INFORMATION SECURITY BEHAVIOR: TOWARDS MULTI-STAGE MODELS

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

Mari Karjalainen, Department of Information Processing Science, University of Oulu, Finland, mari.j.karjalainen@oulu.fi

Mikko Siponen, Department of Computer Science and Information Systems, University of Jyväskylä, Finland, mikko.t.siponen@jyu.fi

Abstract

In order to ensure that employees abide by their organizations' Information Security Policies (ISP), a number of information security policy compliance measures have been proposed in the past. If different factors can explain/predict the information security behavior of those employees who do know the ISP and of those who do not know the ISP, such as is suggested by stage theories, and the existing studies do not control for this issue, then the practical relevance of the existing models will be decreased. In order to test whether different factors explain/predict the information security behavior of those employees who do know the ISP and of those who do not know the ISP, we designed a study using the Protection Motivation Theory (PMT) as the baseline theory. Employees' ISP knowledge was tested by asking a few questions related to their organization's ISP. We divided the data (N=513) into that related to a low knowledge group (regarding the organizations' ISP) and that of a high knowledge group. The results show that the findings between the low knowledge group and the high knowledge group differ substantially. Our results provide an explanation for the inconsistent results in previous IS security research.

Keywords: Information Systems Security, Multi-Stage Model, Protection Motivation Theory.

1 INTRODUCTION

In today's society, information is one of the most valuable assets organizations have. Therefore, organizations have to pay more attention regarding how to protect their critical information. Given this, it is no surprise that Information Systems scholars have devoted increasingly more attention to questions of information security, including in information security special issues of MIS Quarterly (Mahmood et al. 2010) and EJIS (Warkentin & Willison 2009). One of the key issues in information security literature is how employees treat information security. This research paper looks at the practical problem that, although organizations have published policies in place on information security that prescribe required behavior, employees barely comply with these policies (Siponen and Vance 2010). For example, the Information Security Breaches Survey (2010) reported that 92% of large businesses in the United Kingdom had serious security incidents, and the employees caused 80% of them. Easy-to-guess passwords are a typical example of noncompliance with information security policies.

In order to understand why employees comply or do not comply with ISP, several models have been proposed in the past (D'Arcy et al. 2008; Johnston & Warkentin 2010; Siponen & Vance 2010). In most studies, the employees are asked to self-report their intention to comply or actual behavior regarding compliance with ISP. None of the existing studies, including our own articles in leading journals such as *MIS Quarterly* (Siponen &Vance 2010), control for whether employees know the information security policies of their organization. Controlling for employees' knowledge of information security policies is necessary to make sure that the model can be applied to employees with different levels of ISP knowledge. This concern stems from stage models, which suggest that, for any given behavior, people reside at different stages of ISP compliance, and these stages have different factors that influence people's behavior (Weinstein et al. 1998). Stage models in health behavior suggest that those who have knowledge of relevant policies or guidelines regarding health behavior are in different stages than those who do not (Prochaska & DiClemente 1983). If the stage model view were applied to IS security behavior, namely that different factors explain/predict IS security behavior at different stages, then the practical relevance of the existing IS security behavioral research, including our own papers in leading information systems journals (Siponen & Vance 2010), would be questionable. We first realized this problem through our interviews with 80 employees on information security policy compliance. The interviews led us to believe that different factors may explain employees' compliance in the case where employees have different knowledge levels of information security policies, suggesting that there are stages with different independent variables. Given that none of the existing studies controls for this issue, and because of this, the results could have significant implications for information security research. We therefore designed a study to see if different factors (independent variables) explain the IS security behavior of those employees who do know the ISP well and of those who do not know the ISP well.

In our study, we selected the Protection Motivation Theory (PMT) by Rogers and Prentice–Dunn (1997) as the baseline theory because it is the most commonly used model in IS security behavioral studies. According to PMT, change in behavior may be achieved by appealing to an individual's fear. In order to ensure that the results were not related to only one theory (PMT), we added Information Quality by Doll and Torkzadeh (1988) to our model. By adding information quality construct to our model we also tested and ensured that organizations' information security policies are clear and concise to reflect what they actually mean. According to the policy provisions, people in different levels of organization make decisions and behave accordingly, which may not only affect them but

also other people or other organizations. Thus, the quality of information security policy plays an important role how do the people take information security policies into use and comply with it. The model was empirically tested collecting data from four Finnish organizations (N=513). The purpose of this paper is to advance the discussion regarding how to persuade IS security behavior researchers to pay attention to more reliable measures and research approaches. For this reason, our research has important implications for future IS security behavior research.

The rest of the manuscript is organized as follows. The second section discusses the background and related previous research studies. The third section proposes the research model and hypotheses. The fourth section discusses the research methodologies and results. The fifth section is discussion, outlining the key results of the paper, limitations of the research and implications for future research. Finally, the last section provides a conclusion for the manuscript.

2 BACKGROUND AND PREVIOUS WORK

2.1 Background

In our research exploring why employees comply with ISP, we carried out semi-structured qualitative interviews in Finland, Switzerland, the United Arab Emirate and China. The interviewees were randomly selected from employee lists with the criterion that they needed to represent various positions, all of which involved handling valuable information within the organization at their specific locations. Altogether, 80 face-to-face interviews were conducted following the interview principles by Stinger (1999) and Myers and Newman (2007). Seventy-nine interviews were recorded and transcribed to text form (one interviewee preferred the use of field notes).

During these interviews, we observed that employees tend to report that they comply with ISP in general. This is especially the case in the UAE and China and less so in Finland and Switzerland. Regardless of what they reported, most employees did not know the details of their company's ISP, so at best, their compliance was 'hit and miss'. While they reported compliance in terms of generic questions (e.g. 'Do you comply with information security policies?'), many of them also admitted that they may regularly violate various specific ISPs, which made us question the reason behind this (besides a social desirability bias). Further analysis of the interviews suggested that when the employees' level of ISP knowledge differs, different factors (independent variables) seem to explain ISP compliance. The theoretical explanation for this phenomenon is related to the idea of stage theory, suggesting that employees' compliance with ISP is not static but rather dynamic phenomenon and a process that develops through a sequence of stages. According to the stage view, employees could reside at different stages of this process. While no stage models exist as of yet in IS security research, stage theories are common in other areas. For example, research shows that, in addition to human behavior proceeding through a series of stages (in the areas of health decisions (Briedle et al. 2005; Prochacka & DiClemente 1983; Weinstein et al. 1998), moral psychology (Kohlberg 1981) and criminology (Thornberry 1987), the behavior of insects and animals (Briedle et al. 2005; Weinstein et al. 1998) and of organizations (Mohr 1982; Poole et al. 2000) also proceeds through a series of stages. Given that this is the case, it would be safe to assume that employees' IS security behavior could also develop through a series of stages.

A way to prove the existence of stages is to show that at least some factors (or independent variables) are stage-dependent, as suggested by Weinstein et al. (1998). The idea is that if stage-dependent factors do not exist at all, then there is simply no need for stage theories.

Stage models in health behavior suggest that those who have knowledge of the relevant policies or guidelines for health behavior are in different stages than those who do not (Prochaska & DiClemente 1983). In view of this, employees' knowledge of ISP may be broken into different stages of ISP compliance process. For example, Information Quality of the ISP should not be an issue for those who do not know the ISP, but it could be an issue for those who know the ISP well.

In the next section, we will summarize the existing studies and show that none of the existing studies control for employees' knowledge of ISP (or existence of stages).

2.2 Previous Work on Information Security Behavior

Study	Key Idea	Controls for knowledge or include stages
Boss et al. (2009)	Presents an organizational control theory that explains individual IS security precaution behavior.	No
Bulgurcu et al. (2010)	Studies how rational choice explains ISP compliance.	No
Chan et al. (2005)	Explores how the information security climate influences employees ISP compliance.	No
D'Arcy et al. (2008)	Explores how extended deterrence theory explains computer abuse.	No
Guo et al. (2011)	Presents a combined model based on an extension to TRA/TPB.	No
Herath & Rao (2009a)	Integrates PMT, TRA and the deterrence theory.	No
Herath & Rao (2009b)	Studies how penalties, pressures and the perceived effectiveness of employees' actions influence the employees' ISP intentions.	No
Hu et al. (2011)	Examines whether sanctions actually deter employees' noncompliance with ISP.	No
Johnston & Warkentin (2010a)	Investigates how the influence of fear affects the compliance of end users with recommendations to use anti-spyware software.	No
Johnston & Warkentin (2010b)	Examines the effect of perceived source credibility on end user attitudes and intentions to comply with recommended actions to avert spyware.	No
Myyry et al. (2009)	Investigates whether Kohlberg's theory of moral decision-making explains one's intentions to share passwords.	No
Ng et al. (2009)	Investigates how the health belief model explains secure email practices.	No
Pahnila et al. (2007)	Creates a model combining protection motivation theory, the theory of reasoned action, habit and innovation diffusion theory.	No
Siponen et al. (2006; 2007)	Studies how protection motivation theory and rewards explain employees' compliance with ISPs.	No
Siponen & Vance (2010)	Researches how neutralization techniques influence employees' compliance with ISPs.	No
Siponen et al. (2010)	Investigates how protection motivation theory explains employees' compliance with ISPs.	No
Son (2011)	Explains the influence of intrinsic and extrinsic motivation on employees compliance with ISPs.	No
Straub (1990)	Studies how formal sanctions in terms of the Deterrence Theory deter computer abuse.	No

Table 1. Previous work on information security behavior.

As can be seen from Table 1, no existing work on information security behavior controls for whether the respondents know the ISP.

3 POSTULATE AND RESEARCH MODELS

In order to test our postulation that employees with different levels of knowledge of ISP are influenced by different factors, or, in other words, that models can be applied to different levels of ISP knowledge, we selected the Protection Motivation Theory (PMT) as the baseline theory. We selected PMT since it is the most commonly used theory in IS security and other contexts. Another widely used theory in IS is the Deterrence Theory. We did not select this theory since it is connected to the existence of sanctions. Sanctions may vary from organization to organization, if they exists at all, and often the sanctions for ISP violations are not specified, which can be seen in the sense that none of the IS security Deterrence Theory papers specify sanctions. As a result, Deterrence Theory inconsistencies mentioned in the literature (D'Arcy & Herath 2011) can be explained by individuals' different understanding and interpretations of these corporate sanctions and their own experience with these sanctions, both of which are difficult to control for. Finally, the Kohlberg Theory of Cognitive Moral Development and follow-up studies in more than 50 countries suggest that deterrence forms one stage in moral development (Kohlberg 1981). Given that sanctions form one stage of development in terms of Kohlberg' theory of Cognitive Moral Development, we should expect inconsistent results with respect to moral development, but not for knowledge of ISP.

PMT does not present such difficulties, and it is used in more than 30 different contexts. We also added Information Quality to our model as another theory. The rationale for adding another theory is to rule out the possible concern that our results are valid only for one theory—PMT in this case. Next, we'll briefly describe PMT and Information Quality.

PMT aims to motivate people to avoid unhealthy behavior through fear appeals (Rogers & Prentice-Dunn 1997). To date, PMT has been applied to explain over 30 topics, and it is considered to be the leading theory in the area of health behavior motivation (Milne et al. 2000; Rogers & Prentice-Dunn 1997; Sturges & Rogers 1996). The applications of PMT in IS security is included in the studies by Herath and Rao (2009a), Herath and Rao (2009b), Pahnila et al. (2007), Siponen et al. (2006), Siponen et al. (2007), Warkentin and Johnston (2010), Woon et al. (2005) and Workman et al. (2008). PMT is divided into two components: threat appraisal and coping appraisal. Threat appraisal concerns the process of evaluating a fear appeal that is relevant to an individual's perception of how threatened he or she feels. The PMT variables that capture threat appraisal are perceived vulnerability and perceived severity (Rogers & Prentice-Dunn 1997).

Perceived vulnerability assesses how personally vulnerable an individual feels regarding the fact that a negative event will take place if no measures are taken to counter it (Rippentoe & Rogers 1987). Perceived severity refers to the degree of physical and psychological harm a threat can cause (Rippentoe & Rogers 1987).

Coping appraisals consists of two dimensions: response efficacy and self-efficacy (Rogers 1983; Rogers & Prentice-Dunn 1997). In PMT, self-efficacy refers to an individual's ability or judgment of his or her capabilities to perform the coping response actions (Bandura 1977). Moreover, self-efficacy refers to an employee's belief in whether he or she can apply and adhere to IS security policies and procedures easily. Response efficacy refers to the effectiveness of the recommended coping response in reducing threat to an individual (Rogers 1983). It refers to an employee's belief in whether ISP, if complied with correctly, keep IS security breaches at bay.

Information Quality can be defined as fitness for use, which indicates that the most important aspects of Information Quality are usefulness and usability (Strong et al. 1997). Information Quality was included in this research in order to assess how important for their tasks the employees perceive the quality of information security policies to be. An organization's information security policies and the assessment of Information Quality include issues such as the ability to access information quickly, the adequacy of the information, its ease of being understood and how up to date the information is. We included the Information Quality construct in our model in order to compare its relative importance to the low knowledge users versus its importance to the high knowledge users.

We postulate that the employee's level of knowledge of ISP influences which factors of PMT and Information Quality affect the employee's compliance with ISP.

As shown in Figures 1 and 2, we furthermore explore the roles of the control variables of gender and age on IS security policy compliance. We assume no effect from these control variables.

4 RESEARCH METHODOLOGY AND RESULTS

According to Straub (1989) and Boudreau et al. (2001), one can improve the reliability of constructs and results by using validated and tested questions. Accordingly, we used items that have been tried and tested in previous studies when available (Table 2). All the items are measured using a standard seven-point Likert scale (strongly disagree to strongly agree). The data were collected from four Finnish corporations that operate in different areas of business. The security policies of these organizations are communicated similarly through seminars, campaigns and emails. All of these companies have provided their security policies to their employees, and all of these companies have IS security policies available via their intranet networks. Since IS security compliance is a highly sensitive matter for these companies, we are unable to provide further information on these companies and their IS security policies.

In the survey, we controlled for the level of knowledge of a given organization's ISP through five questions that focused on the core issues in the ISP of the organization. The five questions were directly related to the principles of the ISP of the organizations. The answers to the questions were collected by a member of the research team with the help of an information security manager from each company. Questions were selected on the basis that the questions were not ambiguous and did not leave subject to interpretation. In addition, questions were considered as key questions in organizations, as well as concerning the organization's information security policy and the organizations' daily activities. The questions included issues such as how long passwords should be, with whom passwords should be shared, and how documents those are no longer relevant should be handled. Each of the five the questions offered three different multiple choice answer options. We then separately assessed the protective behavior of respondents from the two different groups by adapting PMT and Information Quality. We tested whether there is a difference in the findings between the low knowledge group and high knowledge group.

The questionnaire resulted in 513 relevant responses (response rate = 18.8%). For further analysis, we divided the data into two parts. The first set of data was grouped into the low knowledge category, meaning that the respondents answered 0–2 questions correctly of the five information security policy questions. The data from respondents who answered 3–5 questions correctly were grouped into the high knowledge category.

The number of male respondents was 402 (78.4 %), and the number of female respondents was 109 (21.2%). Two respondents (0.4%) did not reveal their gender. Regarding age distribution, 118 respondents (23%) were less than 30 years old, 152 respondents (29.6%) were 31–40 years old, 148 respondents (28.8%) were 41–50 years old and 91 respondents (17.7%) were more than 50 years old. Four respondents (0.8%) did not reveal their age. Seventy-eight respondents (15.2%) have been employed with their current organization less than one year, 215 respondents (41.9%) have been employed with their current organization 1–10 years and 218 respondents (42.5%) have been employed with their current organization for more than 10 years. Two respondents (0.4%) did not reveal their work history.

4.1 Reliability and Validity

At this stage, we divided the data into two different groups: data from those whose knowledge about their organization's IS security policies was low (N = 340) and data from those whose knowledge about their organization's IS security policies was high (N = 173). Low knowledge indicates that the respondents correctly answered 0–2 of the five basic questions relating to their organization's information security policy. High knowledge indicates that the respondents correctly answered 3–5 of the five basic questions relating to their organization's information security policy. The majority (83%) of the low knowledge respondents responded that they comply with information security policies, 10% responded neutrally (i.e. do not know) and 7% responded negatively. Regarding the high knowledge respondents, 78% responded that they comply IS security policies, 13% responded neutrally and 9% responded negatively. Table 1 shows the age and gender frequencies of both the low and high knowledge groups. Most of the questions used in this research were based on validated questions adapted from prior studies. All the items in the instruments were measured using a seven-point Likert scale ranging from strongly disagree (1) to strongly agree (7).

4.2 The Measurement Model

The descriptive statistics of the study were analyzed using the SPSS 20 software package. Data analysis was conducted using the Smart Partial Least Squares (PLS) 2.0 structural equation modelling technique (Ringle et al. 2005). PLS is a powerful path modelling procedure because of its minimal demands on measurement scales (i.e. both category- and ratio-level indicators can be used in the same model), sample size, and residual distributions (Chin & Newsted 1999). We selected component-based Smart PLS because of the nature of the research. By nature, this research is more predictive than confirmatory theory testing by nature. In order to ensure the validity and reliability of the instruments, convergent and discriminant validity were assessed. Convergent validity indicates whether the indicators represent the same factor. Convergent validity was ensured by assessing the factor loadings and by calculating the variance extracted. As Tables 2 and 3 show, all model items loaded well and exceeded 0.50 (Hair et al. 2006), except the self-efficacy item selfef3, which was dropped. Average variance extracted (AVE) indicates the latent variable's ability to explain the variance of its indicators. AVE should be greater than 0.50, which indicates that the latent variable better explains construct-related variance than error variance (Hair et al. 1998). Tables 2 and 3 report that the variance extracted from all the constructs exceeded 0.50. The internal consistency and reliability among the indicators were assessed by calculating Cronbach's alpha and the composite reliability. Tables 2 and 3 also show that Cronbach's alpha coefficient exceeds the suggested value of 0.60 for all constructs (Hair et al. 2006; Nunnally 1978). The composite reliability of all the constructs exceeded the suggested value of 0.7 (Nunnally 1978).

Measure	Items	Frequency low knowledge group	Percent	Frequency high knowledge group	Percent
Gender	Male	271	79.2	131	75.7
	Female	67	19.4	42	24.3
Missing		4	1.4		
Age	≤ 30	77	22.5	42	24.3
	31 - 40	102	30.0	51	29.5
	41 - 50	94	27.5	55	31.8
	>50	68	20.0	23	13.3
Missing				2	1.2

Table 1. Age and gender frequencies of the low and high knowledge groups.

Construct	Items	Factor loadings	Average variance extracted	Composite reliability	Cronbach's alpha
Actual compliance Based on (Fishbein & Ajzen 1975) Adapted from (Moon & Kim 2001)	Compli1 Compli2	0.960 0.952	0.914	0.955	0.906
Intention to comply Based on (Fishbein & Ajzen 1975) Adapted from (Moon & Kim 2001)	Intent1 Intent2	0.941 0.954	0.899	0.949	0.887
Perceived severity Woon et al. (2005)	Sever1 Sever2 Sever3	0.836 0.814 0.775	0.654	0.850	0.742
Perceived vulnerability Woon et al. (2005)	Vulner1 Vulner2 Vulner3	0.842 0.930 0.743	0.709	0.879	0.796
Response efficacy Woon et al. (2005)	Respef1 Respef2 Respef3	0.635 0.811 0.885	0.615	0.825	0.736
Self-efficacy Woon et al. (2005)	Selfef1 Selfef2 Selfef3	0.805 0.908 Dropped	0.736	0.848	0.651
Information Quality Lee et al. (2002).	Infq1 Infq2 Infq3 Infq4 Infq5 Infq6	0.675 0.761 0.743 0.692 0.803 0.787	0.555	0.882	0.850

Table 2. Low knowledge group: convergent validity, internal consistency and reliability.

Construct	Items	Factor loadings	Average variance extracted	Composite reliability	Cronbach's alpha
Actual compliance	Compli1	0.943	0.887	0.940	0.874
	Compli2	0.949			
Intention to comply	Intent1	0.900	0.817	0.900	0.777
	Intent2	0.908			
Perceived severity	Sever1	0.923	0.583	0.786	0.649
	Sever2	0.886			
	Sever3	0.637			
Perceived vulnerability	Vulner1	0.807	0.691	0.870	0.791
	Vulner2	0.860			
	Vulner3	0.878			
Response efficacy	Respef1	0.737	0.685	0.866	0.785
	Respef2	0.860			
	Respef3	0.878			
Self-efficacy	Selfef1	0.907	0.757	0.862	0.685
	Selfef2	0.831			
	Selfef3	Dropped			
Information Quality	Infq1	0.748	0.590	0.896	0.862
	Infq2	0.815			
	Infq3	0.750			
	Infq4	0.739			
	Infq5	0.709			
	Infq6	0.787			

Table 3. High knowledge group: convergent validity, internal consistency and reliability.

Discriminant validity tests the extent to which the constructs, which should not correlate with each other, are not correlative. Discriminant validity was assessed by computing the correlations between all construct pairs, calculating the square root of the average variance extracted and calculating the cross-loadings of the items. All the cross-correlations were below the threshold value of 0.90 (Hair et al. 1998). The square root of average variance extracted should usually be greater than the pair-wise correlations of the constructs. The number of items, mean, standard deviation and correlations of the constructs, as well as the square roots of the average variance extracted (bolded) are displayed in Tables 4 and 5. As shown in Tables 4 and 5, the square root of the variance extracted from all the constructs is larger than all other cross-correlations. We also tested the loadings and cross-loadings of the items on their constructs. Items loaded more strongly to their own factor than to any other factor. Hence, the reliability and validity of the constructs in the model were acceptable, which confirmed that the operationalization was successful.

Construct	# of items	Mean	SD	1.	2.	3.	4.	5.	6.	7.
1. Actual compliance	4	5.85	1.07	**0.956**						
2. Intention to comply	5	6.16	0.97	0.650	**0.943**					
3. Severity	4	5.05	1.18	0.207	0.175	**0.809**				
4. Vulnerability	4	4.71	1.18	0.112	0.071	0.452	**0.842**			
5. Response efficacy	4	4.77	1.12	0.141	0.160	0.087	0.074	**0.784**		
6. Self-efficacy	2	4.71	1.24	0.212	0.152	0.146	0.122	0.169	**0.858**	
7. Information Quality	2	4.28	1.10	0.182	0.169	0.128	0.049	0.315	0.349	**0.745**

SD = Standard deviation. Note: The bolded diagonal elements are the square roots of the average variance extracted.

Table 4. Low knowledge group: mean, standard deviation and correlations of the constructs.

Construct	# of items	Mean	SD	1.	2.	3.	4.	5.	6.	7.
1. Actual compliance	4	5.55	1.27	**0.942**						
2. Intention to comply	5	6.00	1.10	0.286	**0.904**					
3. Severity	4	5.02	1.12	0.308	0.288	**0.764**				
4. Vulnerability	4	5.00	1.14	0.187	0.212	0.389	**0.831**			
5. Response efficacy	4	4.78	1.17	0.257	0.275	0.102	0.010	**0.823**		
6. Self-efficacy	2	4.63	1.38	0.294	0.167	0.102	-0.068	0.264	**0.870**	
7. Information Quality	2	4.39	1.16	0.286	0.226	0.211	-0.026	0.529	0.464	**0.768**

Table 5. High knowledge group: mean, standard deviation and correlations of the constructs.

4.3 The Research Models

The research models and the results are displayed in Figures 1 and 2, which show the estimated path coefficients and the significance of the path (indicated with asterisks). Tests of significance were performed using the bootstrapping procedure. Bootstrapping t-test values are indicated below the path coefficient value. In order to assess the differences in individuals' protective behavior, we divided the data (N = 513) into data associated with the low knowledge group (N = 340) and data associated with the high knowledge group (N = 173) regarding the individuals' knowledge of their organization's information security policies.

In the case of low information security policy knowledge (Figure1), standardized betas show that severity (ß = 0.158) and response efficacy (ß = 0.129) have a significant impact on intention. Intention (ß = 0.633) has a significant impact on information security policy compliance. Vulnerability and self-efficacy have insignificant impacts on intention. Control variables have insignificant impacts on compliance. Overall, the research model accounts for 6.3% ($R^2 = 0.063$) of the variance in intention. The whole model accounts for 43.2% ($R^2 = 0.432$) of the variance in IS security policy compliance.

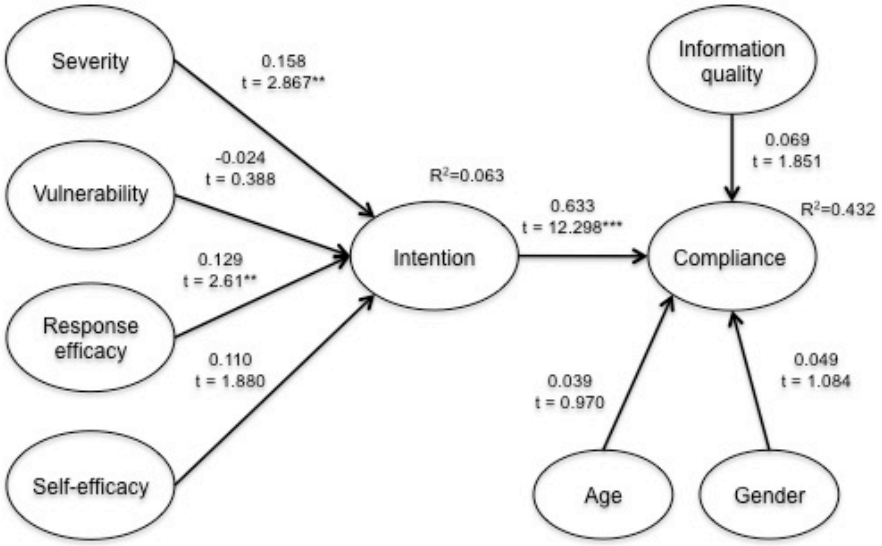

Figure 1. Low knowledge group: research model.

In the case of high information security policy knowledge (Figure 2), standardized betas show that severity (ß = 0.200), vulnerability (ß = 0.141) and response efficacy (ß = 0.230) have significant impacts on intention. Self-efficacy has an insignificant impact on intention. Intention (ß = 0.633) has a significant impact on information security policy compliance. The control variable of age (ß = 0.153) has a significant impact on compliance, whereas gender has an insignificant impact on compliance. Overall, the research model accounts for 16.7% (R^2 = 0.167) of the variance in intention. The whole model accounts for 49.6% (R^2 = 0.496) of the variance in information security policy compliance.

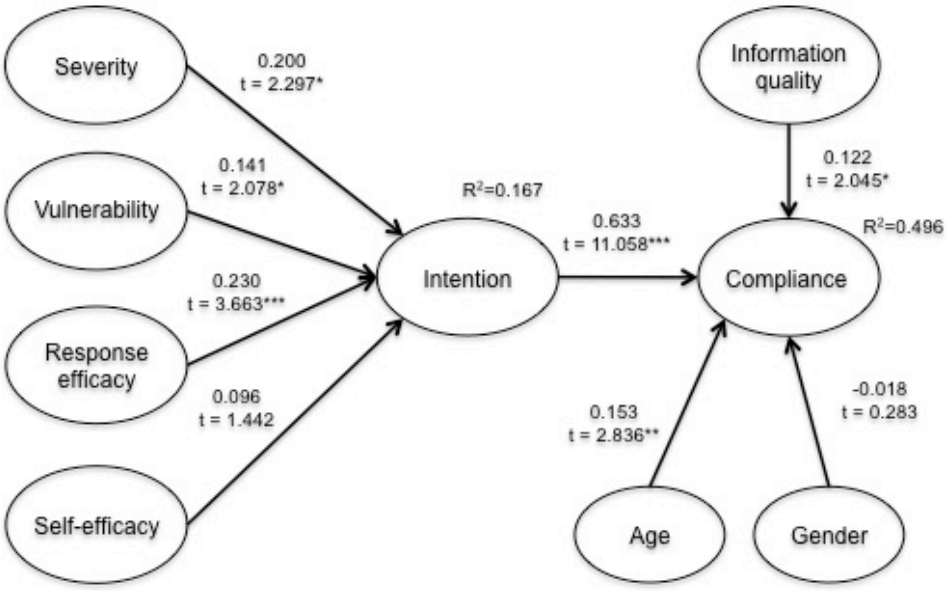

Figure 2. High knowledge group: research model.

5 DISCUSSION

We examined whether employees' level of ISP compliance forms at different stages where the exact same independent variables do not explain the behavior in both stages. As a key contribution, this study provides support for stage theory thinking, namely that there exists different stages in employees ISP compliance, and the exact same independent variables do not explain the behavior in

both stages. Our 'stages' were employees with low knowledge of their organization's ISP and those with high knowledge of their organization's ISP.

Our findings indicate, in the case of low knowledge of an organization's information security policies, that the direct paths from severity and response efficacy to intention to comply with information security policies were significant. Intention to comply with information security policies had a significant effect on actual compliance. In the case of high knowledge of an organization's information security policies, severity, vulnerability and response efficacy have significant impacts on intention to comply with information security policies. The significance of severity and vulnerability suggest that employees are aware of the information security threats and their severity and consequences for the organization. To be more precise, our findings reveal that those who have a high knowledge of their organization's information security policies are not only aware of the fact that the information security breaches are becoming increasingly serious for the organization, but they are also aware that the consequences could be increasingly severe for the normal business of the organization if the threat were to occur.

It is an interesting finding that the impact of self-efficacy on intention was insignificant. Although respondents are aware of their organization's information security policies, they rely on security staff to keep the information security breaches at bay, and they do not strongly believe their own actions can keep the information security breaches at bay. It could be that, if there have not been information security incidents within the organization, employees do not have a perception of danger and are therefore not motivated to take protective action (Rogers & Prentice–Dunn 1997). Another explanation could be related to the 'boomerang interaction effect'. If the threat is high, people do not believe they will be able to cope with the danger, and the intention to perform coping responses diminishes (Rogers & Prentice–Dunn, 1997).

Information quality has a significant impact on information security compliance. This finding differs from the finding of the low knowledge group. This finding suggests that respondents perceive that information security policies are relevant and sufficiently up to date for their work and they do adhere to them, but they do not rely on their own capabilities to cope with information security breaches. With respect to control variables, age has a significant impact on compliance. This finding also differs from the finding of the low knowledge group.

Intention to comply with information security policies had a significant impact in both groups 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).

The coefficients of determinations differed when comparing the low and high knowledge groups, especially in the case of compliance intention. Regarding the high knowledge group, the model accounts for 16.7% of the variance in intention and, respectively, the percentage for the low knowledge group is 6.3%. In other words, respondents who are more familiar with their organization's information security policies have substantially lower protection motivation intention compared to respondents in the high knowledge group. This is one of the most important findings of the study considering that the respondents of both knowledge groups responded that they comply with IS policies very conscientiously. This finding reveals that using self-reporting questionnaires without controlling for individuals' actual behavior may result in misleading conclusions. The whole model accounts for 49.6% of the variance in information security policy compliance for the high knowledge group and 43.2% for the low knowledge group. It is also interesting that the coefficient of determination (R^2) is fairly high in the low knowledge group compared to the high knowledge group

considering the low knowledge group's low knowledge level of the organization's information security policies. In all, as our findings show, it is important to pay attention to the reliability of the research design, the research measures and especially the research approach in the early stages of the study.

5.1 Limitations and Implications for Future Research

Our model does not adhere strictly to a stage theory as such; however, our results support stage theory thinking. Future research is needed to further explore the different stages related to employees' information security behavior. In addressing this issue, we especially call for inductive studies and new theory development that unveils the different stages of information security behavior. With respect to gender distribution, majority of the respondents were male (78.4%). This should be taken into account when considering the generalizability of the results.

For those who continue to develop non-stage models— the existing information security models listed in Table 1 being examples of their work—we encourage these information security scholars to control for the employees' knowledge of ISP and hence show the applicability of their models to people who have different levels of knowledge of their corporation's ISP.

6 CONCLUSION

Employees' careless information security behavior is a problem that has concerned information security research and practice. IS security research has approached this problem by developing and testing a number of information security policy compliance models, explaining or predicting employees' information security behavior. Our interviews with 80 employees on ISP compliance caused us to question whether different factors explain information security behavior for those employees who know the ISP well and for those who do not know it well, such as is suggested by stage theories. None of the existing studies control for this issue, namely whether employees know the information security policies. Controlling for employees' knowledge of information security policies is important because it ensures that the model in question is applicable to employees with different levels of knowledge regarding information security policies. If different factors explain or predict IS security behavior for employees with different levels of knowledge of the information security policies, as suggested by stage theories, and the existing studies do not control for this issue, then the practical relevance of the existing models will be decreased.

In order to test whether different factors explain/predict the information security behavior of those employees who do know the ISP and of those who do not know the ISP, we designed a study using the Protection Motivation Theory (PMT) as the baseline theory. In order to make sure that the results were not related to only one theory (PMT), an Information Quality theory was added to the model. The proposed model was tested using a sample of 513 employees in Finland. Employees' actual ISP knowledge was tested by asking a few basic questions related to their organization's ISP. We divided the data (N = 513) into that of a low knowledge group (N = 340) and that of a high knowledge group (N = 173), depending on how much the respondents were aware of the ISP of their respective organizations. Low knowledge indicates that the respondents answered correctly to 0–2 of the five basic questions related to their organization's information security policy, including how long passwords should be, with whom passwords should be shared, and how documents that are no longer relevant should be handled. High knowledge indicates that the respondents answered correctly 3–5 of the five basic questions related to their organization's ISP. About 80% of the respondents in both groups responded that they comply with ISP. The findings show that there are significant differences between the groups. Our results may explain the inconsistent results in information security as resulting from different levels of knowledge of information security policies. A plausible theoretical explanation for our results (and inconsistencies in previous information security research) can be related to the stage theory viewpoint, suggesting that different knowledge levels can be seen as different stages of employees' ISP compliance. At a minimum, future research on information security behavioral studies needs to control for employees' knowledge of ISP.

References

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behaviour change, Psychological Review 84(2), 191-215.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security, European Journal of Information Systems, 18(2), 151- 164.

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

Briedle, C., Riemsma, R.P., Pattenden, J., Sowden, A.J., Mather, L., Watt, I.S., and Walker, A. (2005). Systematic review of the effectiveness of health behavior interventions based on the transtheoretical model. Psychology and Health*,* 20(3*)*, 283-301.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly 34(3), 523-548.

Chan, M., Woon, I. and Kankanhalli, A. (2005) Perceptions of information security in the workplace: Linking information security climate to compliant behavior. Journal of Information Privacy & Security, 1(3), 18-41

Chin, W.W. and Newsted, P.R. (1999). Structural Equation Modeling Analysis with Small Samples Using Partial Least Squares. Statistical Strategies for Small Sample Research. In Statistical Strategies for Small Sample Rerearch (Hoyle, R. Ed.), pp. 307-341, Sage Publications, Thousand Oaks, CA.

D'Arcy, J. and Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. European Journal of Information Systems, 20(6), 643-658.

D'Arcy, J., Hovav, A. and Galletta, D.F. (2008). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research 20(1), 79-98.

Doll, W.J. and Torkzadeh, G. (1988). The measurement of end-user computing satisfaction. MIS Quarterly, 12(2), 259-274.

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

Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. Journal of Management Information Systems, 28(2), 203-236.

Hair, J.F.J., Anderson, R.E., Tatham, R.L. and Black, W.C. (1998). Multivariate Data Analysis. Fifth edition: Prentice Hall Inc, Upper Saddle River, New Jersey.

Hair, J.F.J., Black, W.C, Babin, B.J, Anderson, R.E. Tatham, R.L. (2006). Multivariate data analysis. Sixth edition, Pearson Prentice Hall.

Herath, T. and Rao, H.R. (2009a). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.

Herath, T., and Rao, H. R. (2009b). Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness, Decision Support Systems, 47(2), 154–165.

Hu, Q., Zhang, C. and Xu, Z. (2011). How can you tell a hacker from a geek? Ask whether he spends more time on computer games than sports! In DeWald Information Security Research Workshop Blacksburg, Virginia.

ISBS (2010). Information Security Breaches Survey. PricewaterhouseCoopers on behalf of the UK Department of Business, Enterprise and Regulatory Reform (BERR). URL: http://www.pwc.co.uk/audit-assurance/publications/isbs-survey-2010.jhtml. Cited 2013/4/16.

Johnston, A.C., and Warkentin, M. (2010a). Fear appeals and information security behaviors: An empirical study. MIS Quarterly 34(3), 549-566.
Johnston, A.C. and Warkentin, M. (2010b). The influence of perceived source credibility on end user attitudes and intentions to comply with recommended IT actions. Journal of Organizational and End User Computing, 22(3), 1-21
Kohlberg, L. (1981). Essays on Moral Development, Vol. I: The Philosophy of Moral Development. Harper & Row, San Francisco, CA.
Lee, Y.W., Strong, D.M., Kahn, B.K. and Wang R.Y.(2002). AIMQ: A methodology for information quality assessment. Information & Management 40(2), 133-146.
Milne, S, Sheeran, P. and Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. Journal of Applied Social Psychology, 30(1), 106-143.
Mohr, L.B. (1982). Explaining Organizational Behavior. Jossey-Bass, San Francisco.
Moon, J.W and Kim, Y.G. (2001). Extending the TAM for a World-Wide-Web context. Information & Management, 38(4), 217-230.
Myers, M. and Newman, M. (2007). The qualitative interview in IS research: Examining the craft. Information and Organization, 17(1), 2-26.
Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. and Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study, European Journal of Information Systems 18(2), 126-139.
Ng, B., Kankanhalli, A. and Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815–825.
Nunnally, J.C. (1978). Psychometric Theory, MacGraw-Hill, New York.
Pahnila, S., Siponen, M. and Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 156b - 156b.
Poole, M.S., Van de Ven, A.H., Dooley, K. and Holmes, M.E. (2000). Organizational Change and Innovation Processes: Theory and Methods for Research. Oxford University Press, Oxford.
Prochaska, J. & DiClemente, C. (1983). Stages and processes of self-change of smoking: Toward an integrative model of change. Journal of Consulting and Clinical Psychology 51(3), 390-395.
Ringle, C.M., Wende, S. and Will, A. (2005). SmartPLS 2.0 (M3) Beta. Hamburg.
Rippetoe, S. and Rogers, R.W. (1987). Effects of components of protection - Motivation theory on adaptive and maladaptive coping with a health threat. Journal of Personality and Social Psychology, 52(3), 596-604.
Rogers, R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation theory. In Social Psychophysiology (Cacioppo, J. and Petty, R. Eds.), Guilford, New York.
Rogers, R.W. and Prentice-Dunn, S. (1997). Protection motivation theory. In Handbook of Health Behavior Research I: Personal and Social Determinants (Gochman, D.S. (Ed.), pp. 113-132, Plenum Press, New York, NY.
Siponen, M. and Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487–502
Siponen, M., Pahnila, S., Mahmood, M,A. (2010). Compliance with information security policies: An empirical investigation. IEEE Computer, 43(2), 64-71.
Siponen, M.T., Pahnila, S. and Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. In Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007), New Approaches for Security, Privacy and Trust in Complex Environments (Venter H, Eloff M, Labuschagne L, Eloff J & von Solms R. Eds.), pp. 133-144 Sandton, South Africa.
Siponen, M., Pahnila, S. and Mahmood, A. (2006). Factors influencing protection motivation and IS security policy compliance. Innovations in Information Technology, 1–5.
Son, J. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information and Management, 48(7), 296-302.
Stinger, E.T. (1999). Action Research. Second edition. Sage Publications, Thousand Oaks CA.
Straub, D.W. (1989). Validating instruments in MIS research. MIS Quarterly, 13(2), 147-169.
Straub, D.W. (1990). Effective IS security: An empirical study. Information_System Research, 1(2), 255-277.
Strong, M.D., Lee W.Y. and Wang, Y.R. (1997). Data quality in context. Communications of The ACM 40(5), 103-110.

Sturges, J.W. and Rogers R.W. (1996). Preventive health psychology from a development perspective: An extension of protection motivation theory. Health Psychology 15(3), 158-166.
Thornberry, T.P. (1987). Toward an Interactional Theory of Delinquency. Criminology 25 (4), 863-891.
Venkatesh,V., Morris, M.G., Davis, G.B. and Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478.
Warkentin, M. and Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. European Journal of Information Systems, 18(2), 101-105.
Weinstein, N.D., Rothman, A.J. and Sutton, S.R. (1998). Stage theories of health behavior: Conceptual and methodological issues. Health Psychology 17(3), 290 – 299.
Woon, I.M.Y., Tan, G.W. and Low, R.T. (2005). A protection motivation theory approach to home wireless security. In Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas, pp. 367-380.
Workman, M., Bommer H.W., Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior 24(1), 2799-2816.