The Sufficiency of the Theory of Planned Behavior for Explaining Information Security Policy Compliance

Teodor Sommestad, Teodor.Sommestad@foi.se, Swedish Defence Research Institute (FOI), Olaus Magnus väg 42, Linköping, Sweden.

Henrik Karlzén, Henrik.Karlzen@foi.se, Swedish Defence Research Institute (FOI), Olaus Magnus väg 42, Linköping, Sweden

Jonas Hallberg, Jonas.Hallberg@foi.se, Swedish Defence Research Institute (FOI), Olaus Magnus väg 42, Linköping, Sweden

Purpose: The theory of planned behavior is an established theory that has been found to predict compliance with information security policies well. This paper challenges this assumption that the theory includes all constructs that explain information security policy compliance and investigates if anticipated regret or constructs from the protection motivation theory add explanatory power.

Design/methodology/approach: Responses from 306 respondents at a research organization was collected using a questionnaire-based survey. Extensions in terms of anticipated regret and constructs drawn from protection motivation theory are tested using through hierarchical regression analysis.

Findings: Adding anticipated regret and the threat appraisal process results in improvements of the predictions of intentions. The improvements are of sufficient magnitude to warrant adjustments of the model of theory of planned behavior when it is used in the area of information security policy compliance.

Originality/value: This study is the first test of anticipated regret as a predictor of information security policy compliance and the first to assess its influence in relation to the theory of planned behavior and protection motivation theory.

Keywords: Theory of planned behavior, Policy compliance, Information security, Protection motivation theory, Anticipated regret.

1 Introduction

Employee behavior plays an important role in the information security posture of virtually all organizations. Most organizations therefore develop and communicate information security policies (i.e., information security rules and procedures) aimed at governing and supporting employees. These policies typically describe the acceptable use of computer resources, the responsibilities regarding information security, the type of training that employees should have and the consequences of security policy violation. Because the behavior mandated in information security policies is believed to provide the appropriate information security level for a given organization, it follows that policy compliance is desirable from the organization's perspective. However, data suggest that more than half of all of information security breaches are caused by employees violating the information security policy (Gordon et al., 2004).

A prominent theory in social psychology is the theory of planned behavior (TPB) (Fishbein and Ajzen, 2010). A recent systematic review found that this theory is approximately as good at predicting intentions and behavior related to information security policy compliance as it is at predicting other behaviors (e.g., health- and consumer-related behaviors) – approximately 40 percent of the variance in intentions has been explained in survey research (Sommestad and Hallberg, 2013). However, the review also indicates that none of the 16 quantitative studies included in the meta-analysis tested the theory "by the book". Furthermore, many of the tests combined concepts drawn from the TPB with concepts drawn from other theories into new models/theories without first addressing the sufficiency of the original TPB.

This paper attempts to test the TPB according to the guidelines provided in the related literature and a test of the sufficiency assumption associated with the theory. Specifically, the assumption that the constructs and relationships included in the TPB are sufficient for explaining information security policy compliance is tested. This study tests whether significant improvements can be obtained by adding variables drawn from protection motivation theory (PMT) or a construct reflecting the regret individuals anticipate if they do not comply with information security policies. Promising results have been associated with both these extensions. According to the correlations presented by Ifinedo (2012), the explained variance increased from 0.60 to 0.70 when the variables of the PMT are included. The inclusion of anticipated regret has been found to result in an average increase in the explained variance of 0.07 when studies of diverse set of behaviors were

reviewed (Sandberg and Conner, 2008). In this paper, we test whether these extensions result in sufficient amounts of additional explained variance considering information security policy compliance behavior to motivate a change of the TPB. The tests are performed through a hierarchical regression analysis.

The structure of this paper is as follows. Section 2 presents the theoretical background and details the hypotheses tested. Section 3 describes the method used in the test. Section 4 presents the results. Section 5 discusses the results, and section 6 presents the conclusions drawn.

2 Theoretical background

In this section, the theories and constructs providing the bases for this study as well as the tested model and hypotheses are presented. The TPB is described in section 2.1. The tested extensions drawn from PMT and the concept of anticipated regret are described in sections 2.2 and 2.3, respectively. In section 2.4, the studied constructs and their relationships are presented. Section 2.5 details the hypotheses addressed in the study.

2.1 The theory of planned behavior

The TPB (Ajzen, 1991) and its predecessor, the theory of reasoned action (Fishbein, 1979), offer an established framework for predicting behavioral intentions and actual behavior. According to the theory, illustrated in Figure 1, behavior is influenced by people's *intentions* and *actual behavior control*, where *actual behavior control* moderates the effect of *intentions*. Most applications use *perceived behavior control* as a proxy because of the difficulties associated with measuring *actual behavior control*, as advocated by Ajzen (1991), one of the originators of the TPB. Additionally, the moderating role of *perceived behavior control* has been difficult to establish empirically, and many models include it side-by-side with *intentions* in a simpler additive/linear model.

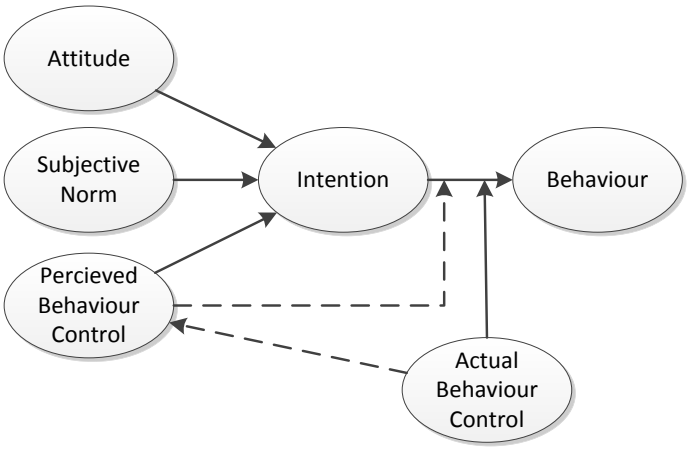

Figure 1. The theory of planned behavior (adapted from Fishbein and Ajzen (2010)).

The TPB states that *intentions* are influenced by *attitude*, *perceived norms*, and *perceived behavior control*. Their influences are assumed to be linear, i.e., the effects can be modeled using additive models. Although the theory claims that these three constructs are sufficient to explain the *intentions* concerning a behavior in question, there is no universal ordering of their importance. On the contrary, the relative importance of the constructs differs among populations and behaviors. For instance, for behaviors over which people feel they have almost full control, the variable *perceived behavior control* is of little value because it is equal for all respondents (Ajzen, 1991) .

A recent meta-analysis of security policy compliance behavior found the following sample-weighted correlation coefficients between variables: *attitude-intention* (0.48), *perceived norm-intention* (0.52), *perceived behavior control-intention* (0.45), *intention-behavior* (0.83) and *perceived behavior control-behavior* (0.35) (Sommestad and Hallberg, 2013). These coefficients for security policy compliance are higher than the coefficients reported by Armitage and Conner (2001) for other behaviors studied in relation to the TPB. Taken together, they also explain slightly more variance in intentions and behavior.

The originators of the theory are (and have been) open to including additional variables in their theoretical framework if the proposed addition is (1) behavior-specific, (2) possible to conceive as a causal factor of behavior, (3) conceptually different from existing predictors, (4) applicable to a wide range of behaviors studied by social scientists and (5) able to consistently improve prediction of intentions or behavior (Ajzen, 2011; Fishbein and Ajzen, 2010). The idea that the TPB is good as is, without any additional variable(s), is referred to as the sufficiency assumption.

2.2 Protection motivation theory

A competing theory to the TPB is protection motivation theory (PMT). PMT was first formulated as a theory of fear appeals in 1975 (Rogers, 1975) before it was extended in 1983 (Maddux and Rogers, 1983; Rogers, 1983) to a more general theory of persuasive communication. It posits that two cognitive processes determine individuals' intentions to perform a protective behavior, i.e., their protection motivation. These two processes are *threat appraisal* and *coping appraisal*.

In the *threat appraisal* process, the individual assesses how *vulnerable* he or she is (i.e., the probability that a bad thing will happen) and the *severities* of the potential incidents (i.e., the consequences/costs of the bad things that may happen). The theory states that if the *threat appraisal* results in a sense of high *vulnerability* and a sense of high *severity*, the individual will be more motivated to apply protective measures. Conversely, appraisals of low *vulnerability* and low *severity* will lead to low protection motivation. Although the psychological constructs covered by the TPB (e.g., *attitude*) can be related to how high the threat is, we argue that they are to be seen as conceptually different, as supported by empirical results in the information security domain. For instance, all correlations between the TPB variables and the PMT variables *vulnerability* and *severity* are reported to be less than 0.42 in a study by Ifinedo (2012) and less than 0.25 in a study by Herath and Rao (2009). Occasionally, a variable for intrinsic and extrinsic rewards (e.g., the "coolness" or positive social status effects of taking risks) is included in the *threat appraisal* process in PMT applications. However, its role is disputed. For example, rewards is not considered one of the main components by Norman et al. (2005) and the small number of studies including covering it forced Milne et al. (2000) to exclude it from the their meta-analysis.

The process of *coping appraisal* involves three constructs: *response efficacy*, *response cost* and *self-efficacy*. *Response efficacy* captures the individual's perception of how efficient the suggested protective behavior is at remediating the threat, i.e., whether it lowers the risks associated with the bad thing. In our view, *response efficacy* is not covered by existing constructs of the TPB. Furthermore, the TPB does not include *response costs*, i.e., the estimated costs (e.g., time and money) that arise if the coping method is employed. Previous research supports this position: all correlations reported by Ifinedo (2012) and Herath and Rao (2009) between constructs of the TPB and the PMT constructs *response cost* and *response efficacy* are below 0.50. *Self-efficacy* reflects the individual's self-assessed ability

to perform the behavior in question. In line with Fishbein and Ajzen (2010), we see this as identical to the concept of perceived behavior control and thus already considered in the TPB.

It is worth noting note that protection motivation theory considers cases in which individuals can choose whether to apply a specific protective measure. That is, there needs to be a baseline for which the individual can appraise the threat and a protective measure which the individual should use to cope. This is quite different from the framework provided by the TPB. The TPB addresses a specific behavior and does not focus on the differences between two specific alternative actions (coping or not coping). However, for information security policy compliance, the alternatives are apparent and dichotomous – the baseline is the information security threat, and the coping method is to actually follow the information security policy. Thus, both theories are appropriate for the case of policy compliance.

2.3 Anticipated regret

Anticipated regret, or anticipated affect, reflects the anticipation of "*the negative, cognitive-based emotion that it experienced when we realize that the present situation could have been better had we acted differently*" (Sandberg and Conner, 2008). In their meta-analysis of 20 studies on such behaviors as playing the lottery, having unsafe sex and speeding, Sandberg and Conner (2008) found that the inclusion of *anticipated regret* added an additional 0.07 explained variance to the variance already explained by the TPB.

Along with past behavior and self-identity, the merits of *anticipated regret* were reviewed by Fishbein and Ajzen (2010) for possible extensions to the TPB. They regard *anticipated regret* as conceptually similar to the attitude coupled to an alternative behavior and thus not in conflict with, and able to be accommodated within, their theoretical framework. They conclude that "*[t]he additional variance accounted for by anticipated affect can thus be explained as just another indication a consideration of both performance and nonperformance of a behavior leads to better prediction than a consideration of only one or the other."*

Anticipated regret has not been tested quantitatively as a predictor of information security policy compliance in any of the studies reviewed by Sommestad et al. (2014). However, it seems plausible that incompliance with security policies could be associated with regret. Regret ought to be especially relevant when the threat is perceived as probable and serious. A substantial overlap is therefore expected between the concept of *anticipated regret* and the output

of the threat appraisal process. In other words, it reasonable to expect the link between intention and the PMT constructs *vulnerability* and *severity* to be strongly related to the link between *intention* and *anticipated regret*. On the other hand, *anticipated regret* focuses on emotions, whereas the *threat appraisal* process focuses on risks associated with undesirable events.

2.4 Constructs and relationships

Figure 2 depicts the relationships between *anticipated regret*, the constructs from the PMT and the constructs from the TPB. As noted above, *self-efficacy of coping appraisal* is already included in TPB as *perceived behavior control*. In this operationalization, the rewards associated with exposure to the threat, such as the coolness of exposing computers to risks, are not included.

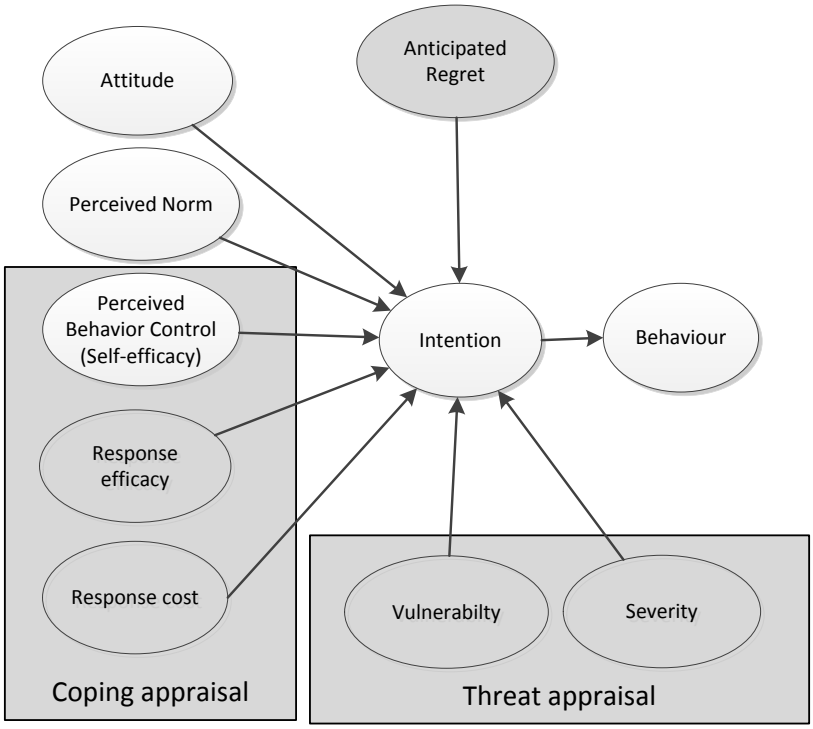

Figure 2. The theory of planned behavior and the tested extensions (grey).

2.5 Hypotheses

This paper addresses the hypotheses listed in Table 1**.** Hypothesis H1 concerns the validity of the TPB itself for information security policy compliance. This has been established in multiple previous studies (see Sommestad and Hallberg (2013)) but is necessary to establish in this study as well to ensure internal validity for the testing of the other hypotheses. Hypotheses H2 to H4 address the sufficiency assumption of TPB when used for information security policy

compliance, i.e., whether TPB can be improved by adding more variables to the model.

H2 to H3 address contributions gained from the *threat appraisal* process and the *coping appraisal* process of the PMT, respectively. The explanatory power gained by adding *anticipated regret* is tested in H4. H5 to H7 address the extent to which these three additions make independent contributions, i.e., that they do not overlap with one another. Note that hypotheses H5 to H7 are dependent on H2 to H4 and that all other hypotheses rely on H1. For instance, if H2 is false, H5 must also be false (however, the opposite is not true).

Table 1. Hypotheses tested.

The relationships stated in the theory of planned behavior	
H1	The relationships of the TPB explain security policy compliance behavior intentions and behavior.
Added efficacy from constructs of protection motivation theory	
H2	If threat appraisal, i.e., perceived vulnerability and severity of information security incidents, is added to the TPB, it explains a substantial amount of additional variance in information security policy compliance intention.
H3	If coping appraisal, i.e., response efficacy and response cost, is added to the TPB, it explains a substantial amount of additional variance in information security policy compliance intentions.
Anticipated regret	
H4	If anticipated regret is added to the TPB it explains a substantial amount of additional variance in information security policy compliance intentions.
Independence of contributions	
H5	If threat appraisal and coping appraisal are added to the TPB both of them explain a substantial amount of additional variance in information security policy compliance intentions.
H6	If threat appraisal and anticipated regret are added to the TPB both of them explain a substantial amount of additional variance in information security policy compliance intentions.
H7	If coping appraisal and anticipated are added to the TPB both of them explain a substantial amount of additional variance in information security policy compliance intentions.

The originators of TPB require that an addition to the original model should explain a "sufficient amount of additional variance" (Ajzen, 2011; Fishbein and Ajzen, 2010). There is no standard for how much "sufficient" is in this case, but some guidance is provided by one of the creators of the theory. Ajzen (1991) states that an improvement of 0.06 is "a significant contribution", while an improvement of 0.017 in explained variance is a "virtually unchanged" explanatory power. This leaves some room for interpretation. In this research, we interpret this guideline in an inclusive manner and suggest that an improvement in adjusted explained variance of at least 0.02 is sufficiently substantial improvement to warrant a change of the

TPB. The statistical guidelines for multiple linear regression in TPB studies provided by Hankins et al. (2000) were used as a basis in the tests. Unless otherwise stated, statistical significance is set to the 5% level.

3 Method

The seven hypotheses were tested by a questionnaire-based survey distributed to the employees of a research organization. Section 3.1 describes the development of the questionnaire, and section 3.2 describes the data collection procedure. Section 3.3 discusses the construct validity and the reliability of the measurement.

3.1 Measurement instrument

Through a large number of applications, tests and reviews of the TPB, a considerable amount of knowledge concerning how to best operationalize the theory in general has been accumulated. In Fishbein and Ajzen (2010) and Ajzen (2012), caveats are discussed, and descriptions of how items should be operationalized are given. The parts of this measurement instrument associated with TPB are based on the example and template for direct scales given by Fishbein and Ajzen (2010). Thus, both instrumental and experiential attitudes were measured. Items of *perceived norms* measured both injunctive norms and descriptive norms, and *perceived behavior control* covered both autonomy and capability factors. *Intentions* were measured as outright intention predictions of future behavior. *Behavior* was measured as self-assessed current behavior. Three to four items were used for each TPB construct.

The variables from PMT were operationalized in a conventional manner, as Norman et al. (2005) suggest. Six items were used to operationalize *threat appraisal*, three for *vulnerability* and three for *severity*. These items were formulated to reflect the general threat of information security incidents and were not tied to information security policy compliance. *Response efficacy* was operationalized with three items concerning the impact of following information security policies on the vulnerability of the organization and the probability of severe incidents. *Response cost* was operationalized by asking respondents whether information security policies had a negative impact on privacy, efficiency, quality or the support that can be gained from information technology.

In line with the definitions of (Fishbein and Ajzen, 2010; Sandberg and Conner, 2008), items related to *anticipated regret* asked the respondents how they would feel after not complying with the policy. Three items were used, asking about the probability that the

respondents would regret violating the policy, feel worried after not following it and dwell on it afterwards.

In addition to the items discussed above, the questionnaire included an introductory section describing the purpose of the survey, a section explaining the question format, questions about the respondent's role within the organization and questions not directly related to the hypotheses tested in this research.

Before questions were formulated, a questionnaire with open-ended questions was distributed to 12 persons with different roles in the target population to survey general beliefs related to the studied constructs. The answers were used as input in the formulation of the questionnaire items, e.g., to form bipolar scales for the attitude items. The layout and understandability were reviewed iteratively by six employees within the surveyed organization before a final version was established. All questions in the questionnaire were formulated in Swedish and, except for the demographic questions at the beginning, all questions were associated with the behavior of complying with the information security policy and rules within the specific organization surveyed. These items were answered using a seven-point semantic differential scale. Their mean value is used to form the construct of interest.

A translated version of the items included in the final version is provided in the appendix.

3.2 Data collection

This study employed a between-subject design and surveyed perceptions of employees of the Swedish Defence Research Agency (FOI). The organization is distributed over four sites and has approximately 1000 employees, with a median age of 45 years and a relatively even age distribution. Approximately 35 percent hold a PhD. Approximately 800 work as researchers and 200 as managers or with internal services (e.g., IT or facilities).

The internal mail service distributed one printed copy of the survey to each employee during September 2013. A reminder was distributed electronically one week later. Surveys received within the first three months after the distribution were included in the analysis. A total of 311 questionnaires were returned within this time period. Of these, 306 contained the responses necessary for the analysis. Visual inspection of QQ-plots and histograms suggests that all constructs are approximately normally distributed except attitude, response efficacy and current behavior, which suffer from

ceiling effects (with many respondents answering maximum). The results of ANOVA (which is robust to deviations from the normality assumption (Schmider et al., 2010)) show that no mean differences of statistical significance ($p<0.05$) could be found between respondents returning the survey in different months for the 11 constructs. Thus, the survey does not appear to suffer from problems due to non-response bias. Furthermore, the number of respondents from different departments, sites and roles match the overall distribution in the organization, suggesting that the respondents are representative of the organization.

3.3 Construct validity and reliability

Only five respondents used the feedback section to report difficulties in answering the questions in the questionnaire. Three of these reports concerned difficulties in answering when the abstraction level is overall policy compliance rather than specific behavior (e.g., passwords on USB sticks). Two complained about the language and understandability of the questions.

Both the proposed addition of anticipated regret and the constructs of TPB and PMT are well established. Because this survey does not posit new constructs and builds on previous work on how questions should be formulated, the construct validity of the present survey is to some extent already given. However, Table 2 provides further support for the presence of convergent and discriminant validity for their operationalizations. The discriminant validity is usually considered acceptable in confirmatory factor analysis when the average variance extracted (AVE) is higher than all of the cross-correlations (Gefen et al., 2000). This is the case for all constructs when principal component analysis is used. A commonly used threshold to establish convergent validity is that most of the item loads to their constructs are above the threshold of 0.6 (Chin, 1998). As seen in the appendix, this is the case for all but three items (associated with *intention*, *vulnerability* and *response cost*, with loadings of 0.57, 0.56 and 0.57, respectively). We chose to retain these items to maintain content validity.

Table 2. Reliability (α) and average variance extracted (AVE) of constructs and the correlations between them.

	α	AVE	Current behavior	Intention	Attitude	Perceived Norm	Perceived Behavior Control	Anticipated Regret	Vulnerability	Severity	Response Efficacy
Current behavior	0.82	0.74									
Intention	0.76	0.68	0.64								
Attitude	0.87	0.85	0.47	0.52							
Perceived Norm	0.79	0.79	0.44	0.41	0.36						
Perceived Behavior Control	0.63	0.59	0.52	0.47	0.48	0.44					
Anticipated Regret	0.81	0.82	0.46	0.53	0.45	0.31	0.40				
Vulnerability	0.61	0.58	0.17	0.13	0.29	0.13	0.18	0.18			
Severity	0.70	0.65	0.31	0.40	0.37	0.18	0.35	0.43	0.38		
Response Efficacy	0.84	0.80	0.35	0.35	0.51	0.37	0.50	0.32	0.26	0.30	
Response Cost	0.81	0.63	-0.34	-0.36	-0.35	-0.32	-0.32	-0.18	-0.08	-0.19	-0.29

The reliability, i.e., accuracy, of psychological measurements can be measured using Cronbach's alpha (Cronbach and Shavelson, 2004). The reliability of all but two constructs (*perceived behavior control* and *vulnerability*) exceeded 0.70, a commonly used threshold (Peterson, 2014). The reliability values for *perceived behavior control* (α=0.63) and *vulnerability* (α=0.61) are on the border of unacceptable, meaning that the answers to the three items used to measure these constructs are somewhat inconsistent. Without speculating too much about why the consistency is low for these constructs, we suggest that it might be because they are both operationalized in two dimensions: *perceived behavior control* is designed to capture both autonomy and capacity, and *vulnerability* is designed to capture both the probability an incident takes place and the probability that it leads to losses. This is further discussed in section 5.1.

4 Results

This section address the hypotheses posed in section 2.5. Section 4.1 address the overall model of TPB, section 4.2 address extensions drawn from PMT, section 4.3 address *anticipated regret* as an extension, and section 4.4 address the independence (or overlap) of the contributions.

4.1 Relationships stated in the theory of planned behavior

All relationships in the TPB have significant correlations ($p<0.01$), with correlation coefficients in the range of 0.41 to 0.64. Analysis of partial correlations shows that *attitude* (0.35), *perceived norm* (0.22) and *perceived behavior control* (0.21) have significant ($p<0.001$) correlations with *intention* when the other variables are controlled. Significant partial correlations ($p<0.001$) are also present between *current behavior* and *intentions* (0.56) and *perceived behavior control* (0.26). In a linear regression model, TPB explains 0.36 of the adjusted variance in intention and 0.44 of the adjusted variance in current behavior.

All relationships described by TPB are confirmed, and the model explains a respectable portion of variance in the predicted variables. Thus, H1 can be accepted for this sample and this operationalization of the TPB.

4.2 Added efficacy from constructs of the protection motivation theory

Both H2 and H3 concern the extra explanatory power gained if concepts of PMT are added to TPB.

H2 states that individuals' *threat appraisal* (i.e., perceived *vulnerability* and *severity*) will add explanatory ability. A linear model that includes *threat appraisal* explains 0.40 of the adjusted variance explained in intentions, an additional explained variance of 0.04.

H3 states that more variance in intentions is explained if individuals' *coping appraisal* is included. In addition to *perceived behavior control*, which is included in TPB, *coping appraisal* includes the variables *response efficacy* and *response cost*. The adjusted variance explained including these two factors is 0.37, i.e., a meager improvement of 0.01 additional explained variance. Only *response cost* has a significant contribution in the regression model ($p<0.01$).

With our interpretation of "a substantial amount" of additional variance, H2 holds, whereas H3 can be rejected.

4.3 Added efficacy from constructs of anticipated regret

H4 address the proposal of adding *anticipated regret* to TPB to explain additional variance in intentions. When *anticipated regret* is added to the model, the adjusted variance explained increases by 0.07 to 0.43, with a statistically significant ($p<0.001$) contribution

from *anticipated regret*. Thus, *anticipated regret* provides a substantial improvement to TPB, and H4 can be accepted.

4.4 Independence of contributions

The independence of the contributions made by the different extensions can be assessed by comparing the models hierarchically. Table 3 summarizes the (adjusted) explained variance of each model. H5-H7 can be tested by comparing these models.

Table 3. Explained variance of the models. Included concepts are marked with a "●".

	Regression model							
	1	2	3	4	5	6	7	8
TPB	●	●	●	●	●	●	●	●
Threat Appraisal		●			●	●	●	
Coping Appraisal			●		●	●		●
Anticipated Regret				●		●	●	●
Explained variance	0.36	0.40	0.37	0.43	0.41	0.45	0.44	0.44

From this table it is clear that there is an overlap between the extra variance explained by *anticipated regret* and variables in the *threat appraisal process*. *Threat appraisal* adds 0.04 explained variance to the TPB (model 1 vs. model 2), and *anticipated regret* adds 0.07 explained variance to the TPB (model 1 vs. model 4); together, they add 0.08 explained variance to the TPB (model 1 vs. model 7). Thus, the extra explained variance when *threat appraisal* is added after *anticipated regret* is not sufficient to accept H6. The overlap between these two factors can also been observed when comparing simpler models with only these concepts. *Anticipated regret* and *threat appraisal* each explain 0.29 and 0.16 of the variance in intentions, respectively; in combination, they explain 0.31 of the variance in intentions.

The extra variance explained for the *coping appraisal* process is independent of the model it is added to. However, its contribution of 0.01 variance explained is insufficient to satisfy H5 and H7. In other words, although the *coping appraisal* does not explain the same variance as other additions, it fails to explain enough extra variance to be able to challenge the sufficiency assumption (as we interpret it).

In summary, using our definition of a sufficient amount of extra explained variance, H5 is rejected because the contribution from *coping appraisal* is low, H6 is rejected because the contribution from *threat appraisal* is covered by *anticipated regret*, and H7 is rejected because the contribution from *coping appraisal* is low.

5 Discussion

This section starts with a discussion of the validity of this study and the possibility of generalizing its conclusions. Thereafter, the interpretation of the results in regard to making changes to and extending the TPB is discussed.

5.1 Threats to validity

Similarly to many previous surveys on this topic, generalizations from this study should be made cautiously. The sample frame used to test the hypotheses addressed in research is well defined: a Swedish defense research organization with highly educated employees, a fairly even age distribution and approximately 1000 employees distributed over four geographical locations. This workplace definitely represents an organization in which information security is of relevance and policies are important. The response rate is also acceptable (approximately 30 percent) and comparable to previous studies in the domain. Furthermore, there is nothing controversial about the results associated with the TPB in this test – the correlation coefficients and explained variance in this test are similar to those of previous tests on information security policy compliance reviewed by Sommestad and Hallberg (2013). However, there are many potential problems associated with drawing general conclusions from these results. For instance, variables associated with the Swedish culture and with this particular organization's culture or policies may distort or skew the results obtained. Additional studies that repeat these findings in other sample frames are needed before they can be assumed to be valid for information security policy compliance in general.

Another potential issue with validity is the low reliability associated with measurements of *perceived behavior control* and *vulnerability*. As noted above, we suspect that this is related to the fact that both of these factors entail two closely related dimensions. *Perceived behavior control* includes both capacity (e.g., "I am certain that I can adhere to the security policy") and autonomy (e.g., "Whether I adhere to the security policy is entirely within my control") (Fishbein and Ajzen, 2010). *Vulnerability* includes the presence of weaknesses (e.g., "The information systems are vulnerable to attacks by outsiders") and the probability than someone will try to compromise security (e.g., "Any vulnerabilities in the information systems will be exploited by unauthorized agents"). Some support for this hypothesis can also be found in the data. The reliability is higher between items associated with the same dimensions: the two items that concern the likelihood that someone will try to compromise security have a reliability score of 0.72, and the two constructs that

concern capability have a reliability score of 0.69. These values are generally acceptable (a commonly used threshold is 0.7 (Peterson, 2014)). Poor reliability is the main issue limiting the predictive ability of the measurement. In other words, it may have reduced the explanatory power of *perceived behavior control* and *vulnerability* in these tests. It is possible that a more accurate scale would have resulted in another result for H6 (concerning the independence of *threat appraisal* and *anticipated regret*), but no other dependencies are apparent.

5.2 Extending the theory of planned behavior

The results of this analysis suggest that peoples' *anticipated regret* and *threat appraisal* are important for their behavioral intentions. Furthermore, these concepts are not entirely mediated by the existing variables of the TPB. Consequently, these concepts ought to be considered when information security policy compliance is to be explained or influenced.

As discussed above, the relationship between *anticipated regret* and attitude is somewhat hazy. In the case of information security policy compliance, anticipated regret is also conceptually similar to unsafe expectations, which the typical *threat appraisal* process ought to produce. That is, people who perceive the probability and severity of incidents as high ought to be more likely to regret not complying with policies. The overlap is also apparent in the statistics. *Anticipated regret* and *threat appraisal* explained 0.29 and 0.16 of the variance in intentions, respectively; in combination, they explained 0.31 of the variance in intentions. Individually, they added 0.07 and 0.04 to the TPB explained variance, respectively, while they added 0.08 together. Thus, a considerable proportion the variance explained by *threat appraisal* is already accounted for by *anticipated regret.*

One reasonable interpretation of this finding is that, when used for information security policy compliance, the TPB lacks a component concerning the negative emotion or risk of not being compliant. Intuitively, an extension in this direction fits the nature of information security well, where threats and risks associated with non-behavior are of relevance. It is also easy to relate this finding to a component capturing negative emotions or perceived risk as a causal factor of compliance in the sense that increased compliance can be expected if a person becomes convinced that incompliance is bad and/or will be regretted.

In the future, an extended variant of the TPB specially designed for information security compliance behavior that incorporates

negative effects of incompliance should be tested. It appears that the concept of *anticipated regret* is a suitable basis for such an extension.

5.3 Replacing parts of the theory of planned behavior

The result of this test suggests that the TPB, when used for information security policy compliance, can be improved by adding either *anticipated regret* or the variables in the *threat appraisal* process of the PMT. An alternative to extending the TPB with new constructs and relationships is to replace existing constructs with other constructs that are better suited for information security policy compliance. Deliberately or not, a number of studies have done so already by refactoring the TPB into a new theory for security behavior (cf. Sommestad and Hallberg (2013)).

Overall, there are strong exploratory tendencies in empirical studies of information security policy compliance (Sommestad et al., 2014). Many models have been proposed for information security policy compliance behavior. As of March 2012, at least 29 empirical (survey-type) studies had been published on security policy compliance. The majority of the proposed constructs have only been tested in one study, and no two studies had studied the same prediction model (theory). Consequently, there is no strong empirical support for challenging the TPB in regard to information security policy compliance. For this reason, we believe it is somewhat premature to dismiss the existing constructs of the TPB and the relationships it describes, not least because of the great number of empirical studies on other behaviors that offer support for the TPB. Nevertheless, a post-hoc analysis of this study suggests that there may be worth doing so if a prediction is to be made with as few variables as possible. *Anticipated regret* increases the adjusted explained variance in intentions (by 0.03-0.05) regardless of which TPB variable it replaces, and the prediction becomes slightly better if *threat appraisal* replaces *perceived norms* (0.02) or *perceived behavior control* (0.01).

Similarly to the gains obtained by extending the TPB, this finding shows a clear potential for improvement relative to the baseline that the TPB offers for information security policy compliance: more variance may be explained using the same number of constructs. However, at least two arguments can be made against this route. First, the TPB is a fairly solid theoretical framework, and a change in the existing theory should be supported not only statistically but also by a clear explanation of why the change makes sense for information security policy compliance behavior. Second, a new

variable that explains all of the variance of an existing variable and more would also add extra explanatory power if it was added as an additional variable (as in this study) and thus be recognized in such tests. It also appears highly unlikely that a new variable explaining the same variance in the population as an existing variable would be conceptually distinct from the existing variable it replaces. Thus, it is probably best viewed as an extension or reinterpretation of that concept.

6 Conclusion

This study confirmed the relationships described by the TPB when used for information security policy compliance in a new sampling frame. Three promising extensions to the TPB were tested empirically. Two of these extensions resulted in a sufficient amount (>0.02) of additional explained variance in intentions to motivate a change of the TPB: *anticipated regret* and *threat appraisal*. There is a considerable overlap between these two concepts, and the inclusion of *anticipated regret* makes the contribution of *threat appraisal* insufficient. *Coping appraisal* offered only a small improvement in the predicted variance and failed to improve the TPB based on the criteria used in this test.

7 References

Ajzen, I., 1991. The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50, 179–211.

Ajzen, I., 2011. The theory of planned behaviour: reactions and reflections. Psychol. Health 26, 1113–27.

Ajzen, I., 2012. Theory of Planned Behavior [WWW Document]. URL http://people.umass.edu/aizen/tpb.html (accessed 8.19.13).

Armitage, C.J., Conner, M., 2001. Efficacy of the Theory of Planned Behaviour: a meta-analytic review. Br. J. Soc. Psychol. 40, 471–99.

Chin, W., 1998. Commentary: Issues and opinion on structural equation modeling. MIS Q. 22.

Cronbach, L.J., Shavelson, R.J., 2004. My Current Thoughts on Coefficient Alpha and Successor Procedures. Educ. Psychol. Meas. 64, 391–418.

Fishbein, M., 1979. A theory of reasoned action: Some applications and implications.

Fishbein, M., Ajzen, I., 2010. Predicting and Changing Behavior: The Reasoned Action Approach. Psychology Press, New York, NY, USA.

Gefen, D., Straub, D., Boudreau, M., 2000. Structural equation modeling and regression: Guidelines for research practice. Commun. Assoc. Inf. Syst. 4.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., Richardson, R., 2004. COMPUTER CRIME 2004 CSI / FBI Computer Crime and Security Survey. Computer (Long. Beach. Calif).

Hankins, M., French, D., Horne, R., 2000. Statistical guidelines for studies of the theory of reasoned action and the theory of planned behaviour. Psychol. Health 15, 151–161.

Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: A framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18, 106–125.

Ifinedo, P., 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. In: Computers and Security. Langford Lane, Kidlington, Oxford, OX5 1GB, United Kingdom, pp. 83–95.

Maddux, J.E., Rogers, R.W., 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. J. Exp. Soc. Psychol. 19, 469–479.

Milne, S., Sheeran, P., Orbell, S., 2000. Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. J. Appl. Soc. Psychol. 30, 106–143.

Norman, P., Boer, H., Seydel, E.R., 2005. Protection motivation theory. In: Conner, M., Norman, P. (Eds.), Predicting Health Behaviour: Research and Practice with Social Cognition Models. Open University Press, pp. 81–126.

Peterson, R.A., 2014. Meta-analysis of Alpha Cronbach's Coefficient. J. Consum. Res. 21, 381–391.

Rogers, R.W., 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change. J. Psychol. 91, 93–114.

Rogers, R.W., 1983. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In: Cacioppo, J., Petty, R. (Eds.), Social Psychophysiology. Guilford Press, New York, New York, USA.

Sandberg, T., Conner, M., 2008. Anticipated regret as an additional predictor in the theory of planned behaviour: a meta-analysis. Br. J. Soc. Psychol. 47, 589–606.

Schmider, E., Ziegler, M., Danay, E., Beyer, L., Bühner, M., 2010. Is It Really Robust? Reinvestigating the Robustness of ANOVA Against Violations of the Normal Distribution Assumption. Methodol. Eur. J. Res. Methods Behav. Soc. Sci. 6, 147–151.

Sommestad, T., Hallberg, J., 2013. A review of the theory of planned behaviour in the context of information security policy compliance. In: Janczewski, E., Wolf, H., Shenoi, S. (Eds.), International Information Security and Privacy Conference. Springer Berlin / Heidelberg, Auckland.

Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J., 2014. Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf. Manag. Comput. Secur. 22, 42–75.