) from four different companies. The results show that threat appraisal, self-efficacy and response efficacy have a significant impact on intention to comply with information security policies. Sanctions have a significant impact on actual compliance with information security policies. Intention to comply with information security policies also has a significant impact on actual compliance with information security policies.

## 1 Introduction

Up to 90% of organizations confront at least one information security incident within any given year [5, p. 684]. To cope with the increase in information security threats, not only technical solutions, but also information management methods and policies have been proposed. Employees, however, seldom comply with these information security procedures and techniques, placing the organizations' assets and business in danger [32, p. 125]. To address this concern, several information security compliance approaches have been proposed. Aytes and Connolly [3], Siponen [29] and Puhakainen [24] have criticized these extant approaches as lacking not only

theoretically grounded methods, but also empirical evidence on their effectiveness. In fact, only three approaches [4], [34], [35] meet these important criteria. This paper fills this gap in research by first building a new theoretical model, explaining how employees' compliance with information security policies and guidelines can be improved. In this model, we combine PMT with the modern GDT and TRA. The model is then validated using an empirical study.

The results of this study are of relevance to researchers and practitioners. Since the extant studies on information security policy compliance present only anecdotal information on the factors explaining employees' adherence to information security policies with three exceptions mentioned above, it is of utmost importance to study this issue. This information is also useful for practitioners who want to obtain empirically proven information on how they can improve their employees' adherence to information security policies, and hence improve the information security of their organizations.

The paper is organized as follows. The second section reviews previous works. The third section proposes the research model and the fourth discusses the research methodology. The results are presented in the fifth section. The sixth section discusses the implications of the study.

## 2 Previous work on information security policy compliance

To understand the fundamental limitations of the extant works on information security policy compliance, these works have been divided into three categories: (1) conceptual principles without an underlying theory and empirical evidence; (2) theoretical models without empirical support; (3) empirical support grounded upon theories. These categories are discussed next.

**Conceptual principles** present practical principles and suggestions for improving employees' compliance with information security polices. These studies include generic information security awareness training programs by Sommers and Robinson [30], McCoy and Fowler [20 p. 347], Thomson and von Solms [36], McLean [21], Spurling [31, p. 20], and Parker [22, p. 464].

Perry [23, pp. 94-95] offers practical principles for the improvement of information security behavior: highlighting information security violations, sending managers to information security seminars, and getting consultants to evaluate the information security state of the organization. Gaunt [11], Furnell, Sanders and Warren [10] and Katsikas [16] all propose information security awareness programs for improving information security behavior in healthcare contexts. Furnell et al. [9] propose the use of information security training software that helps users to become aware of potential risks and the corresponding information security countermeasures. Finally, Wood [39] suggests 53 means for ensuring that employees comply with information security procedures, such as information security advertisements on coffee mugs.

While all the above propose interesting principles for increasing information security awareness, none of them are theoretically grounded or offer empirical evidence to support their principles in practice.

**Theoretical models without empirical support** contain studies that contribute to the creation of theoretical insights on how employees' information security policy compliance can be increased. Aytes and Connolly's [3] study suggests that the perceived probability and desirability of the outcomes of the individuals' choices explains users' security behavior. Lee and Lee [17] use the social bonds theory, the theory of planned behavior, the social learning theory, and GDT to explain computer crimes, while Siponen [29] suggests the use of the theory of planned behavior, the theory of intrinsic motivation, and need-based theories to ensure that employees follow information security policies and guidelines. Thomson and von Solms [37] suggest the use of social psychology to improve employees' information security behavior.

To summarize, while these works contribute to the creation of theoretical insights on how employees' information security compliance can be increased, they are lacking empirical evidence on their practical usefulness.

**Empirical works grounded upon theories** include Aytes and Connolly [4], Straub [34], Straub and Welke [35] and Woon et al. [40]. Aytes and Connolly [4] use the Rational Choice Model to explain why workers violate information security procedures. Straub [34] and Straub and Welke [35] use the GDT to investigate whether investment in information security measures reduces computer abuse. Weekly hours dedicated to information security, dissemination of information security polices and guidelines, stating penalties for non-compliance, and the use of information security software were found to be most effective deterrents [34, p. 272-273]. Finally, Woon et al. [40] found that the perceived severity of the information 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 literature review, while several information security awareness, education and enforcement approaches exist, only four approaches are theoretically and empirically grounded. Of these three, Woon et al. [40] study wireless network users, while Straub [34] and Straub and Welke [35] focus on classical deterrence theory, and Aytes and Connolly [4] apply the Rational Choice Model. Thus, excluding Straub [34], Straub and Welke [35], and Aytes and Connolly [4], the prior approaches do not offer an exploratory model or evidence of what factors affect employees' information security policy compliance. This study aims to fill this gap.

## 3 The research model

The theoretical model combines PMT, TRA and GDT. PMT is best known for its use in health science: it has been used to motivate people to avoid unhealthy behavior. PMT is divided into two components: threat appraisal and coping appraisal. The former is further divided into threat and coping appraisal, while the latter consists of self-efficacy, response efficacy and response costs. PMT emphasizes the changes produced by persuasive communications [27]. Persuasive communications is based on interacting, aiming to alter the way people think, feel or behave. Thus, the goal of

persuasion is to motivate or to influence an individual's attitude or behavior in a predetermined way.

'Intention to comply with information security policies' and 'actual compliance with information security policies' are based on TRA [8]. Attitude indicates a person's positive or negative feelings toward some stimulus object [2]. According to Ajzen [2], 'intentions' captures 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 engage in a behavior, the more likely the behavior is to be carried out. According to our model, the stronger the intention to comply with information security policies is, the more likely it is that the individual will actually comply with the information security policies.

**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 encounter it [25]. In the context of our study, the negative event is any information security threat. Therefore, in the context of our study, perceived vulnerability refers to employees' perceived assessment of whether their organization is vulnerable to information security threats, which will take place if no measures are taken to counter them.

Perceived severity, on the other hand, refers to the degree of both physical and psychological harm the threat can cause [25]. In our study, it refers to potential harm caused by information security breaches in the organization context. Here our assumption is that if organizations' 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 on the organization (perceived severity), they will not comply with information security policies. Therefore, we hypothesize:

*H1: Threat appraisal affects employees' intention to comply with information security policies.*

**Coping appraisal** is a measure consisting of three dimensions: response efficacy, self-efficacy, and response cost [26], [27]. Response efficacy relates to the belief in the perceived benefits of the coping action [26], that is, belief that carrying out the coping action will remove 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 [6]. Placing self-efficacy theory in the context of our study, it refers to workers' beliefs in whether they can apply and adhere to information security policies; this belief will lead to compliance with these policies. Maddux and Rogers [19] found in their study that self-efficacy was the most powerful predictor of intention. In our study, the response costs were not studied.

Therefore, we hypothesize:

*H2: Self-efficacy affects employees' intention to comply with information security policies.*

*H3: Response efficacy 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. One of the leading theories in the field is GDT, which was originally developed for controlling criminal behavior [14]. Traditionally, the classical deterrence theory suggests that certainty, severity, and celerity of punishment affect people's decisions on whether to commit a crime or not [14]. Certainty means that an individual believes that his or her criminal behavior will be detected, while severity means that it will be harshly punished. Celerity signifies that the sanctions will occur quickly. Straub [34] found that stating penalties for information security policy non-compliance increases proper information security behavior. However, studies by Straub [34] and Straub and Welke [35] employ what Higgins et al. [14] refer to as the classical deterrence theory. Therefore, these seminal studies by Straub [34], [35] do not address three important components of contemporary GDT: social disapproval, self-disapproval and impulsivity. Social disapproval refers to the degree to which family members, friends and co-workers disapprove of the 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:

*H4. Sanctions affect employees' actual compliance with information security policies.*

**Intentions** indicate people's willingness to try to perform the behavior in question [2], adherence to information security policies in this case. Rogers and Prentice-Dunn [27] 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 [38], which, in the context of our study, is adherence to information security policies. Moreover, in our study, behavioral intention is an indicator of the effects of persuasion related to information security policies. Thus we can hypothesize:

*H5. Employees' intention to comply with information security policies affects actual compliance with information security policies.*

## 4 Research methods and results

According to Straub [33] and Boudreau et al. [7], 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.** Constructs and their theoretical background

| Construct | Theoretical background | Adapted from |
|---|---|---|
| Intention to comply | TRA | [1] |
| Actual compliance | TRA | [18] |
| Threat and copying appraisal | PMT | [27] |
| Sanctions | GDT | [14] |

All the items are measured using a standard seven-point Likert scale (strongly disagree – strongly agree). Since the measures presented in Table 1 are not previously tested in the context of information security policy compliance, the present research tests these measures in the information security 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 of 3130 respondents were asked to fill out the web-based questionnaire. The distribution of the respondents was quite geographically spread all over Finland. Taking into consideration missing data and invalid responses we had a total sum of reliable responses of 917, the response rate being 29.3%. 56.1% were males and 43.9% females.

**Reliability and validity**. The data analysis was conducted using SPSS 14.0 and AMOS 6.0 structural equation modeling software (SEM). The mean, standard deviation and correlations of the constructs are shown in Table 2. The content validity of the instrument was ensured by the pilot test as discussed above. 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 2 shows all the model items loaded well, exceeding 0.50 [12]. Divergent validity was assessed by computing the correlations between constructs. Correlations between all pairs of constructs were below the threshold value of 0.90. The variance extracted of all the constructs exceeded 0.5 [13]. 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 [12]. Hence, the reliability and validity of the constructs in the model are acceptable.

**Table 2.** Mean, standard deviation and correlations of the constructs.

| Construct | Mean | Standard deviation | 1. | 2. | 3. | 4. | 5. | 6. |
|---|---|---|---|---|---|---|---|---|
| 1. Actual compliance | 6.16 | 0.98 | 1 | | | | | |
| 2. Intention to comply | 6.35 | 0.88 | 0.848 | 1 | | | | |
| 3. Threat appraisal | 5.72 | 0.99 | 0.374 | 0.351 | 1 | | | |
| 4. Response efficacy | 4.75 | 1.43 | 0.203 | 0.193 | 0.215 | 1 | | |
| 5. Self-efficacy | 5.89 | 1.02 | 0.407 | 0.402 | 0.322 | 0.256 | 1 | |
| 6. Sanctions | 3.80 | 1.58 | 0.217 | 0.132 | 0.333 | 0.156 | 0.140 | 1 |

**Table 3.** 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 | | |
| 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 | | |
| Sanctions | Sanctio1 | 0.91 | 0.83 | 0.90 |
| | Sanctio2 | 0.96 | | |
| | Sanctio3 | 0.89 | | |
| | Sanctio4 | Dropped | | |
| | Sanctio5 | 0.59 | | |
| | Sanctio6 | Dropped | | |

The model was assessed using the maximum likelihood method. The fitness of the model was tested in structural equation modeling using goodness-of-fit criteria, which in practice indicate the degree of compatibility between the proposed model and the observed covariances and correlations.

**Table 4.** Convergent validity and internal consistency and reliability.

| Model | | Criteria |
|---|---|---|
| $\chi^2$ | 8.361 | |
| **df** | 3 | |
| p | 0.039 | |
| CMIN/DF | 2,787 | 2-3 |
| CFI | 0.997 | >0.9 |
| NFI | 0.995 | >0.9 |
| RMSEA | 0.044 | <0.05 |

The fit indexes (Table 4) chosen for this study are based on the literature, and represent three different fit characteristics: absolute fit, comparative fit measures and global fit measures. The chi-square test (χ2) with degrees of freedom, p-value and sample size is commonly used for absolute model fit criteria [15, 28]. Root mean square error of approximation fit index (RMSEA) is used to assess the error due to the simplifying of the model. The Comparative Fit Index (CFI) and Normed Fit Index (NFI) are recommended for model comparison, for comparison between the hypothesized and independent models [15, 28]. Overall goodness of fit was assessed with relative chi-square; χ2/degree of freedom (CMIN/DF). The fit indices indicate that the research model provides a good fit with the data.

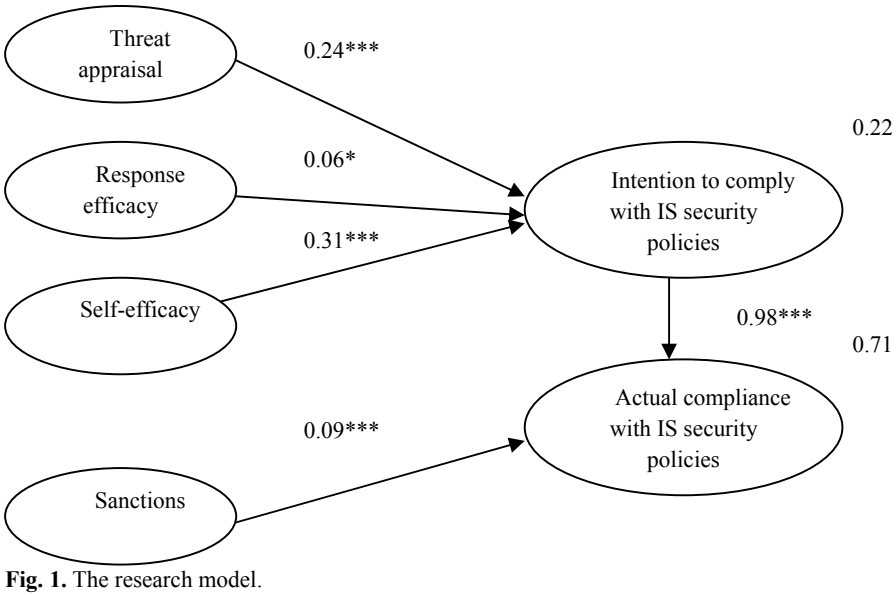


**Fig. 1.** The research model.

The research model yielded a χ2 value of 8.361 with 3 degrees of freedom, with a p value of 0.039 (Fig. 1). The findings indicate that the direct path from threat appraisal (ß = 0.24) to intention to comply with IS security policies is significant. The correlation (Table 2) between threat appraisal and intention to comply with IS

security policies was quite high (0.351), explaining alone about 12.3% of the variance in intention to comply with IS security policies. Response efficacy (ß = 0.06) and self-efficacy (ß = 0.31) also have a significant effect on intention to comply with IS security policies. Sanctions (ß = 0.09) have a significant effect on actual compliance with IS security policies. Intention to comply with IS security policies (ß = 0.98) has a significant effect on actual compliance with IS security policies. In all, the research model accounts for 71% (R2 = 0.71) of the variance in actual compliance.

## 5 Conclusive 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 have not only to be aware of, but also 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 (1) theoretically and (2) empirically grounded principles to ensure that employees comply with information security policies. To address these two problems in the current research, this study first put forward a new model in order to explain employees' information security compliance. This model combined the Protection Motivation Theory, the Theory of Reasoned Action and the General Deterrence Theory. Second, to validate this model empirically, we collected data (N = 917) from four companies.

We found that threat appraisal has a significant impact on intention to comply with information security policies. Hence, it is important that employees are made aware of the information security threats and their severity and celerity for the organization. To be more precise, our findings suggest that practitioners should emphasize to the employees that not only are information security breaches becoming more and more serious for the business of organizations, but their severity to the business of the organization is also increasing.

Self-efficacy, referring to employees' beliefs in whether they can apply and adhere to information security policies, will lead to compliance with these policies in the context of our study, and has a significant impact on intention to comply with information security policies. This finding stresses the perceived relevance of information security policies. If employees do not perceive information security policies as relevant and sufficiently up-to-date for their work, they will not adhere to the policies. Yet it also suggests that it is important to ensure through information security education or verbal persuasion, for example, that employees really can use information security measures.

Our results show that response efficacy has a significant effect on intention to comply with information security policies. In order to minimize IS security breaches, first it is important that the organization's IS security personnel is aware of IS

security threats and knows how to react them. Second, IS security policy should be clear and up-to-date, and third, employees should comply with IS security policies.

Sanctions have a significant impact on actual compliance with information security policies. This 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 also suggest that the detection must occur quickly. Also, on the basis of our findings, information security practitioners should realize that social pressure (sanctions: social disapproval) towards information security policy compliance from top management, the employee's immediate supervisor, peers and information security staff is important for ensuring employees' information security policy compliance. This is consistent with the findings that social environment has an effect on individuals' behavior [2]. To create and ensure such verbal persuasion, top management, immediate supervisors and information security staff should clearly and explicitly explain the importance of complying with information security polices to their employees. This finding has implications for the information security education strategy of organizations. In the light of our finding, organizations should pay special attention to educating top management, supervisors and information security staff in order that they can spread the word on the importance of adherence to information security policies, and hence create social pressure towards information security policy compliance. This is good news for large corporations who may face difficulties educating all their employees.

Finally, intention to comply with information security policies has a significant impact on actual compliance with information security policies. Intention is a motivational factor that influences a behavior by indicating how hard people are willing to try and how much of an effort they are planning to exert in order to perform the behavior. The stronger the intention to engage in the behavior, the more likely it is to be performed [2].

## 6 References

1. Agarwal, R. and J. Prasad, Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology. *Information Systems Research*, 1998. 9(2): p. 204-215.
2. Ajzen, I., "The Theory of Planned Behavior", *Organizational Behavior and Human Decision Processes* 50,2, 1991, 179-211.
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. Aytes, K. and Connolly, T., "Computer and Risky Computing Practices: A Rational Choice Perspective", *Journal of Organizational and End User Computing*, 16,2, 2004, 22-40.
5. Bagchi, K. and Udo, G., "An analysis of the growth of computer and Internet security breaches", *Communications of AIS* 12, 2003, 684–700.
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. Fishbein, M. and Ajzen, I., Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research. MA, Addison-Wesley. 1975.
9. Furnell, S. M., Gennatou, M. and Dowland P. S., "A prototype tool for information security awareness and training", *International Journal of Logistics Information Management*, 15, 5, 2002, 352-357.
10. Furnell, S., Sanders, P. W. and Warren, M. J., "Addressing information security training and awareness within the European healthcare community", in Proceedings of Medical Informatics Europe '97. 1997.
11. Gaunt, N., "Installing an appropriate information security policy in hospitals", *International Journal of Medical Informatics*, 49, 1, 1998, 131-134.
12. 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.
13. Hair, J.F.J., Black, W.C, Babin, B.J, Anderson, R.E., Tatham, R.L., Multivariate data analysis. Sixth ed. 2006: Pearson Prentice Hall.
14. 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.
15. Hoyle, R.H., Structural Equation Model. Conceprts, Issues, and Applications., ed. H. Rick, Hoyle. 1995: SAGE publications, Inc.
16. Katsikas, S. K., "Health care management and information system security: awareness, training or education", *International Journal of Medical Informatics*, 60, 2, 2000, 129-135.
17. Lee, J. and Lee, Y., "A holistic model of computer abuse within organizations", *Information management & computer security*, 10, 2, 2002, 57-63.
18. 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.
19. Maddux, J.E. and R.W. Rogers, Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of experimental social psychology*, 1983. 19: p. 469-479.
20. 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.
21. McLean, K., "Information security awareness - selling the cause", in Proceedings of the IFIP TC11, Eighth International Conference on information security, IFIP/Sec '92. 1992.
22. Parker, D. B., Fighting Computer Crime: A new Framework for Protecting Information, John Wiley & Sons, USA. 1998.
23. Perry, W. E., Management Strategies for Computer Security, Butterworth Publishers, USA. 1985.
24. Puhakainen, P. Design Theory for Information Security Awareness, 2006. Ph.D Thesis, the University of Oulu, Finland.
25. 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.
26. 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.
27. 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.
28. Schumacker, R.E. and R.G. Lomax, A Beginner's Guide to Structural Equation Modeling. 1996, Mahwah, New Jersey: Lawrence Erlbaum Associates. 288.

29. Siponen, M., "A Conceptual Foundation for Organizational Information Security Awareness", *Information Management & Computer Security*, 8, 1, 2000, 31-41.
30. 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.
31. Spurling, P., "Promoting security awareness and commitment", *Information Management & Computer Security*, 3, 2, 1995, 20-26.
32. Stanton, J. M., Stam, K. R., Mastrangelo, P. and Jolton, J., "An analysis of end user security behaviors", *Computers & Security*, 24, 2005, 124-133
33. Straub, D. W., "Validating Instruments in MIS Research", *MIS Quarterly*, 13, 2, 1989, 147-169.
34. Straub, D.W., "Effective IS Security: An Empirical Study", *Information Systems Research*, 1, 3, 1990, 255-276.
35. Straub, D.W. and Welke, R.J., "Coping with Systems Risk: Security Planning Models for. Management Decision-Making", *MIS Quarterly*, 22, 4, 1998, 441-469.
36. Thomson, M.E. and von Solms, R., "An effective information security awareness program for industry", in proceedings of the WG 11.2 and WG 11.1 of the TC-11 IFIP, 1997.
37. Thomson, M. E. and von Solms, R., "Information security Awareness: educating your users effectively", *Information Management & Computer Security*, 6, 4, 1998, 167-173.
38. 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
39. Wood, C. C., "Information Security Awareness Raising Methods", *Computer Fraud & Security Bulletin*, Elsevier Science Publishers, Oxford, England, June 1995, pp 13-15.
40. 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.