


The Theory of Planned Behavior and Information Security Policy Compliance

Teodor Sommestad, Henrik Karlzén & Jonas Hallberg


To cite this article: Teodor Sommestad, Henrik Karlzén & Jonas Hallberg (2019) The Theory of Planned Behavior and Information Security Policy Compliance, Journal of Computer Information Systems, 59:4, 344-353, DOI: [10.1080/08874417.2017.1368421](https://doi.org/10.1080/08874417.2017.1368421)

To link to this article: <https://doi.org/10.1080/08874417.2017.1368421>

 View supplementary material 



 Published online: 18 Sep 2017.

 Submit your article to this journal 

 Article views: 257

 View related articles 

 View Crossmark data 

 Citing articles: 2 View citing articles 



The Theory of Planned Behavior and Information Security Policy Compliance

Teodor Sommestad, Henrik Karlzén, and Jonas Hallberg

Swedish Defence Research Agency, Linköping, Sweden

ABSTRACT

Much of the research on security policy compliance has tested the relationships posited by the *theory of planned behavior*. This theory explains far from all of the measurable variance in policy compliance intentions. However, it is associated with something called the sufficiency assumption, which essentially states that no variable is missing from the theory. This paper addresses this assumption in the context of information security policy compliance. A meta-analysis of published tests on information security behavior and a review of the literature in related fields are used to identify variables that have the potential to improve the theory's predictions. These results are tested using a random sample of 645 white-collar workers. The results suggest that the variables anticipated regret and habit improve the predictions. The variables increase the explained variance by 3.4 and 2.6 percentage points, respectively, when they are added individually, and by 5.4 percentage points when both are added.

KEYWORDS

Computer misuse; information security; policy compliance; policy violation; security policy; theory of planned behavior

Introduction

In information-intensive organizations, employees take actions that affect the organization's information security. For example, the information security is influenced by how employees treat their email, web browsers, and USB sticks, as well as the underlying information in, e.g., medical records, industrial intellectual properties, economic forecasts, or control system readings.

A common practice that aims to lower the information security risk is to establish an information security policy. Assuming an adequate information security policy is in place, it follows that compliance with the policy is desirable, even if not all employees do comply.

A large number of studies have been performed on this subject, and a large number of variables have been proposed as antecedents of security policy compliance or security policy compliance intention. The observed regression weights and correlation coefficients have been summarized in a number of reviews.^{1–5} However, there is no overall agreement on the best theoretical framework for security policy compliance behavior, e.g., with some researchers using protection motivation theory and others deterrence theory⁵ or the *theory of planned behavior* (TPB).^{2–4} The meta-analyses in refs. 2 and 3 both found that the most popular theory used to find antecedents of information security policy compliance was the TPB, which is one of the most well-established theories in the behavioral sciences.⁶ The theory's originators have postulated the so-called “sufficiency assumption”, i.e., that its predictions cannot be improved by adding more variables. Even though one third of the variance in intention cannot be explained by the theory's predictor variables, this assumption has not yet been refuted.

This paper addresses the sufficiency assumption in the context of information security policy compliance behavior. It is

tested whether there are variables that improve the predictions of security policy compliance behavior when they are added to a prediction model after the variables of the TPB. The added explanatory powers of 11 variables are tested in a random sample of 645 Swedish white-collar workers, which is the largest random sample that has ever been used in a survey that explicitly tests the TPB in the context of security policy compliance.

The remainder of this paper is outlined as follows. First, the TPB is described, along with previous research related to the TPB and security behavior. Second, the data collection and analysis methods are presented. Third, the results are presented. Fourth, the implications of these results are discussed. Last, the paper is concluded.

The theory of planned behavior and information security compliance behavior

The sections below describe the variables and relationships of the theory of planned behavior (TPB), potentially missing variables (i.e., the sufficiency assumption), and the hypotheses that is tested in this paper. The TPB deems behavior the result of intentions and behavioral control, with intentions determined by a set of beliefs, which are grouped into attitudes, norms, and perceived behavioral control. Eighteen studies were found that quantitatively tested the TPB in relation to the intention of security compliance behavior, and the results were similar to those for more general behaviors. Some of these studies, as well as some additional studies, revealed that there is room for challenging the sufficiency assumption of the TPB; i.e., it seems that further variables could improve the explained variance of the TPB. One hypothesis is formulated for each of the 11 variables found that shows promise in such an extension of the TPB.

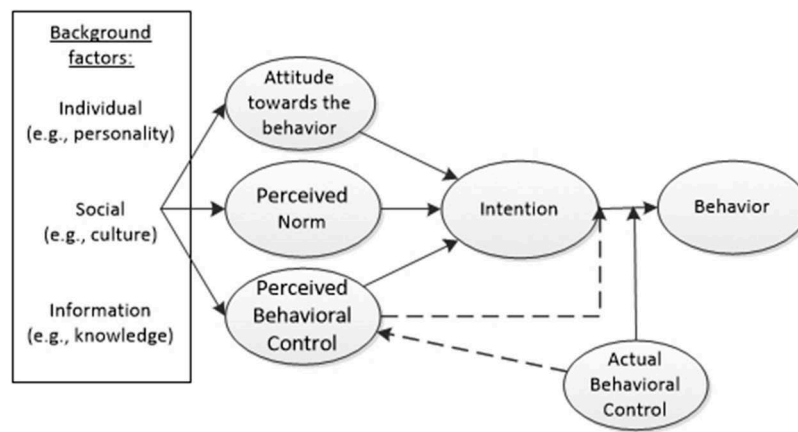


Figure 1. Variable relationships according to theory of planned behavior.

Variables and relationships

The variables and relationships of the TPB are outlined in Figure 1. According to the theory, behavior is determined by intentions (INT) to perform the behavior and by actual behavioral control. The behavioral control moderates the effect of intentions on behavior. Thus, given that a person can control his or her behavior, the person's intention will determine his or her behavior. Although actual behavioral control is what really moderates the effect of intentions, most applications use perceived behavioral control (PBC) as a proxy because of the difficulties associated with measuring actual behavioral control. The use of PBC as a proxy is advocated in ref. 7.

According to the theory, intention (INT, e.g., "I will stop smoking") is determined by attitudes toward the behavior (ATT, e.g., "smoking is problematic"), perceived norms (PNO, e.g., "most people such as me do not smoke"), and perceived behavioral control (PBC, e.g., "I am sure I can quit"). These three constructs are the results of beliefs and the strength of these beliefs. Attitudes are determined by behavioral beliefs, norms are determined by normative beliefs, and perceived behavioral control is determined by control beliefs. The theory describes how the assessments of the underlying beliefs should be aggregated into attitudes, norms, and perceived behavioral control. However, in studies concerned with predicting intentions and behaviors (and not with explaining the underlying reasons), the three constructs are often assessed directly, together with intentions and behavior.

The TPB has been subjected to a number of quantitative tests related to security compliance behavior, especially concerning behavioral intentions. By utilizing the search procedure of ref. 2, we found eighteen studies that tested variable relationships concerning INT posited by the TPB in relatively clear manners. The correlation coefficients (r) reported in these studies and the adjusted variances (\bar{R}^2) that the TPB variables collectively explain are listed in Table 1, together with sample-weighted mean correlations and their 95% confidence intervals, which were calculated with Medcalc. It is clear that the studies' results vary quite a bit. Although the confidence intervals are not that large, there are many studies whose results fall outside the intervals; in the most extreme case, when measuring ATT, 10 of the 15 studies fall outside the interval. For PNO, there is even a negative relationship to INT in one study. Although care

was taken to ensure that the scales and methods were comparable among the studies, it is unavoidable that studies have some particularities in the form of measurement error, e.g., slight differences in questionnaire item wording or cultural differences between populations. This is attenuated by larger samples, in both single studies and meta-analyses.²

The explanatory powers of the effect sizes in Table 1 may be compared with how well the TPB explains other types of behaviors (e.g., exercise and consumer behavior). The 95% confidence interval for variance explained by INT (0.34–0.48) covers the explained variances that were reported in meta-analyses of more general behaviors.^{27–29}

The sufficiency assumption

Through the large number of applications, tests, and reviews of the TPB, a considerable amount of knowledge has been accumulated. Refs. 6 and 30 discuss many of the proposals that have been made concerning missing variables in the TPB. In these discussions, they present the "sufficiency assumption", i.e., the assumption that no variables are missing. However, the originators of the theory are (and have been) open to including an additional variable if the proposed variable is (1) behavior-specific, (2) possible to conceive as a causal factor of behavior, (3) conceptually different from the existing predictors, (4) applicable to a wide range of behaviors studied by social scientists, and (5) able to explain a sufficient amount of additional variance.^{6,30} The originators also concede that criterion (5) is more important than the rest, e.g., the extension of the norm variable to include not only injunctive norms but also descriptive ones,²⁸ despite failing to meet all sufficiency criteria. Furthermore, in the present research, we are open to relaxing criterion (4) in favor of an extension or adaptation that is especially suitable and meaningful for information security policy compliance-related behaviors.

Eleven previous quantitative studies on information security policy compliance have, explicitly or implicitly, tested criterion (5) of the sufficiency assumption for the security-specific variant of the TPB by adding variables to the TPB. In such studies, the explanatory power that is added by the other variables can be inferred from the cross-correlations between all the predictors of

Table 1. Correlation coefficients and explained variance in studies involving TPB variables.

Reference	Antecedents of intention (INT)			\bar{R}^2	N
	ATT	PNO	PBC		
Refs. 8–9	0.29	0.82	0.54	0.70	106
Ref. 10	0.52	0.41	0.47	0.35	306
Ref. 11	0.61	0.58	0.31	0.49	669
Ref. 12	0.37	0.37	0.29	0.21	205
Ref. 13	0.52	0.32	0.42	0.33	194
Ref. 14	0.69	0.50	0.32	0.59	124
Ref. 15	0.49	0.61	0.22	0.40	113
Ref. 16	0.48	0.49	0.40	0.35	464
Ref. 17	0.38	0.59	0.51	0.39	312
Ref. 18	0.36	0.21	0.49	0.25	176
Ref. 19	0.30	0.60	0.60	0.50	148
Ref. 20	0.54	0.15	0.38	0.34	205
Ref. 21	0.37	–0.04			246
Ref. 22	0.61	0.53			306
Ref. 23	0.25				462
Ref. 24			0.67		435
Ref. 25			0.47		210
Ref. 26			0.34		275
Mean (random effects)	0.46	0.46	0.44	0.41	
Low 95%	0.39	0.35	0.37	0.34	
High 95%	0.53	0.56	0.51	0.48	
Number of respondents (N)	4036	3574	3942	3022	
Number of studies (k)	15	12	14	12	

Abbreviations: intention (INT), attitude (ATT), perceived norms (PNO), perceived behavioral control (PBC), adjusted explained variance (\bar{R}^2), number of respondents (N).

the TPB, the other predictor variable, and the variable to be predicted. The results are summarized in Table 2, and the variables that add the most explanatory power will form the basis for the hypotheses of the present study.

Several variables in Table 2 show promising results while other show a negligible improvement in the explained variance. *Non-compliance detection certainty* and *punishment severity* have correlations to intention of 0.26–0.40 (refs. 21 and 44) and 0.22–0.26 (refs. 20 and 45), respectively, but they improved the explained variance in previous research by only 0 and 1 percentage points, respectively and have clear overlaps with perceived norms. They are therefore excluded from the present study. The variables *organizational commitment* and *general perceived goal orientation*

(i.e., competitiveness) did not improve the explanatory power in previous studies and are also hard to relate to specific behaviors. The lack of specificity runs contrary to the principle of compatibility in ref. 6 that in an operationalization of the theory, it should (only) be possible to associate all variables to the same action (e.g., following), target (e.g., the security policy), context (e.g., at work), and time (e.g., the next year). The same applies to *security breach concern*, which describes a general concern. Some other variables in Table 2 show neither quantitative nor qualitative promise. *Perceived rule orientation*, *security culture*, and *sanctions* are closely related to *perceived norms* and *punishment severity*. *Resource availability* is related to *perceived behavioral control*. *Rewards*, *benefit of compliance*, *cost of non-compliance*, and

Table 2. Additional variance explained in intentions (change in \bar{R}^2).

	Mean	Ref. 14	Ref. 11	Ref. 10	Ref. 15	Ref. 16	Ref. 17	Ref. 18	Ref. 12	Ref. 19	Ref. 20	Refs. 8,9
Anticipated regret	0.06			0.06								
General information security awareness ^a	0.05					0.07			0.02			
Past behavior (habit, current behavior)	0.04			0.12								–0.03
Info. sec. policy awareness	0.01					0.01						
Non-compliance detection certainty	0.01				–0.02		0.01				0.04	
Rewards	0.00		–0.01			0.01						
Cost of compliance (response cost)	0.00	–0.02		0.01		0.02	0.00					
Intrinsic cost	0.00					0.00						
Technology awareness (trends)	0.00								0.00			
Punishment severity	0.00				–0.03		–0.01				0.03	
Response efficacy	–0.01	–0.01	–0.01	–0.01		–0.01	0.01	–0.01				
Perceived goal orientation	–0.01									–0.01		
Threat severity	–0.01	–0.04	0.00	0.02			–0.01					
Threat susceptibility	–0.01	–0.02	0.00	–0.01		0.00	–0.01					
Sanctions	–0.01					–0.01						
Benefit of compliance	–0.01					–0.01						
Cost of noncompliance	–0.01					–0.01						
Intrinsic Benefit	–0.01					–0.01						
Organizational commitment	–0.01				–0.04		0.02					
Security breach concern	–0.01						–0.01					
Resource availability	–0.01						–0.01					
Perceived rule orientation	–0.02									–0.02		
Top management participation	–0.03									–0.03		
Security culture	–0.04				–0.04							

^aThe directions of the correlations in the two studies are opposite to each other.

intrinsic benefit are all similar to *cost of compliance* as well as the protection motivation theory's threat appraisal construct, which has been shown to be covered by the variable *anticipated regret*.¹⁰

Hypotheses

The present study is, like most previous research, focused on the prediction of intentions rather than behavior. The motivation for this is that intentions are easier to measure than behavior. The hypotheses tested in this study concern criterion (5) of the sufficiency assumption, i.e., explanatory power can be improved by including new variables. More specifically, for each of the 11 variables, there is a hypothesis stating that the TPB-based prediction of the intention to comply with information security policies can be improved by adding the variable. The 11 hypotheses are:

- Predictions of intention to comply with information security policies are improved if general information security awareness (GISA) is added to the prediction model of the TPB.
- Predictions of intention to comply with information security policies are improved if information security policy awareness (ISPA) is added to the prediction model of the TPB.
- Predictions of intention to comply with information security policies are improved if anticipated regret of non-compliance (AR) is added to the prediction model of the TPB.
- Predictions of intention to comply with information security policies are improved if work impediment of compliance (WI) is added to the prediction model of the TPB.
- Predictions of intention to comply with information security policies are improved if cost of compliance (CC) is added to the prediction model of the TPB.
- Predictions of intention to comply with information security policies are improved if involvement in information security work (INV) is added to the prediction model of the TPB.
- Predictions of intention to comply with information security policies are improved if the respondent's information security capability (RISC) is added to the prediction model of the TPB.
- Predictions of intention to comply with information security policies are improved if the organization's information security capability (OISC) is added to the prediction model of the TPB.
- Predictions of intention to comply with information security policies are improved if habit (HAB) is added to the prediction model of the TPB.
- Predictions of intention to comply with information security policies are improved if information security threat severity (SEV) is added to the prediction model of the TPB.
- Predictions of intention to comply with information security policies are improved if security education, training, and awareness (SETA) is added to the prediction model of the TPB.

All the variables included in the hypotheses have resulted in quantitative improvements in previous tests or are considered promising for other reasons. More detailed descriptions of them and the rationale for their inclusion are given below.

The variable *general information security awareness* has been introduced to capture the influence of the "overall knowledge and understanding" related to information security,¹⁶ such as the potential harm caused by malware. Although general information security awareness does not have a specific action and has targets other than the security policy, it may help understanding how specific policy compliance behaviors fit into a larger puzzle of advantageous behaviors. Thus, it may link a specific recommendation (e.g., to not share user accounts) to other behaviors (e.g., legal requirements on the organization) to influence compliance intentions. The variable *information security policy awareness* is similar, but stresses the importance of specific knowledge related to the information security policy.¹⁶

The variable *anticipated regret* pertains to the expectation of "negative, cognitive-based emotion".³¹ Ref. 6 considers anticipated regret (or affect) to be an attitude associated with not performing the behavior. They suggest that knowledge of views associated with not performing the behavior may improve predictions of intentions, as would knowledge of norms or behavioral control associated with not performing the behavior. However, they consider the costs associated with including these extensions to be too large to motivate an extension of the TPB. On the other hand, a meta-analysis of behaviors in areas other than information security showed a considerable increase in the explained variance (0.07) if anticipated regret was added to the TPB.³¹ The study in ref. 10 found a similar increase in the explained variance for information security policy compliance intention. Thus, anticipated regret seems promising from a quantitative perspective and may explain some of the missing explanatory power related to information security policy compliance.

Variables that measure direct negative effects from policy compliance have added measurable explanatory power in several studies (cf. Table 2). Two hypotheses are related to such variables. One hypothesis concerns *work impediment*, and addresses situations where the employees are forced to work in a certain way because of the information security policy. The other is the *cost of compliance*, which is operationalized as the costs for the employee in terms of extra work or a decreased quality of work output. The two are related: work impediment mainly measures how the employee's work situation is influenced, whereas the cost of compliance measures how the output of this work is influenced.

The variable *involvement in information security work* is included because the conceptually similar, but non-information-security-specific variable *organizational involvement* (i.e., loyalty and reinforced employee relationships) was found to be a good predictor of information security policy compliance.³³⁻³⁵

The variable *respondent's information security capability* is related to the variable *general information security awareness*, but distinguished by being about capability rather than awareness (doing vs. knowing). The respondent's information security capability is also related to *perceived behavioral*

control, but captures the capability to identify threats, which can be used to make decisions that are not covered by the policy or even go against it to improve security. For instance, a person who believes they are very capable of securing information may not care for solutions prescribed by others. The variable has not been tested in relation to the TPB variables in previous research and deserves attention in the present study. The variable *organization's information security capability* has not been tested in relation to the TPB variables in previous research, but is related to many things that may influence policy compliance. First, it is somewhat related to the variable *response efficacy*, which has been tested in many studies. Second, it is likely to have an impact on the quality of the policy itself. Ref. 37 reported a correlation between policy quality and policy compliance intention of 0.43. A person who believes that the organization is capable of handling information security may be more likely to believe in the policy and thus follow it. Another possibility is that a person who believes the organization is capable of handling information security disregards the policy, thinking that someone else already takes care of the information security.

The *habit* of performing a behavior (i.e., past behavior) is, by definition, linked to the probability of performing the behavior again. Ref. 6 argues that habit cannot be a casual factor and thereby fails to meet criterion (2) of the sufficiency assumption. However, as ref. 6 notes, an increase in the explained variance at least indicates that some casual factor is missing and that habit is a stepping stone. Previous studies also suggest that habit will add explanatory power. Ref. 25 observed a correlation between habit and information security policy compliance intention of 0.27, which is similar to the correlation of 0.28 that was obtained in the meta-analysis in ref. 38 for other types of behaviors. Ref. 39 observed an increase in explanatory power of 0.02 for the intention to switch web browsers when they added habit, and Table 2 shows an average increase in the explained variance of 0.04 for intention when habit was added. The variable clearly has potential and, as it has barely been tested, it deserves attention.

Intuitively, the more dangerous the threats are to the organization, the higher the compliance intentions will be. Consequently, the variables *threat severity* and *threat susceptibility* have been tested several times, with mixed results. This study only poses a hypothesis concerning threat severity. This is for two reasons. First, ref. 10 reports that threat severity seems conceptually separate from the existing TPB variables, which is supported by reported correlations in several studies. Second, perceived threat severity has been shown to be almost exclusively a measure of perceived information security risk among employees, with threat susceptibility being virtually superfluous.

Security education, training, and awareness (SETA) activities are common interventions in organizations, such as disseminating information on the policy and commendable behavior. Thus, there is good reason to believe that SETA activities increase employees' compliance intentions. Empirical studies also suggest that such activities have a positive effect, especially if adapted to the recipients and, for example, do not paint too dim a picture of the cost of countermeasure. Two previous studies that investigated the effect of educating or training employees observed

correlations with intention of 0.38 (ref. 41) and 0.44 (ref. 37), respectively. As Table 2 shows, no previous study has tested SETA in relation to the TPB.

Measurement instrument and data collection

This section presents the measurement instrument, data collection procedure, and quality aspects of the measurements. Each construct was covered by two to five questionnaire items, which were based on previous research or, in some cases, developed for this study. Both convergent and discriminant validity were present. A random sample of 2000 individuals was drawn from a frame of 1.5 million Swedish individuals of working age and in occupations with some information security concerns. The response rate was roughly one third, and any non-response bias was found to be mediated by the TPB predictors.

Measurement instrument

A considerable amount of general knowledge concerning how to best operationalize the TPB is available. Refs. 6 and 42 discuss caveats and describe how items should be operationalized. The parts of this measurement instrument associated with the TPB are based on the example and template for direct scales provided by ref. 6. This indicates that both instrumental and experiential *attitudes* were measured, the items of *perceived norms* measured both injunctive and descriptive norms, and *perceived behavioral control* covered both autonomy and capability factors. *Intentions* were measured as outright intention for the future behavior, willingness to perform the behavior, and behavioral expectation.

The items for the variables that were not included in the TPB were either developed for this study or, to varying degrees, based on previous research in the field and translated into the native language of the target population (Swedish). When variables tested in previous research were used, the scales were inspired by that research. For example, the items for anticipated regret were inspired by ref. 10, in which definitions similar to those of refs. 6 and 34 were used. Other scales were developed for the present study. This included involvement in information security work, respondent's information security capability, organization's information security capability, and habit. These were also inspired by the extant literature. For instance, the scale for involvement was inspired by involvement scales used in safety research. Two straightforward dichotomous items were used to measure the training, information, or education on information security that the respondent received during the last year. In addition to these items and those of the TPB, the questionnaire measured other variables related to the respondent's work situation and organization. However, these variables are not used in the present study.

The first version of the questionnaire was distributed for a pre-test to 500 randomly selected individuals in the target population. Of these, 156 (31%) responded to the questions. Tests of inter-rater reliability and construct validity led to two types of modifications. First, when sufficient reliability could be maintained, items were dropped to reduce length.

Second, the wording of some items (e.g., related to attitude) was sharpened to avoid ceiling effects and to obtain more variance in the measurement. In the final survey, two to four items were used for each TPB construct and two to five were used for the others. The survey and study aims were approved by the Swedish Central Ethical Review Board. A translated version of the questionnaire-items is available in Appendix A.

Data collection

The survey was carried out in Sweden, where the government agency Statistics Sweden maintains detailed records on the population and various associated data. The present study primarily used the “Longitudinal Integration Database for Health Insurance and Labour Market Studies” (LISA), which contain information about all individuals in Sweden and their employers.^{40,41} More specifically, this study used records of individuals, their ages, and links between individuals and occupations.

The sample frame was defined as persons between the ages 18 and 65 with occupations where information security is likely to be a concern, i.e., white-collar rather than blue-collar professions. These professions were identified using the coding system “Standard för svensk yrkesklassificering” (SSYK) (see ref. 44) and 85 out of 148 professions were suitable. The professions can be summarized as “commissioned officers of the armed forces”, “various legislators, senior officials and managers” (e.g., politicians and C-level executives), “various professionals” (e.g., physicists, nurses, and statisticians), “technicians and associate professionals” (e.g., pilots, laboratory engineers, and photographers), and “clerks” (e.g., secretaries and travel agents). Professions that were excluded were blue-collar professions, agricultural work, and elementary occupations. The sample frame consisted of roughly 1.5 million individuals (approximately 15% of Sweden’s population), and the study used a simple random sample of 2000 individuals. A separate random sample of 8987 individuals was used for other studies (not reported here), and the samples were coordinated to ensure that each individual was in at most one sample.

The survey was distributed and administered by Statistics Sweden. It was sent to respondents’ home addresses by mail in mid-January 2016. Recipients could respond by mail or through a website. Two reminders followed, which increased the return rate from 23.5% to 33.8%. After removal of returned questionnaires with incomplete responses, responses from those unaware of their organization’s information security policy, and persons who had changed work since the latest LISA records, 645 (32.3%) responses remained. This is comparable in size to those of the largest studies that were presented earlier in Table 2 and is the largest sample ever in a study that is explicitly testing the TPB in this context.

Measurement reliability, validity, and non-response bias

The TPB variables had mean values of 3.79–3.87 with standard deviations of 0.78–0.92 (on a scale of 1–5). Other variables had mean values of 2.97–4.19 with standard deviations of 0.70–1.16 for items on a scale of 1–5; mean values of 2.33–3.27 with standard deviations of 0.93–1.21 for items on a scale

of 1–6; and a mean value of 0.54 with a standard deviation of 0.74 for the item on a scale of 1–2. QQ plots suggested that the responses to the survey items were approximately normally distributed.

The internal reliability in terms of Cronbach’s Alpha was above 0.850 for all variables in the pilot survey, and above 0.699 for all variables in the final survey. Thus, the items for each variable are clearly related to one another and convergent validity is present. All variables except ISPA and GISA (which are undoubtedly somewhat conceptually related) had mean inter-item correlations that were attenuated for measurement errors below the threshold of 0.85.^{7,43} This suggests discriminant validity. Appendixes B and C describes reliability measures.

The threat of non-response bias is always a concern in survey research, and as shown in Appendix D, the respondents did not reflect the sampling frame with respect to all demographic variables. Older people tended to return more surveys than younger people, which is a pattern that Statistics Sweden recognizes for surveys in general. Respondent age had weak, positive correlations (between 0.08 and 0.15) to responses to the TPB variables and weak correlations (between –0.09 and 0.15) to responses to the others. Several other demographic variables were also somewhat unrepresentative. Overall, other differences in return rates and the underlying population ratios were unproblematic. For instance, 55% of returns were from women, this was only minimally lower than frequency of women in the sampling frame (56%); public-sector employees had a somewhat higher tendency of responding (response rate 38%) than private-sector ones (response rate 30%). Fortunately, age, as well as the other measured demographic variables, had insignificant relationships to intention when they were added to the TPB model. In other words, they were mediated by TPB predictors and posed no threat to the validity; thus, no non-response compensatory weighting was needed. Finally, very weak correlations (all –0.03) were present between the return date of the survey and measurements of the TPB variables. Thus, the willingness or ambition to return the questionnaire did not have any problematic relationship to the responses.

Results

The hypotheses concern the variables’ abilities to add predictive power on top of the TPB predictors. The data were used to test whether regression models with additional variables led to significant relationships and increased the adjusted explained variance, i.e., one regression model was constructed for each of the 11 added variables, with the TPB predictors (ATT, PNO, and PBC) included in each. The results are presented in Table 3, with the first data row showing the core TPB predictors only, i.e., without an added variable, with an adjusted explained variance of 0.433. It may be noted that PBC does not make a significant contribution (its standardized regression coefficient, β , has $p \geq 0.05$) in the core model, nor in any other model. The added variables ISPA, AR, INV, OISC, and HAB result in significant β values in each of their models, e.g., ISPA makes a statistically significant contribution ($p < 0.05$) in a model with ISPA and the TPB predictors. Each of the absolute values of β of AR and HAB is

Table 3. Coefficients and explained variance with variables added. Statistically significant predictor variables in bold.

Hypothesis	Added variable	ATT (β)	PNO (β)	PBC (β)	Added variable (β)	$\Delta\bar{R}^2$ (Adjusted)
	None	0.288	0.443	-0.006	-	0.433
1	GISA	0.286	0.434	-0.014	0.061	0.003
2	ISPA	0.281	0.423	-0.036	0.075	0.004
3	AR	0.244	0.356	0.006	-0.217	0.034
4	WI	0.289	0.446	-0.019	-0.002	-0.001
5	CC	0.288	0.444	-0.014	0.003	0.000
6	INV	0.284	0.438	-0.026	0.094	0.007
7	RISC	0.287	0.444	-0.015	0.002	-0.001
8	OISC	0.280	0.434	-0.029	0.073	0.003
9	HAB	0.216	0.369	-0.043	0.219	0.026
10	SEV	0.288	0.443	-0.016	-0.001	-0.001
11	SETA	0.284	0.440	-0.012	0.031	0.001
	AR+HAB	0.181	0.300	-0.023	-	0.054
	All significant	0.177	0.304	-0.034	-	0.058
	All above	0.166	0.302	-0.018	-	0.048

Abbreviations: Attitude (ATT), perceived norms (PNO), perceived behavioral control (PBC), general information security awareness (GISA), information security policy awareness (ISPA), anticipated regret of non-compliance (AR), work impediment of compliance (WI), cost of compliance (CC), involvement in information security work (INV), the respondent's information security capability (RISC), the organization's information security capability (OISC), habit (HAB), threat severity (SEV), security education, training, and awareness (SETA), standardized regression coefficients (β), added adjusted explained variance ($\Delta\bar{R}^2$).

larger than the β value of any of ISPA, INV, and OISC, as is the case for the added adjusted explained variance ($\Delta\bar{R}^2$). AR and HAB are approximately independent, as they each increase the explained variance by 0.034 and 0.026, respectively, and together by 0.054 (close to their sum) when both are included in the same model. Including all of ISPA, AR, INV, OISC, and HAB in one model achieves a further increase of the explained variance of only 0.004. This increase is due to INV, i.e., INV overlaps somewhat with HAB and AR, and has a very small effect on explanatory power, whereas ISPA and OISC do not add any explanatory power. It may be noted that including all 11 variables in a model actually decreases the adjusted explained variance, because the added variables do not all produce a greater increase than expected by chance, i.e., the adjustment makes sure the model is a minimal best fit.

Discussion

The following sections discuss issues related to the measurement process and aspects that have been omitted in the current study. Although there were some potential validity issues, such as discriminating between two added variables or somewhat lacking homogeneity of scope and behavior specificity, these issues did not affect the evaluation of the hypotheses. Two of the 11 tested variable extensions of the TPB showed substantial improvements: anticipated regret and habit. In both cases, the results were unusual; in particular, habit had surprising interactions with core TPB predictors. It is possible that the culture of the study's population affected the results, and this could partly explain the unusual results.

Validity issues

The present study involved sixteen variables, of which many are conceptually complex and difficult to measure in a survey. Three specific issues related to the validity of the results are discussed below.

First, discriminant validity was not present between general information security awareness (GISA) and information

security policy awareness (ISPA). This comes as no surprise, given their conceptual similarity. While both variables made predictions slightly better, the present study was not able to repeat the sizable improvements of previous studies. If both variables are added, the additional explained variance is 0.3 percent points, i.e., only a tenth of previous studies' reports. Second, the present study tested some variables that are general and not specifically related to information security policy compliance behavior, e.g., GISA. While this makes the variable itself unfit of extending the TPB, it is unproblematic in the present study, as no unspecific variable resulted in substantial improvements of the explained variance. Third, there are variables that concern somewhat different scopes. For example, the present study measures intention to comply in an all-encompassing fashion (every rule at all times), but only asks about habits related to situations (rules) that have been encountered previously. This issue is subtle and it is unlikely that it has a substantial impact. Nevertheless, future studies may wish to assess more specific behaviors, e.g., to have items for intention on the form "I intend to follow the rules concerning USB sticks during the next month" and ask explicitly about habits concerning USB sticks.

Possible extensions and adjustments of the TPB

Eleven variables were tested as extensions of the TPB. Only five of these had significant relationships to intention when they were added to the TPB model. This section will focus on the two that gave substantial improvements in the explained variance: anticipated regret of non-compliance and habit.

As noted above, an argument against some of the proposed variables is that they are conceptually covered by the current variables of the TPB and only make measurements of these more accurate. A closer look at the impact of *anticipated regret* on the regression coefficients in Table 3 suggests that it is a simplification to say that it only concerns attitudes. Anticipated regret also consumes a considerable portion of the regression coefficient of perceived norms. Thus, anticipated regret concerns at least attitudes and norms. However, even if the argument is correct and anticipated regret is just

another way of framing the existing variables, the 3.4 extra percentage points of explained variance imply that the items are important. A conservative interpretation of this is that measures related to information security policy compliance are improved by including items related to attitudes about both performing the behavior and not performing the behavior. A less conservative stance is to include it as another variable in the TPB.

With regard to the variable *habit*, the issue is more complicated. While habit resulted in a substantial improvement in explained variance of 2.6 percentage points, this is small compared to the increases in studies of other behaviors. In fact, ref. 6 estimates that studies adding habit explain, on average, 10 percentage points more variance. A possible explanation for this relatively small improvement could be the nature of office work related to information security. A meta-analysis in ref. 18 on the relationship between habit and intention indicated that context stability and the frequency of the behavior moderates the role of habit. In a stable context and for frequently performed behaviors, the increase in the explained variance is 29 percentage points; in an unstable context and for behaviors that are seldom performed, the increase in the explained variance is merely 4 percent points. Thus, the dynamic nature of information security behavior, e.g., due to regular technological advancements, may limit the impact of past behavior. Another possible explanation for the relatively small improvement is that the operationalization of habit is too simple in the present study. This study operationalized habit as past behavior, in line with the definition of ref. 46 and not as the interaction of past behavior and context stability as ref. 47 suggests, or in terms of how automatic the respondent reports the behavior to be.¹⁹ Such definitions may yield stronger results.

In summary, habit resulted in a clear improvement of explanatory power, but not as much as for many other behaviors. Given that more substantial improvements in explained variance were obtained elsewhere without any established changes to the TPB, these results do not warrant a change. Still, the relationship between habit and intention is worth investigating further. Our post hoc tests indicate that there are complex relationships between habit and the TPB variables. When an interaction term is added to a model with habit, the interactions between habit and the predictor variables have relatively strong *negative* statistically significant relationships to intention: $\beta_{\text{HAB*ATT}} = -0.479$ and $\Delta\bar{R}^2 = +0.004$; $\beta_{\text{HAB*PNO}} = -0.726$ and $\Delta\bar{R}^2 = +0.008$; $\beta_{\text{HAB*PBC}} = -0.202$ and $\Delta\bar{R}^2 = 0.000$. With all three interaction terms in the model, $\Delta\bar{R}^2$ increases by 0.007. Thus, *ceteris paribus*, people who are compliant today are less inclined to be compliant in the future if they also have positive attitudes toward compliance and perceive a strong normative pressure for compliance. This peculiar result is left for further research.

Overlooked variables and contingencies

As seen in Figure 1, the TPB does include culture as a background factor. However, the originators also state that variable weights will vary among populations, and previous research on information security policy compliance suggests that national culture does play a role that is not wholly

mediated by the TPB. In particular, studies explicitly comparing the decision models of people in the USA and South Korea have found differences in the perceptions of variables and how important they are to information security policy compliance.⁴⁵ Hofstede has measured cultural dimensions of different nations, and certain traits can be associated with the studied population (here: Sweden).⁴⁷ Some potential influences of these traits are given below.

- The studied population has a culture of low “uncertainty avoidance” and is willing to take risks, which has been found to have a correlation of 0.41 with habit in one study.¹⁶ Thus, it is possible that risk willingness makes respondents less prone to uphold the stability of habitual behavior, making our figure for the additional explained variance of habit unusually low.
- The studied population has very low “masculinity”; e.g., they focus more on consensus than others, leading to relatively high impact of anticipated regret and subjective norms. In addition, low “masculinity” in combination with a tendency for “long-term orientation” may decrease the impact of present-minded variables, such as compliance cost and work impediment. Conversely, it may increase the influence of anticipated regret, which concerns long-term effects.
- The “power distance” is low in the target population. This could have an impact on employees, making them feel like they have the possibility to change the policy if it is difficult to follow, making it unusually hard for them to excuse noncompliance with problematic rules. This may explain the weak influence of perceived behavioral control.

These potential influences should be considered when generalizing this study’s results.

Conclusions

This study distributed a questionnaire to 2000 randomly selected Swedish white-collar workers; 645 valid questionnaire responses were received. These 645 responses were used to test the sufficiency assumption associated with the TPB. Five of the 11 tested variables had significant relationships to intention when added to the TPB variables. For two of these variables, anticipated regret and habit, the added explanatory power was substantial, $\Delta\bar{R}^2 = 3.4$ percentage points and $\Delta\bar{R}^2 = 2.6$ percentage points, respectively. Habit is clearly not a direct causal antecedent of intentions, making anticipated regret the only suitable candidate for extending the TPB. Those who consider anticipated regret as distinct from the existing variables of the TPB should also consider the variable when models of information security policy compliance is addressed. Anticipated regret, which is conceptually similar to attitude and is also related to norms, added 3.4 percent points of explained variance. Habit added 2.6 percent points of explained variance, which is small compared to other contexts. This may be due to the dynamicity of information systems and information security work, which limits the impact of past behavior. It should be noted that the operationalization of habit in the present study may be slightly simplistic. Nevertheless, post hoc tests show

peculiar interactions between habit and TPB predictors, where current compliance indicates future non-compliance for employees with attitudes and norms that are conducive to compliance, yet habit can hardly be causal. Previous studies show varying results, possibly due to different cultures, e.g., this study's population has a high risk tolerance, leading to unstable situations, rather than habitual ones, while high consensus focus and long-term orientation may increase the role of anticipated regret. Finally, perceived behavioral control had a non-significant impact, perhaps due to low power distance, with employees' influence bolstering their behavioral control.

References

- [1] Sommestad T, Karlzén H, Hallberg J. A meta-analysis of studies on protection motivation theory and information security behaviour. *Int J Inf Secur Priv*. 2015;9(1):26–46. doi:10.4018/IJISP.2015010102.
- [2] Sommestad T, Hallberg J, Lundholm K, Bengtsson J. Variables influencing information security policy compliance. *Inf Manag Comput Secur*. 2014;22(1):42–75. doi:10.1108/IMCS-08-2012-0045.
- [3] Milicevic D, Goeken M. Systematic review and meta-analysis of is security policy compliance research. First steps towards evidence-based structuring of the IS security domain. In: Rainer Alt and Bogdan Franczyk, editors. International Conference on Wirtschaftsinformatik. Leipzig, Germany: 2013. p. 1067–81.
- [4] Sommestad T, Hallberg J. 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. Auckland: Springer Berlin /Heidelberg; 2013.
- [5] D'Arcy J, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *Eur J Inf Syst*. 2011;20(6):643–58. doi:10.1057/ejis.2011.23.
- [6] Fishbein M, Ajzen I. Predicting and changing behavior: the reasoned action approach. New York, NY, USA: Psychology Press; 2010.
- [7] Ajzen I. The theory of planned behavior. *Organ Behav Hum Decis Process*. 1991;50(2):179–211. doi:10.1016/0749-5978(91)90020-T.
- [8] Cox J. Information systems user security: a structured model of the knowing-doing gap. *Comput Human Behav*. 2012;28(5):1849–58. doi:10.1016/j.chb.2012.05.003.
- [9] Cox J. Organizational narcissism as a factor in information security[A structured model of the user knowing-doing gap [Dissertation]. Minneapolis (USA); Capella University; 2012.
- [10] Sommestad T, Karlzén H, Hallberg J. The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Inf Comput Secur*. 2015;23(2):200–17. doi:10.1108/ICS-04-2014-0025.
- [11] Siponen MT, Adam Mahmood M, Pahnla S. Employees' adherence to information security policies: an exploratory field study. *Inf Manag*. 2014;51(2):217–24. doi:10.1016/j.im.2013.08.006.
- [12] Al-Omari A, El-Gayar O, Deokar A. Information security policy compliance: the role of information security awareness. In: K. D. Joshi and Youngjin Yoo, editors. 18th Americas Conference on Information Systems 2012, AMCIS 2012.Vol 2. 2012. Association for Information Systems. p. 1633–40.
- [13] Jenkins JL, Durcikova A. What, I shouldn't have done that?: the influence of training and just-in-time reminders on secure behavior. In: Dorothy Leidner and Joyce Elam, editors. International conference on information systems. Milan, Italy: Association for Information Systems. 2013. p. 1–18.
- [14] Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. In: Eugene H. Spafford, editor. *Computers and Security*.Vol 31. United Kingdom: Langford Lane, Kidlington, Oxford, OX5 1GB; 2012. p. 83–95. doi:10.1016/j.cose.2011.10.007.
- [15] Dugo TM. The insider threat to organizational information security: A structural model and empirical test. Auburn (USA): Auburn University; 2007.
- [16] Bulgarcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Q Manag Inf Syst*. 2010;34 (SPEC. ISSUE 3):523–48.
- [17] Herath T, Rao HR. Protection motivation and deterrence: A framework for security policy compliance in organisations. *Eur J Inf Syst*. 2009;18(2):106–25. doi:10.1057/ejis.2009.6.
- [18] Zhang J, Reithel BJ, Li H. Impact of perceived technical protection on security behaviors. *Inf Manag Comput Secur*. 2009;17(4):330–40. doi:10.1108/09685220910993980.
- [19] Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: the critical role of top management and organizational culture*. *Decis Sci*. 2012;43(4):615–60. doi:10.1111/j.1540-5915.2012.00361.x.
- [20] Liao Q, Luo X, Gurung A, Li L. Workplace management and employee misuse: does punishment matter? *J Comput Inf Syst*. 2009;50:49–60.
- [21] Li H, Zhang J, Sarathy R. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decis Support Syst*. 2010;48(4):635–45. doi:10.1016/j.dss.2009.12.005.
- [22] Guo KH, Yuan Y, Archer NP, Connelly CE. Understanding non-malicious security violations in the workplace: a composite behavior model. *J Manag Inf Syst*. 2011;28(2):203–36. doi:10.2753/MIS0742-1222280208.
- [23] Sohrabi Safa N, Von Solms R, Furnell S. Information security policy compliance model in organizations. *Comput Secur*. 2016;56:70–82. doi:10.1016/j.cose.2015.10.006.
- [24] Johnston AC, Wech B, Jack E, Beavers M. Reigning in the remote employee: applying social learning theory to explain information security policy compliance attitudes. In: Dorothy Leidner and Joyce Elam, editors. 16th Americas Conference on Information Systems 2010, AMCIS 2010.Vol 3. Lima, Peru: Association for Information Systems. 2010. p. 2217–30.
- [25] Vance A. Motivating IS security compliance: insights from habit and protection motivation theory. In: E.H. Sibley and P.Y.K. Chau, editors. *Why do employees violate is security policies? insights from multiple theoretical perspectives*. Oulu (Finland): University of Oulu; 2010.
- [26] Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. *MIS Q Manag Inf Syst*. 2010;34 (SPEC. ISSUE 3):549–66.
- [27] Armitage CJ, Conner M. Efficacy of the theory of planned behaviour: a meta-analytic review. *Br J Soc Psychol*. 2001;40(Pt 4):471–99. doi:10.1348/014466601164939.
- [28] Ravis A, Sheeran P. Descriptive norms as an additional predictor in the theory of planned. *Curr Psychology Dev Learn Personal Socia*. 2003;22(3):218–33. doi:10.1007/s12144-003-1018-2.
- [29] McEachan RRC, Conner M, Taylor NJ, Lawton RJ. Prospective prediction of health-related behaviours with the theory of planned behaviour: a meta-analysis. *Health Psychol Rev*. 2011;5(2):97–144. doi:10.1080/17437199.2010.521684.
- [30] Ajzen I. The theory of planned behaviour: reactions and reflections. *Psychol Health*. 2011;26(9):1113–27. doi:10.1080/08870446.2011.613995.
- [31] Sandberg T, Conner M. Anticipated regret as an additional predictor in the theory of planned behaviour: A meta-analysis. *Br J Soc Psychol*. 2008;47(Pt 4):589–606. doi:10.1348/014466607X258704.
- [32] Li H, Zhang J, Sarathy R. Understanding the compliance with the internet use policy from a criminology perspective. In: Andrew B. Whinston, editor. 15th Americas Conference on Information Systems 2009, AMCIS 2009. Vol 5. 2009. San Francisco, CA: Association for Information Systems. p. 3278–85.
- [33] Goo J, Yim M-S, Kim DJ. A path way to successful management of individual intention to security compliance: A role of organizational security climate. In: Ralph H. Sprague, Jr, editor.

- Proceedings of the Annual Hawaii International Conference on System Sciences. 2013. Los Alamitos, CA: IEEE Computer Society. p. 2959–68.
- [34] Goo J, Yim M-S, Kim DJ. A path to successful management of employee security compliance: an empirical study of information security climate. *IEEE Trans Prof Commun.* 2014;57(4):286–308. doi:10.1109/TPC.2014.2374011.
- [35] Ouellette JA, Wood W. Habit and intention in everyday life: the multiple processes by which past behavior predicts future behavior. *Psychol Bull.* 1998;124(1):124–54. doi:10.1037/0033-2909.124.1.54.
- [36] Ye C, Potter RE. The role of habit in post-adoption switching of personal information technologies: an empirical investigation. *Commun Assoc Inf Syst.* 2011;28(June):585–610.
- [37] Sommestad T, Karlzén H, Nilsson P, Hallberg J. An empirical test of the perceived relationship between risk and the constituents severity and probability. *Inf Comput Secur.* 2016;24(2):194–204. doi:10.1108/ICS-01-2016-0004.
- [38] Putri FF, Hovav A. Employees' Compliance with BYOD Security Policy: insights from reactance, organizational justice, and protection motivation theory. In: Avital M, Leimeister JM, Schultze U, eds. 22st European Conference on Information Systems. Tel Aviv, Israel: Association for Information Systems. 2014. p.0–17.
- [39] Ajzen I Theory of Planned Behavior. 2012. <http://people.umass.edu/aizen/tpb.html>. Accessed August 19, 2013.
- [40] Statistics Sweden. No Title. Longitud Integr database Heal Insur labour Mark Stud (LISA by Swedish acronym). 2016. <http://www.scb.se/lisa-en>. Accessed March 29, 2016.
- [41] Gullberg Brännström S. Yrkesregistret Med Yrkesstatistik En Beskrivning Av Innehåll Och Kvalitet (AM76BR1105). Örebro: Statistics Sweden. 2011.
- [42] Campbell DT, Fiske DW. Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychol Bull.* 1959;56(2):81–105. doi:10.1037/h0046016.
- [43] Danner UN, Aarts H, Vries NK. Habit vs. intention in the prediction of future behaviour: the role of frequency, context stability and mental accessibility of past behaviour. *Br J Soc Psychol.* 2008;47(2):245–65. doi:10.1348/014466607X230876.
- [44] Hovav A, D'Arcy J. Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea. *Inf Manag.* 2012;49(2):99–110. doi:10.1016/j.im.2011.12.005.
- [45] Son J-Y. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Inf Manag.* 2011;48(7):296–302. doi:10.1016/j.im.2011.07.002.
- [46] Dinev T, Goo J, Hu Q, Nam K. User behaviour towards protective information technologies: the role of national cultural differences. *Inf Syst J.* 2009;19:391–412. doi:10.1111/j.1365-2575.2007.00289.x.
- [47] Hofstede G What about Sweden? *Cult Dimens.* 2017. <https://geert-hofstede.com/sweden.html>. Accessed April 28, 2017.