Information & Management 49 (2012) 190–198

Contents lists available at SciVerse ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im

Motivating IS security compliance: Insights from Habit and Protection Motivation Theory

Anthony Vance [a,*], Mikko Siponen [b], Seppo Pahnila [b]

[a] Information Systems Department, Marriott School of Management, Brigham Young University, United States
[b] IS Security Research Center, Department of Information Processing Science, University of Oulu, Linnanmaa, P.O. Box 3000, FIN-90014 Oulun yliopisto, Finland[1]

ARTICLE INFO

Article history:
Received 30 January 2010
Received in revised form 23 August 2011
Accepted 23 March 2012
Available online 17 April 2012

Keywords:
Information security policy compliance
Protection Motivation Theory
Habit theory
Information security
Scenario methodology

ABSTRACT

Employees' failure to comply with IS security procedures is a key concern for organizations today. A number of socio-cognitive theories have been used to explain this. However, prior studies have not examined the influence of past and automatic behavior on employee decisions to comply. This is an important omission because past behavior has been assumed to strongly affect decision-making.

To address this gap, we integrated habit (a routinized form of past behavior) with Protection Motivation Theory (PMT), to explain compliance. An empirical test showed that habitual IS security compliance strongly reinforced the cognitive processes theorized by PMT, as well as employee intention for future compliance. We also found that nearly all components of PMT significantly impacted employee intention to comply with IS security policies. Together, these results highlighted the importance of addressing employees' past and automatic behavior in order to improve compliance.

1. Introduction

Organizations typically encounter at least one breach of security due to an information security policy violation per year [1]. Furthermore, it has been estimated that over half of all IS security breaches are indirectly or directly caused by employee failure to comply with IS security procedures [19]. It is not surprising that a critical concern for organizations is the extent to which employees comply with information security policies [6,18]. A number of behavioral approaches have been proposed in the literature for either improving employees' compliance with the security procedures of their organizations or to explain their reasons for computer abuse [16].

Many of behavioral approaches draw upon theories of Criminology and Psychology, such as Deterrence Theory [9], Neutralization Techniques [17] and socio-cognitive [11]. These, while valuable, have not resulted in examination of the influence of past compliance behavior on appraisals of information security threats and coping responses. This is an important omission, since Protection Motivation Theory (PMT) suggests that past behavior strongly influences the process of assessing threats and one's ability to cope with them.

To address this gap, we integrated the full PMT model with habit, a routinized form of past and automatic behavior [10]. Research on the theory of habit has highlighted the pervasive effect of habit on human behavior. This allowed us to examine the influence of routinized past IS security compliance behavior on the threat appraisal and coping mechanisms theorized in PMT.

To evaluate our model, we performed an empirical study in an organization in Finland (with a population of 210 employees). Our results offer relevant insights for both practitioners and researchers.

2. An overview of PMT and past applications in IS security

PMT explains how individuals are motivated to respond to warnings about threats or dangerous behaviors, termed *fear appeals*. In interpreting such messages, individuals use a cognitive process to weigh their response to the threat. PMT includes three factors that explain how threats are perceived, termed *threat appraisal factors*. These are rewards or benefits (any intrinsic or extrinsic motivation for increasing or keeping an unwanted behavior), severity (the magnitude of the threat), and vulnerability (the extent to which the individual is perceived to be susceptible to the threat).

PMT also includes three factors that explain an individual's ability to cope with the threat, termed *coping appraisals*. These are response efficacy (the belief in the perceived benefits of the coping action by removing the threat), response cost (to the individual in implementing the protective behavior), and self-efficacy (the degree that he or she believes it is possible to implement the protective behavior).

* Corresponding author. Tel.: +1 801 361 2531; fax: +1 509 275 0886.
E-mail addresses: anthony@vance.name (A. Vance), mikko.siponen@oulu.fi (M. Siponen), seppo.pahnila@oulu.fi (S. Pahnila).
URL: http://www.anthonyvance.com
[1] http://www.issrc.oulu.fi/.

0378-7206/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.im.2012.04.002

2.1. Previous IS security research using PMT

Because of its general nature, PMT has recently been applied to the domain of information security. Previous work in organizational context have focused on employees compliance with IS security procedures. However, no recent study has fully employed all of the coping and threat appraisals of PMT.

Of the four papers dealing with this [4,7,13,22] none discussed *Antecedent sources of Information* or *Rewards.* All dealt with *Vulnerability* and *Severity*, though Pahnila et al. combined them. All dealt with *Response-* and *Self-Efficacy*. Also response cost was only used in two studies: those by Herath and Rao and Pahnila et al.

In the context of IS security compliance, rewards are considered as only those for compliance, which presents an incomplete view of the cognitive mediating processes central to PMT. Furthermore, past behavior may be considered to be an important source of information influencing protection motivation. However, no studies have investigated sources of information antecedent to the PMT process. To overcome these two gaps, we extended the full PMT model to include habit as an antecedent effect.

3. Theoretical model

Our theoretical model employed habit theory and PMT. The original formulation of PMT explicitly suggested that "prior experience" was a preceding factor for PMT. Also it was noted that the PMT model assumed that both situational cues and habit had important effects on the decision-making process of PMT.

This view was also shared by investigators of the effect of habit, noting that many of the behaviors studied were repetitive, executed on a daily basis, and therefore possibly routine or habitual. We therefore theorized that habit was a determinant of the cognitive mediating process of protection motivation: our integrated model is shown in Fig. 1.

3.1. Protection Motivation Theory

PMT suggests that information about a threat causes a cognitive mediating process in individuals that appraises positive or negative responses. Thus employees' non-compliance with information security policies represents a *maladaptive* response, while compliance with them is an *adaptive* response. The maladaptive response invokes *threat appraisal factors*, which decrease the likelihood of maladaptive response, such as non-compliance with IS security policies

One of the three threat appraisal factors is rewards (or benefits), which results in any intrinsic or extrinsic motivation for increasing or keeping an unwanted behavior which in our context is an employees' non-compliance with information security policies.

Intrinsic and extrinsic rewards will increase the probability of a maladaptive response whereas perceptions of the severity and vulnerability to threats will decrease the probability of such a response. Rewards indicate physical or psychological pleasure or peer approval, which increase the probability of a maladaptive response. If an individual perceives that the reward for not adopting the coping response is higher than adopting it, then the individual will be less likely to adopt the coping response. In our context, we conceptualize rewards as saving time by not complying with the information security policy. Research on information security policy compliance shows that people see saving time as a benefit for non-compliance [21].

Vulnerability is to the probability that an unwanted incident will happen if no actions are taken to prevent it. In our study, vulnerability denotes employees' assessment of whether their

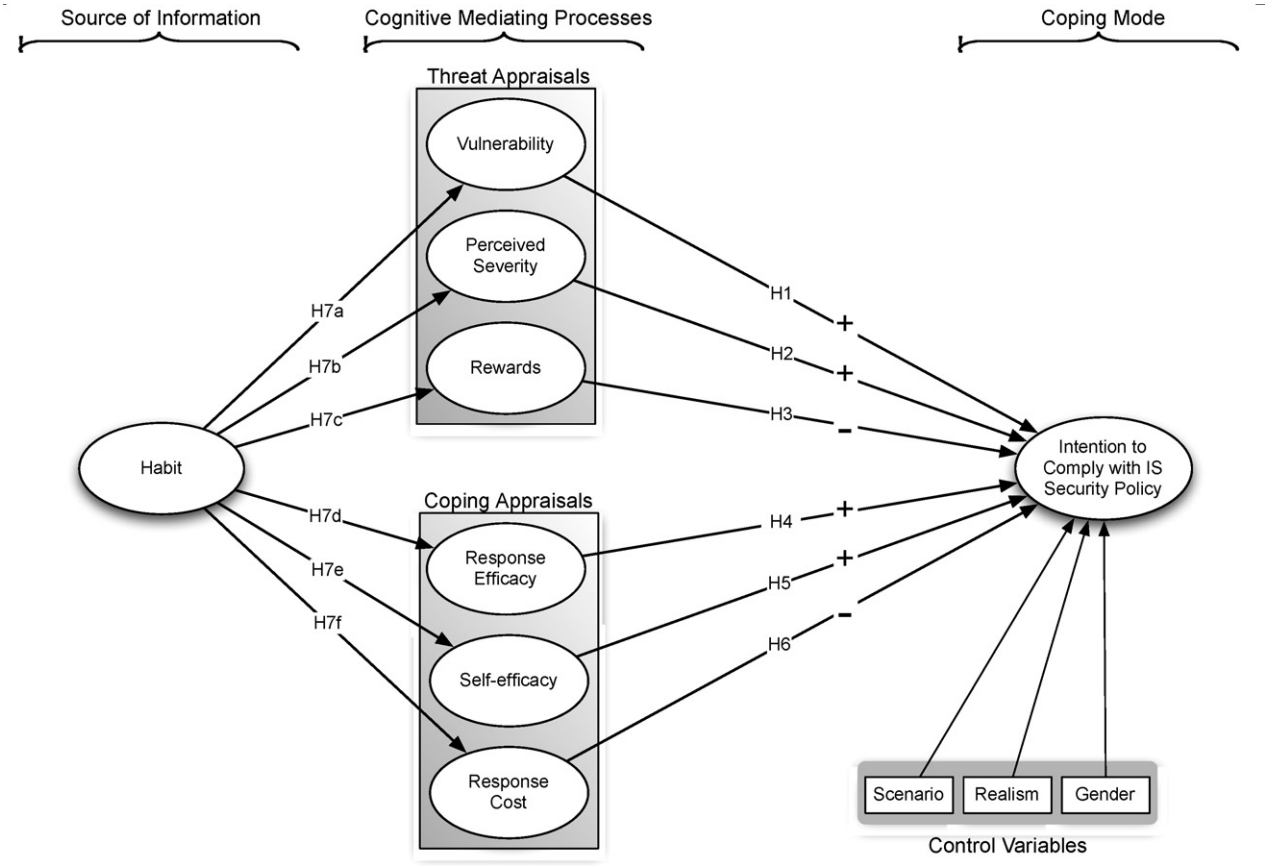

Fig. 1. Research model.

organization is open to IS security threats if no measures are taken to prevent them. Severity, is the level of the potential impact of the threat (i.e., its severity and how severe the damage that it can cause). In our context, it refers to the severity of the IS security breach, and the possible negative event caused by the breach in an organization. Hence, we hypothesized:

H1. Vulnerability positively affects employees' intention to comply with IS security policies.

H2. Perceived severity positively affects employees' intention to comply with IS security policies.

H3. Rewards negatively affect employees' intention to comply with IS security policies.

PMT also consists of coping appraisal factors, which depend on the increase of the adaptive response (here this is employees' compliance with information security policies). In our context, compliance with IS security policies should be an effective protection against IS security threats.

Self-efficacy in our study, refers to employees' belief that they can successfully comply with IS security policies, which should enhance compliance with policies and procedures. Finally, response cost includes the inconvenience incurred in complying with IS security policies. Hence, we hypothesized:

H4. Response efficacy positively affects employees' intention to comply with IS security policies.

H5. Self-efficacy positively affects employees' intention to comply with IS security policies.

H6. Response cost negatively affects employees' intention to comply with IS security policies.

3.2. Habit theory

Habit is a form of routinized behavior. Often habit is assessed with a measurement of past behavior or behavioral frequency. This view has been criticized, because behavioral frequency alone does not recognize the automatic character of habit [20]. To address this concern, Verplanken and Orbell [20] developed and validated a habit instrument that recognizes the key element of the habit construct: automaticity.

Based on these arguments, we used the habit instrument of Verplanken and Orbell [20].

Prior research has approached the issue from three perspectives: the moderating effect of habit on the relationship between intention and IT use, the direct effect of habit on IT use, and the direct effect of habit on intentions to use IT.

The protection motivation process seeks to influence individuals' well-established practices. According to PMT, prior experience includes feedback from personal experiences with targeted maladaptive and adaptive responses.

Habit theory suggests that many actions occur without conscious decision to act and are performed because individuals are accustomed to performing them; frequently repeated behavior is more controlled by situational cues than conscious decision-making.

Further, it proposes that the initiation of a new behavioral pattern requires a conscious decision and the new behavior will gradually become automatic. Cues, that trigger automatic behavior are numerous, clear and consistent. Because situational cues relate closely to habitual behavior, then awareness of threats, trigger the cognitive process (in our study, the PMT process), which leads to intention to behave. Ortiz de Guinea and Markus [12] emphasized that automatic behavior was not solely triggered by behavioral sequence but rather by a set of goals and the means developed to achieve the goals.

Thus, we posit that habitual behavior to comply with IS security policies has a negative influence on response cost and rewards, and is positive for all other constructs of PMT. Hence, practicing the habit of complying with IS security policies decreases both the rewards for non-compliance and the response cost (e.g., time lost when complying with IS security policies). In turn, practicing the habit of complying with IS security policies will have a positive influence on severity, self-efficacy, response efficacy, and vulnerability. Thus, we hypothesized:

H7a. Habit positively influences vulnerability.

H7b. Habit positively influences perceived severity.

H7c. Habit negatively influences rewards.

H7d. Habit positively influences response efficacy.

H7e. Habit positively influences self-efficacy.

H7f. Habit negatively influences response cost.

4. Research design

We used a hypothetical scenario method which presented respondents with a detailed vignette describing an action or decision. Respondents were then asked to respond to survey items. Such methods are a common way of assessing anti-social and ethical/unethical behavior, and are increasingly used in studies of computer abuse [5].

A key step in designing the scenarios in our research was to ensure that they were realistic and commonplace to respondents. First, in order to ensure the content validity of our scenarios, we surveyed a panel of 111 IS security experts and information security managers at a variety of Finnish organizations using an open-ended questionnaire to list four IS security procedure violations that were both common and consequential. We obtained 54 responses yielding a 49% response rate. We then categorized responses using content analysis and ranked the responses.

We presented the results of the top ten violations to the security management department of our target organization. Members of the department were asked to select five of these which were both common and a problem in *their* organization. Based on these, we (with the organization's security management teams) developed five scenarios of different IS policy violations. These were: sharing passwords, failing to lock or log off a workstation, allowing reading confidential material at printers, allowing children at home to use and install software on a work laptop, and copying highly sensitive information to a USB stick without encryption (refer to Table A1 for the scenarios). Each scenario was reviewed by five information security managers to ensure that the designed scenarios were realistic in content. Based on their feedback, the scenarios were revised.

4.1. Instrumentation

All items were adapted from previously validated instruments when possible. All items were measured on an 11-point Likert scale from 0 to 10. Composite measures for deterrence constructs were calculated to create a sanction measure that reflected both the risk and cost of perceived punishment by multiplying each severity measure by its associated certainty measure. All measurement items are shown in Table A2.

Two dependent variables were used to measure the likelihood a respondent would perform in the same way as the scenario

character; the intention items were reversed to obtain a measure of intention to comply. This use of intention as a dependent variable is consistent with PMT, as protection motivation has typically been measured by behavioral intention. The response scale for this item ranged from 0 (no chance at all) to 10 (100 percent chance). In addition to items measuring latent constructs, we included a single-item measure that asked respondents to rate the reality of the given scenario. This item ranged from 0 (not believable) to 10 (100 percent believable).

4.2. Pretest

In addition to the expert review of the scenarios, the survey items were reviewed by six information security managers to evaluate the content validity and relevance of the survey items; then we pretested our instrument to evaluate the psychometric properties of the items.

A small convenience sample was chosen for the pretest. Data were collected from 42 graduate students at a Finnish university. This sample was chosen because these students had been made aware of, and are obliged to follow, the university information security policy. Factorial validity was assessed using Principal Components Analysis; item reliabilities were assessed using Cronbach's α. Items contributing to either poor factor validity or reliability were either rephrased or dropped from the survey.

4.3. Primary data collection

Primary data was collected from a Finnish municipal organization. We chose a single organization so that we could ensure that the scenarios were realistic and contextually relevant to those who responded, as realism is a key concern of the scenarios method. The target population was therefore all clerical and administrative staff of the organization.

This particular organization was selected because of its use of IS security policies. Furthermore, the organization publishes its IS security policies and employs an IT manager responsible for policy compliance. The organization's management sent an email to approximately 500 of its clerical and administrative staff to request their participation by filling out the web-based instrument anonymously. The instrument was physically located at a university to further ensure that respondents could count on the privacy of their response. Furthermore, the employees were told that the main purpose of the survey was academic research, and that independent university scholars would analyze the results.

The survey yielded 210 survey responses—a response rate of 42 percent; 22 percent were from male and 78 were from female employees. Given the difficulties in obtaining information security-related data from companies [8], the response rate can be regarded as relatively high.

5. Analysis

We tested our model for convergent and discriminant validity, reliability, and performed tests for common methods bias; the tests are documented in Appendix B. The results showed that our model met or exceeded the accepted thresholds for rigorous IS research.

The results of our theoretical model testing are shown in Fig. 2. We analyzed our model using SmartPLS 2.0. We chose this because of its ability to evaluate the measurement and structural models simultaneously, and because of its known value in exploratory theory-building research.

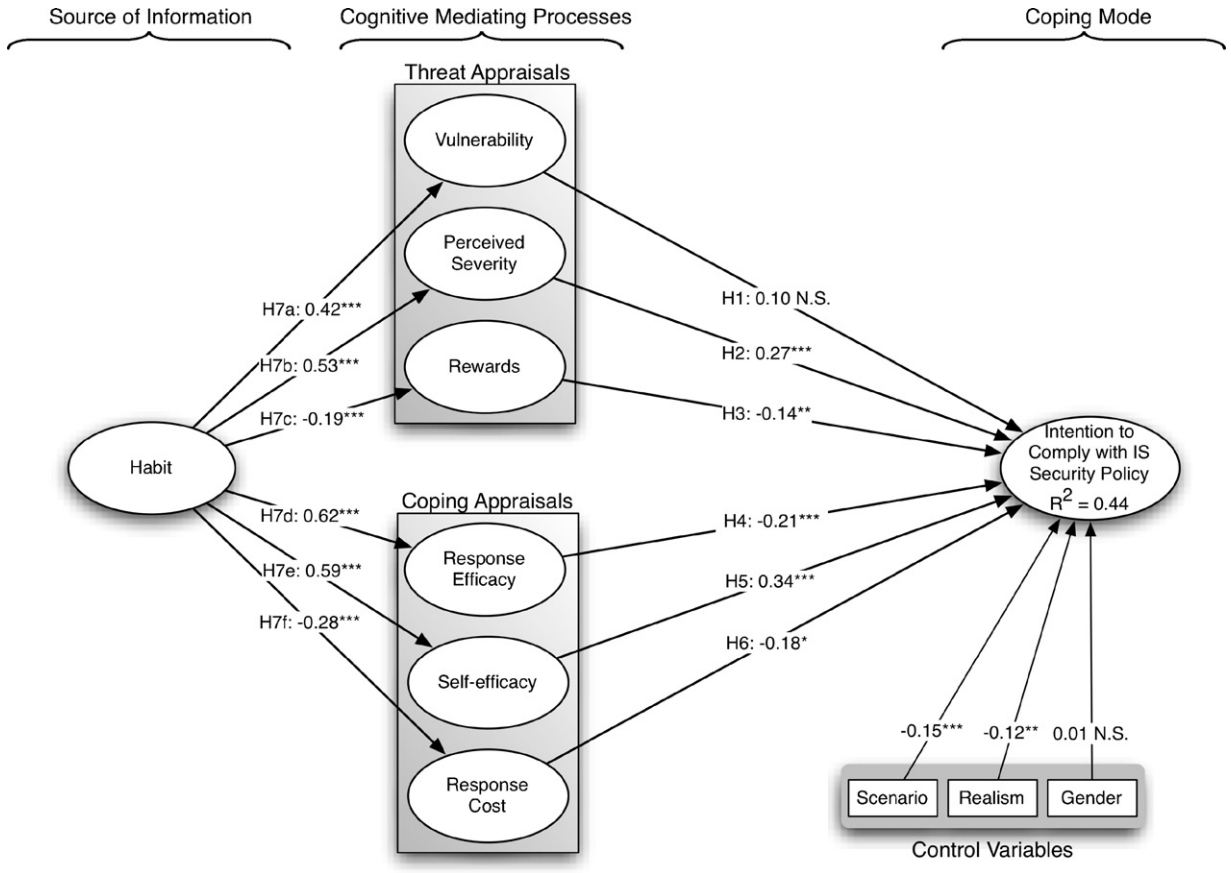

Fig. 2. Research model results. *Note*: $^{***}p < 0.01$; $^{**}p < 0.03$; $^{*}p < 0.05$.

5.1. Evaluating control variables

In testing our model, we also evaluated the effects of three control variables: gender, scenario type, and perceived realism of the scenario. We included the scenario type because we randomly assigned different scenarios to participants. A one-way ANOVA found that respondents' reported intentions to comply differed significantly depending on the type of scenario received (3.7, $p < 0.03$). Respondents were most likely to comply with the policy about not sharing the work laptop with children (mean of 9.2), followed by not reading confidential information and locking the workstation (mean of 8.2 and 8.1 respectively). Finally, respondents were least likely to comply with the policy to not share passwords (mean of 7.8).

Similarly, we found that the perceived realism of the scenario received significantly correlated with reported compliance intention ($r = -0.17$, $p < 0.05$). This indicates that the more realistic the scenario, the less likely respondents are to comply with the policy, which may imply that the more commonplace the violation or the more a respondent can identify with the situation, the less likely respondents are to comply with the policy. For this reason, we included perceived realism as a control variable.

5.2. Results of the theoretical model analysis

Contrary to expectations, *vulnerability* had an insignificant effect on *intention to comply*. Thus, H1 was not supported. In contrast, *perceived severity* positively affected *intention* (path coefficient 0.27; $p < 0.01$) and *rewards* negatively affected *intention* (-0.14; $p < 0.03$) as theorized. Therefore, hypotheses H2 and H3 were both supported.

With respect to the hypothesized coping appraisals, *response efficacy* significantly affected *intention*, albeit in the opposite direction to what we theorized (-0.21; $p < 0.01$). Thus, H4 was not supported. However, both *self-efficacy* (0.34; $p < 0.01$) and *response cost* (-0.18; $p < 0.05$) affected *intention* as expected. Therefore, H5 and H6 were supported. Finally, for the hypothesized effects of *habit* on the PMT variables, all hypotheses were strongly supported (H7a: 0.42; H7b: 0.53; H7c: -0.19; H7d: 0.62; H7e: 0.59; H7f: -0.28), and were significant at the $p < 0.01$ level.

6. Discussion

First, we found that habit towards compliance with IS security policies had a significant impact on all components of PMT. While this finding is consistent with theory, we found no empirical studies that have explored this relationships between habit and the PMT in the context of IS.

This indicated that habit has an important role in the context of employees' compliance with information security policies. Thus habit has a significant influence on whether employees feel that subjected to threat if they did not comply with IS security policies; it also had significant influence on perceived severity of the threat, if they felt that complying with IS security policies could help to minimize security breaches (response efficacy), and if they felt able to comply with the IS security procedures (self-efficacy).

Also, if a person felt that IS security procedures inconvenienced work (response costs), or found that complying with such procedures added time to complete "normal" work tasks (rewards), then the person would continue to maintain the belief.

Second, severity of the threat had a positive impact on employees' intention to comply with IS security policies. This is consistent with PMT and empirical tests of the theory. With respect to related work, Herath and Rao had previously found that response efficacy explained attitude.

Third, vulnerability had an insignificant impact on employees' intention to comply with IS security policies, implying that vulnerability does not increase one's intention to comply. While this is not consistent with PMT, it is consistent with other findings in the IS security domain. For example, although Workman et al. noted that vulnerability was significant in explaining the likelihood of employees omitting IS security precautions (measured both objectively and subjectively), the size of the path coefficients demonstrating these effects were too small to be considered meaningful. It appears that our respondents generally did not believe that they would be subjected to information security threats if they did not comply with the IS security policy.

Fourth, self-efficacy had a positive impact on employees' intention to comply with IS security policies. This is consistent with PMT. For example, in IS, Pahnila et al. noted that self-efficacy was significant in explaining omission of IS security measures.

Fifth, rewards negatively influenced employees' intention to comply with IS security policies. This was consistent with PMT (though we found no empirical studies that had explored the effect of rewards in the context of employees' IS security policy compliance within organizations).

Sixth, response cost negatively influenced employees' intention to comply with IS security policies, meaning that employees consider the inconvenience of adhering to IS security policies a legitimate reason for not complying with those policies. This is consistent with PMT. While we found no previous empirical research in this area of IS.

Seventh, response efficacy had a significant negative effect on intention to comply, which was in the opposite direction, as theorized. In addition, examination of the latent variable correlations showed that response efficacy was positively correlated with intention ($r = 0.21$; a bivariate correlation of the two constructs is also significant, $r = 0.22$, $p < 0.01$).

To investigate why response efficacy was positively correlated with intention, but negatively influenced intention, we tested whether multicollinearity could have changed the sign of the effect in the model by examining whether the variance inflation factor (VIF) scores were above the commonly accepted threshold of 10. However, all scores were less than 2.2, indicating that multicollinearity was not likely to have been present in our results.

We examined whether a suppressor effect had occurred in our model [2]. This occurs when one independent variable explains significant variance in another predictor variable; i.e., one independent variable hides or suppresses the true effect of another. We found that both perceived severity and self-efficacy acted as suppressors for response efficacy in our model. Thus, while H4 was not supported in our test of the model, considered alone, response efficacy positively affected intention (path coefficient of 0.22, $p < 0.01$), consistent with PMT.

6.1. Limitations

Our study had the typical limitations. First, the data was obtained from one organization, which may include biases unique to the sample. Therefore, care should be taken in generalizing findings to other organizations. Second, the administrative and clerical workers at the organization we sampled were predominantly female. Although our tests did not find any difference in compliance based on gender, it has been found to be an important factor in other IT contexts.

Third, our study was limited in terms of its use of intention as the dependent variable. Measures of intention are widely accepted as needed, especially in criminological research, there is also strong

evidence of a strong relationship between intention and actual behavior [15].

A fourth limitation is that we only measured compliance in the context of four scenarios. Although these were rigorously validated for content validity, it is possible that compliance results may be different for scenarios describing other situations.

6.2. Implications for practice

We found that severity of threats had a significant impact on intention to comply with IS security policies. Based on this, it is important to help employees understand that non-compliance can cause serious information security problems for their organization. Companies must organize IS security seminars or training sessions where employees are made aware of possible IS security threats and their severity and speed. In addition, supervisors should spread this message among their subordinates.

Practitioners need to change their organizational culture and working environment to encourage compliance with IS security policies to be regarded as a necessity rather than a hurdle that impedes employees from performing their job.

Obviously, IS security practices and procedures must not be cumbersome, as this will only serve to create a feeling that adherence to IS security practices takes too much time. It is also important to ensure that IS security policies are perceived to be relevant and easy to use. Thus organizations should perform usability reviews of all of their IS security techniques and practices.

With respect to vulnerability, our findings suggest that organizations need to stress that they could be subject to information security threats if employees do not take IS security seriously and comply with policies. This information could be spread through IS security seminars, training sessions, etc.; there is no room for exceptions and no excuse for non-compliance.

7. Conclusions

Employees' adherence to IS security policies is important in ensuring the information security of organizations. Prior work examining IS security policy compliance has not applied the full model of PMT. Moreover, the influence of past and automatic IS security compliance behavior on the threat appraisal and coping responses of PMT has not been fully examined in prior research. We integrate the full PMT model with the Theory of Habit. To evaluate our model, we performed an empirical study in Finland. Our results strongly support our integrated model.

A number of implications for practice were highlighted. First, practitioners need to ensure that employees recognize information security threats and the risks that these threats pose to their organization. Also, it is important to tell employees that their organization is likely to be subjected to information security threats if they do not take IS security techniques and practices seriously and comply with the policies. Second, employees should know that compliance with IS security policies is part of their work responsibility. Third, organizations need to ensure that information security practices and procedures are not difficult to use. Finally, it is important to make sure that employees comply with IS security policies.

Appendix A. Scenarios and instrumentation

Table A1

Hypothetical scenarios.

Violation	Scenario
Reading confidential documents	Jack goes to the shared office printer alone, and sees a document printed by someone else. The document is labeled as "Confidential". The information security policy prohibits reading confidential information, but Jack is curious and quickly reads through the document.
Failing to report computer virus	Gina is browsing possible questionable websites at work and the anti-virus program alerts her that a virus has been installed on her computer. Although the information security policy requires that viruses be removed by IT support staff, Gina decides to take care of the virus problem by herself.
Allowing children to play with laptop	Linda takes her work laptop to home to work. Her kids want to use the laptop for playing games. Linda is upset because her kids do not have a computer, unlike their friends. Her company's security procedures prohibit sharing work computers with anyone. Linda lends her laptop to her children and later she realizes that the kids have installed a number of programs to it. Linda does not tell to anyone about this issue.
Using unencrypted portable media	Niles is working on a position that requires access to his company's personnel details. His company's information security policy prohibits copying this data to unencrypted portable media, such as USB drives. However, Niles is going on a business trip and would like to analyze the personnel data during his trip. Niles copies the personnel data to his portable USB drive without encryption and takes it off company premises.
Locking PC	Kathy's supervisor asks Kathy to leave her PC unlocked, so that other employees are able to use it. Her company's information security policy prescribes that all users must lock their PC every time they leave their computer. Nevertheless, Kathy leaves the PC unlocked.
Sharing passwords	Heather uses a file server at work that she can access by typing in her password. The company has an information security procedure that passwords must not be shared. However, Heather is on a business trip and one of her co-workers needs a file on the file server. Heather shares her password with her co-worker.

Table A2
Measurement items.

Construct	Item	Item text	Adapted from
Habit	Habit1[a]	Complying with information security policies is something I do frequently.	[20]
	Habit10[a]	Complying with information security policies is something I have no need to think about doing.	
	Habit11[a]	Complying with information security policies is something that's typically "me."	
	Habit12[a]	Complying with information security policies is something I have been doing for a long time.	
	Habit2	Complying with information security policies is something I do automatically.	
	Habit3	Complying with information security policies is something I do without having to consciously remember to do so.	
	Habit4	Complying with information security policies is something that makes me feel weird if I do not do it.	
	Habit5[a]	Complying with information security policies is something I do without thinking.	
	Habit6[a]	Complying with information security policies is something that would require effort not to do.	
	Habit7	Complying with information security policies is something that belongs to my (daily, weekly, monthly) routine.	
	Habit8	Complying with information security policies is something I start doing before I realize I'm doing it.	
	Habit9[a]	Complying with information security policies is something I would find hard not to do.	
Intention to comply with the information security policy	Int1 (r)	What is the chance that you would do what [the scenario character] did in the described scenario?	[14]
	Int2 (r)	I would act in the same way as [the scenario character] did if I was in the same situation.	[14]
Perceived severity	PerceivedSev1	An information security breach in my organization would be a serious problem for me.	[21]
	PerceivedSev3	If I would do what [the scenario character] did, there would be serious information security problems for my organization.	
	PerceivedSev4[a]	If I would do what [the scenario character] did, serious information security problems would result.	
Perceived vulnerability	PerceivedVuln1[a]	I could be subjected to an information security threat, if I would do what [the scenario character] did.	[21]
	PerceivedVuln2	My organization could be subjected to an information security threat if I did what [the scenario character] did.	
	PerceivedVuln3	An information security problem could occur if I did what [the scenario character] did.	
Response efficacy	ResponseEff1	Complying with information security policies in our organization keep IS security breaches down.	
	ResponseEff2	If I comply with information security policies, IS security breaches are scarce.	[21]
	ResponseEff3	Careful compliance with IS security policies helps to avoid IS security problems.	[21]
Self-efficacy	Self-efficacy1	I can comply with information security policies by myself.	[b]
	Self-efficacy3	Doing the opposite of what the [scenario character] did would be difficult for me to do.	[b]
	Self-efficacy4	Doing the opposite of what the [scenario character] did would be easy for me to do.	[b]
Perceived realism	Real	How realistic do you think the above scenario is?	New
Response cost	ResponseCost4	Complying with information security policies inconveniences my work.	[21]
	ResponseCost5	There are too many overheads associated with complying with information security policies.	[21]
	ResponseCost6	Complying with information security policies would require considerable investment of effort other than time.	[21]
Rewards	Rewards1	If I would do what [the scenario character] did, I would save time.	New
	Rewards2	If I would do what [the scenario character] did, I would save work time.	New
	Rewards3	Non-compliance with the information security policies saves work time.	New

Note: All items were measured on an 11-point scale from 0 (strongly disagree) to 10 (strongly agree). (r), item reversed.

[a] Dropped to improve reliability or construct validity.

[b] S.K. Wurtele, J.E. Maddux, Relative contributions of protection motivation theory components in predicting exercise intentions and behavior, Health Psychology 6 (5) (1987) 453–466.

Appendix B. Model and instrument validation

B.1. Model validation

We used Partial Least Squares to assess the reliability and construct validity of the measurement model. In doing so, we followed the procedures outlined in Gefen and Straub [3] to test discriminant and convergent validity. To test convergent validity, we performed bootstrap with 600 resamples. We then examined the *t*-test scores for the loadings of items on their intended constructs. Convergent validity is shown when the *t*-scores are at or above 1.96. Results from this test showed that items generally significantly loaded on their intended constructs. Items that did not were dropped from the measurement model. Another bootstrap was performed, which showed that all items significantly loaded on the appropriate construct.

To test discriminant validity, two tests were performed. First, discriminant validity in the measurement model was evaluated by examining the pattern of item loadings across constructs in the model. Discriminant validity is demonstrated when items load more highly on their intended construct than on other constructs in the model. The difference between an item loading on its intended construct and its next highest loading should be at least .10. Examining Table B1, we see that nearly all items meet this criterion, with the exception of item "PerceivedSev3," which loads on the construct *vulnerability* with .80, which is .09 lower than its intended loading on *perceived severity*. However, given the close theoretical similarity between these two constructs, this single exception can be considered acceptable.

A second test evaluated discriminant validity in the structural model by comparing the square root of each construct's average variance extracted (AVE) score with the construct's correlations with other constructs in the model. The square root of the AVE should be much higher than any construct correlation. An examination of Table B2 shows that every construct easily meets this guideline. Overall, the results of both tests demonstrate excellent discriminant validity.

Finally, to test the reliability of measurement items, we calculated Cronbach's α as well as the composite reliability score, which is evaluated in the same way as Cronbach's α. Both scores are reported in Table B2. All items exhibited a reliability score over the .60 threshold accorded to exploratory research.

B.2. Tests for common method bias

Because measures for the dependent and independent variables were taken from the same instrument, we performed two tests to gauge the influence of common methods bias on our data. First, we

Table B1
Cross loadings of measurement items to latent constructs.

Construct	Item	1	2	3	4	5	6	7	8
Habit (1)	Habit2	**0.90**	−0.26	0.45	0.59	−0.29	−0.21	0.56	0.35
	Habit3	**0.73**	−0.21	0.40	0.40	−0.22	−0.20	0.44	0.28
	Habit4	**0.61**	−0.17	0.38	0.36	−0.15	−0.09	0.26	0.36
	Habit7	**0.84**	−0.22	0.44	0.58	−0.22	−0.08	0.50	0.38
	Habit8	**0.58**	−0.10	0.28	0.29	−0.09	−0.13	0.35	0.16
Intention (2)	Int1	−0.28	**0.96**	−0.43	−0.22	0.38	0.40	−0.45	−0.38
	Int2	−0.24	**0.96**	−0.43	−0.19	0.27	0.40	−0.46	−0.33
Perceived severity (3)	PerceivedSev1	0.48	−0.24	**0.82**	0.44	−0.14	−0.11	0.31	0.34
	PerceivedSev3	0.44	−0.50	**0.89**	0.49	−0.13	−0.23	0.46	0.80
Response efficacy (4)	ResponseEff1	0.51	−0.19	0.42	**0.83**	−0.28	−0.26	0.49	0.39
	ResponseEff2	0.46	−0.19	0.49	**0.79**	−0.12	−0.13	0.39	0.34
	ResponseEff3	0.56	−0.15	0.44	**0.86**	−0.25	−0.10	0.44	0.43
Response cost (5)	ResponseCost4	−0.21	0.27	−0.13	−0.18	**0.79**	0.33	−0.21	−0.08
	ResponseCost5	−0.25	0.29	−0.06	−0.21	**0.83**	0.37	−0.15	−0.05
	ResponseCost6	−0.15	0.20	−0.18	−0.22	**0.64**	0.36	−0.19	−0.16
Rewards (6)	Reward1	−0.17	0.29	−0.08	−0.15	0.44	**0.78**	−0.20	−0.11
	Reward2	−0.09	0.44	−0.23	−0.16	0.33	**0.89**	−0.29	−0.18
	Reward3	−0.23	0.29	−0.18	−0.17	0.40	**0.82**	−0.25	−0.17
Self-efficacy (7)	Self-Efficacy1	0.54	−0.22	0.28	0.46	−0.17	−0.25	**0.72**	0.25
	Self-Efficacy3	0.28	−0.37	0.31	0.30	−0.13	−0.19	**0.74**	0.25
	Self-Efficacy4	0.51	−0.48	0.46	0.46	−0.25	−0.25	**0.85**	0.34
Perceived vulnerability (8)	PerceivedVuln2	0.41	−0.35	0.72	0.43	−0.11	−0.17	0.36	**0.90**
	PerceivedVuln3	0.31	−0.28	0.45	0.37	−0.09	−0.15	0.27	**0.82**

Table B2
Construct correlations, AVE, and reliabilities.

Construct	CR	α	AVE	1	2	3	4	5	6	7	8
Habit (1)	0.86	0.79	0.55	**0.74**							
Intention (2)	0.96	0.92	0.93	0.27	**0.96**						
Perceived severity (3)	0.85	0.65	0.74	0.53	0.45	**0.86**					
Response efficacy (4)	0.86	0.77	0.68	0.62	0.21	0.54	**0.83**				
Response cost (5)	0.80	0.62	0.57	−0.28	−0.34	−0.15	−0.26	**0.76**			
Rewards (6)	0.87	0.77	0.69	−0.19	−0.42	−0.20	−0.19	0.46	**0.83**		
Self-efficacy (7)	0.82	0.67	0.60	0.58	0.47	0.46	0.54	−0.24	−0.30	**0.77**	
Vulnerability (8)	0.85	0.65	0.74	0.42	0.37	0.70	0.47	−0.12	−0.19	0.37	**0.86**

Note: CR, composite reliability; α, Cronbach's α; AVE, average variance extracted.

performed Harman's one-factor test to see whether one factor accounted for the majority of variance in the data. To do so, we entered all items used in the instrument into an unrotated exploratory factor analysis. This yielded 20 factors, the largest of which accounted for 31 percent of the variance, showing no evidence of common methods bias. As an additional test, we examined the latent variable correlations (see Table B2) to see whether any two latent constructs correlated highly (at .90 or more), another possible manifestation of common methods bias. No constructs were found to correlate so highly. Given these results, we conclude that there is little threat of common methods in our data.

References

[1] K. Bagchi, G. Udo, An analysis of the growth of computer and internet security breaches, Communications of the Association for Information Systems 12 (46), 2003, pp. 684–700.
[2] R. Cenfetelli, G. Bassellier, Interpretation of formative measurement in information systems research, MIS Quarterly 33 (4), 2009, pp. 689–708.
[3] Gefen, Straub, A practical guide to factorial validity using PLS-graph: tutorial and annotated example, Communications of the Association for Information Systems 16 (5), 2005, pp. 91–109.
[4] T. Herath, H.R. Rao, Protection motivation and deterrence: a framework for security policy compliance in organisations, European Journal of Information Systems 18 (2), 2009, pp. 106–125.
[5] A. Hovav, J. D'Arcy, Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea, Information and Management 49 (2), 2012, pp. 99–110.
[6] Jai-Yeol, Son, Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies Information and Management 48 (7), 2011, pp. 296–302.
[7] A. Johnston, M. Warkentin, Fear appeals and information security behaviors: an empirical study, MIS Quarterly 34 (3), 2010, pp. 549–566.
[8] A.G. Kotulic, J.G. Clark, Why there aren't more information security research studies, Information and Management 41 (5), 2004, pp. 597–607.
[9] S.M. Lee, S.G. Lee, S. Yoo, An integrative model of computer abuse based on social control and general deterrence theories, Information and Management 41, 2004, pp. 707–718.
[10] M. Limayem, S.G. Hirt, Force of habit and information systems usage: theory and initial validation, Journal of the AIS 4 (1), 2003, pp. 65–97.
[11] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, A. Vance, What levels of moral reasoning and values explain adherence to information security rules? An empirical study European Journal of Information Systems 18 (2), 2009, pp. 126–139.
[12] A. Ortiz de Guinea, L.M. Markus, Why break the habit of a lifetime? Rethinking the roles of intention, habit, and emotion in continuing information technology use MIS Quarterly 33 (3), 2009, pp. 433–444.
[13] S. Pahnila, M. Siponen, A. Mahmood, Employees' behavior towards IS security policy compliance, 40th Annual Hawaii International Conference on Systems Sciences, 2007.
[14] N.L. Piquero, A.R. Piquero, Control balance and exploitative corporate crime, Criminology 44 (2), 2006, pp. 397–430.
[15] G. Pogarsky, Projected offending and implications for heterotypic continuity, Criminology 42 (1), 2004, pp. 111–135.
[16] P. Puhakainen, M. Siponen, Improving employees' compliance through information systems security training: an action research study, MIS Quarterly 34 (4), 2010, pp. 757–778.
[17] M. Siponen, A. Vance, Neutralization: new insights into the problem of employee information systems security policy violations, MIS Quarterly 34 (3), 2010, pp. 487–502.
[18] M. Siponen, R. Willison, Information security management standards: problems and solutions, Information and Management 46 (5), 2009, pp. 267–270.
[19] J. Stanton, K. Stam, P. Mastrangelo, J. Jolton, Analysis of end user security behaviors, Computers and Security 24 (2), 2005, pp. 124–133.
[20] Verplanken, Orbell, Reflections on past behavior: a self-report index of habit strength, Journal of Applied Social Psychology 33 (6), 2003, pp. 1313–1330.
[21] I. Woon, G. Tan, R. Low, A protection motivation theory approach to home wireless security, International Conference on Information Systems (ICIS) 2005, pp. 367–380.
[22] M. Workman, W. Bommer, D. Straub, Security lapses and the omission of information security measures: a threat control model and empirical test, Computers in Human Behavior 24 (6), 2008, pp. 2799–2816.

Anthony Vance is as Assistant Professor of Information Systems in the Marriott School of Management of Brigham Young University. He has earned Ph.D. degrees in Information Systems from Georgia State University, USA; the University of Paris—Dauphine, France; and the University of Oulu, Finland. He received a BS in IS and Masters of Information Systems Management (MISM) from Brigham Young University. His previous experience includes working as a visiting research professor in the Information Systems Security Research Center at the University of Oulu, where he remains a research fellow. He also worked as an information security consultant for Deloitte. His work is published in *MIS Quarterly*, *Journal of Management Information Systems*, and *European Journal of Information Systems*.

Mikko Siponen is a Full Professor and Director of the IS Security Research Center in the Department of Information Processing Science at the University of Oulu, Finland. He holds a Ph.D. in Philosophy from the University of Joensuu, Finland, and a Ph.D. in Information Systems from the University of Oulu, Finland. He has 40 published papers in journals such as *MIS Quarterly*, *Information & Management*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Information & Organization*, and *Information Systems Journal*. He has received over 5.4 million USD of research funding from corporations and numerous funding bodies. He has served as a senior editor three times for ICIS and ECIS.

Seppo Pahnila received his Ph.D. in Information Processing Science from the University of Oulu in Finland. His research interests include information systems security, information security policy compliance, personalized information systems and E-commerce. He has published in *IEEE Computer*, *European Journal of Information Systems*, *Communications of the ACM*, *Pacific Asia Journal of the Association for Information Systems*, *Behavior & Information Technology*, and *International Journal of Bank Marketing*.