A Review of the Theory of Planned Behaviour in the Context of Information Security Policy Compliance

Teodor Sommestad and Jonas Hallberg

Swedish Defence Research Agency
Olaus Magnus väg 42, Linköping, Sweden
{Teodor.Sommestad,Jonas.Hallberg}@foi.se

Abstract. The behaviour of employees influences information security in virtually all organisations. To inform the employees regarding what constitutes desirable behaviour, an information security policy can be formulated and communicated. However, not all employees comply with the information security policy. This paper reviews and synthesises 16 studies related to the theory of planned behaviour. The objective is to investigate 1) to what extent the theory explains information security policy compliance and violation and 2) whether reasonable explanations can be found when the results of the studies diverge. It can be concluded that the theory explains information security policy compliance and violation approximately as well as it explains other behaviours. Some potential explanations can be found for why the results of the identified studies diverge. However, many of the differences in results are left unexplained.

Keywords: information security, security policy, security rule, policy compliance, policy violation, computer misuse, theory of planned behavior.

1 Introduction

In virtually all organisations, the behaviour of the employees significantly influences information security. A common practice, which is intended to lower the information security risk, is to establish an information security policy. Information security policies describe, for instance, the consequences of security policy violation, the acceptable use of computer resources, the responsibilities regarding information security, and the type of training that employees should have. As described in [1], the objective of an information security policy is "to provide management direction and support for information security". Thus, one of the central themes of an information security policy is to describe suitable and unsuitable behaviours. Assuming an adequate information security policy, it follows that compliance with the policy is desirable. Unfortunately, not all employees comply with the information security policy.

A meta-analysis of different variables' influence on information security policy compliance and violation can be found in [2]. This paper extends the results in [2] with the results from additional studies and a deeper analysis of those parts that are related to the *theory of planned behaviour* (TPB) [3]. The TPB is one of the most well

L.J. Janczewski, H.B. Wolfe, and S. Shenoi (Eds.): SEC 2013, IFIP AICT 405, pp. 257–271, 2013.

established theories in the behavioural sciences, and the relationships described in the TPB are among the most frequently tested in models of information security policy compliance and violation behaviour. Although several prediction models for information security policy compliance and violation share theory with the TPB, there have been few attempts to test the TPB on its own in the information security context. In most studies that involve variables and relationships drawn from the TPB, the tested model includes variables from several theories. For instance, the variables from the TPB are combined with the variables from protection motivation theory in the model used by Ifinedo [4].

In this paper, we try to assemble the pieces and cues from previous work related to (but not necessarily exclusively addressing) the TPB in the context of information security policy compliance and violation. Two research questions are investigated:

1. How well does the TPB explain information security policy compliance and violation?
2. When divergent results are reported, can a reasonable explanation be made?

The outline is as follows. In section 2, the TPB is briefly described. In section 3, the review method is presented. In section 4, the synthesis of the extracted results is presented and the research questions are addressed. In section 5, the reliability of the answers to the research questions and their implications for practitioners and researchers are discussed. In section 5, the results are discussed and recommendations for practitioners and future research are provided. The paper is concluded in section 6.

2 The Theory of Planned Behaviour

The TPB [3] and its predecessor, the theory of reasoned action [5], has attracted considerable attention within the behavioural research community. An indicator of its popularity is the number of citations made to the original article (i.e., [3]) for the TPB (more than 23,000 citations in Google Scholar as of January 2013). The core variables and relationships of the TPB are outlined in Figure 1.

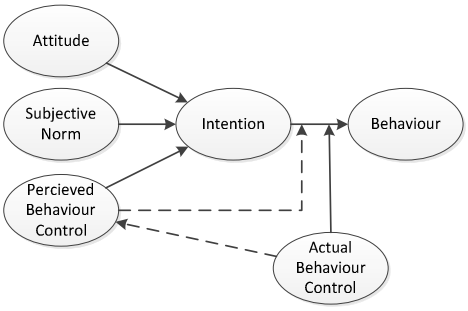

Fig. 1. The theory of planned behaviour (adapted from [6])

According to the theory, behaviour is influenced by intentions related to the behaviour and by actual behaviour control, which moderates the effect of intentions on behaviour. Although actual behaviour control is what really moderates the effect of intentions, most applications use perceived behaviour control (PBC) as a proxy because of the difficulties associated with measuring actual behaviour control. The use of PBC as a proxy is advocated by Ajzen [3], one of the originators of the TPB.

The TPB states that intentions (INT) are influenced by attitude (ATT), subjective norms (SN), and perceived behaviour control (PBC). The influences are assumed to be linear, i.e., the effects can be modelled using additive models. Whereas the theory claims that these three constructs are sufficient to explain the intentions concerning a behaviour in question, there is no universal ordering of their importance. On the contrary, the relative importance of the constructs differs among populations and behaviours. For instance, for behaviours for which there is complete volitional control, perceived behaviour control is of little value because it is equal for all respondents [3].

ATT, SN, and PBC are the results of the beliefs of the individual in question and the strength of these beliefs. ATT is determined by behavioural beliefs, SN is determined by normative beliefs, and PBC is determined by control beliefs. The theory describes how the assessments of the underlying beliefs should be aggregated into ATT, SN, and PBC. However, in studies concerning predicting intentions and behaviours (and not with explaining the underlying beliefs that form them), these three constructs are often assessed directly.

Through the large number of applications, tests, and reviews of the TPB, a considerable amount of knowledge concerning the theory in general has been accumulated. Fishbein and Ajzen [6] and Ajzen [7] discuss caveats, extensions, and competing theories and contest the relevance and implications of many of the findings. For example, Fishbein and Ajzen [6] think that the reason that *self-identity* predicts *intentions* is that the questions that measure *self-identity* are in fact questions regarding *intentions*, and Fishbein and Ajzen [6] find little difference between the constructs PBC and *self-efficacy*.

3 The Theory of Planned Behaviour and Studies Regarding Information Security Policy Compliance and Violation

As noted in the introduction, the TPB has been applied in several studies of compliance and direct incompliance with information security policies. The following steps were performed to answer the two research questions: 1) identify studies related to the TPB and information security policy compliance and violation, 2) extract data from the studies and synthesise the results, and 3) identify and test possible explanations for divergent results.

3.1 Studies Included

The aim of this review is to include all quantitative studies of security policy compliance and violation that investigate variable relationships described by the TPB. This systematic review based its search process on the search process performed (and described) in [2]. The systematic review of [2] surveyed quantitative peer-reviewed research regarding security policy compliance and violation published until early 2012. It used structured phrases in Scopus, Inspec, and Complendex, which were complemented with manual searches on the Internet and in databases and review of citations made in the identified studies. The structured search phrases yielded 461 publications, manual searches yielded 6 publications, and reviews of citations yielded 5 publications. These results were filtered by four reviewers to identify the studies that met the well-defined inclusion criteria; i.e., they should (1) explicitly study security policy compliance behaviour, (2) present quantitative results, and (3) be peer-reviewed. The four reviewers found 29 studies that satisfied these criteria [2].

Of the 29 studies included in [2], 14 studies included relationships associated with the TPB and were therefore included in this review. The authors of this paper also reiterated the search procedure performed in [2] during January 2013 to identify recent contributions related to the TPB and security policy compliance and violation. Two additional studies ([8] and [9, 10]) were found from the structured search queries. Table 1 includes information about the consequence studied (Compliance or Violation), the TPB variables included, other variables included, and the sample size (N).

3.2 Data Extraction and Synthesis of Results

Only one of the identified studies covered all the relationships described by the TPB, and only eight studies included all the antecedents of intentions. The models used in 16 studies are thus incomplete with respect to the TPB. The aim is to synthesise the results of the studies to answer the two research questions based on approximations of the overall effectiveness of the TPB. It should be noted that although the variable *descriptive norm* is currently included in SN of the TPB [6], it is treated as an external variable in our analysis to allow straightforward synthesis and comparison among the studies (only one study, [12], includes the variable descriptive norm).

Variables used as dependent and independent variables must share similar definitions and measurements scales for a synthesised result to be meaningful. The authors reviewed the measurement scales used in the different studies to assess their similarity. For the 16 studies, the scales are judged sufficiently similar to motivate a synthesis, although differences do exist. The possible influence of differences in definitions on measurement scales are addressed as part of the answer to research question 2, whether reasonable explanations for divergent results can be determined.

A common and practical effect size to use when results of multiple studies are synthesised is the Pearson correlation between variables. If correlation coefficients were missing in the papers, the authors were contacted and the coefficients or the raw data of the study were requested. Seppo Pahnila kindly provided us with additional data from [11] and explained the dependencies between the studies reported in [15] and [11]. Unfortunately, none of the other authors contacted were able to complement their results with correlation coefficients because they did not retain the data.

Table 1. Studies and the variables used in their models

Reference	Consequence	Year of publication	Antecedents of intention			Antecedents of behaviour		Other antecedents included in the model	N
			ATT	SN	PBC	INT	PBC		
[9, 10]	C	2012	●	●	●	●	●	none	106
[11]	C	2010	●	●	●	●	●	response efficacy, visibility, threat appraisal, deterrences, rewards	904 to 908
[12]	C	2009	●	●	●			descriptive norm, organisational commitment, punishment severity, punishment certainty	312
[13]	C	2010	●	●	●			None	464
[14]	V	2007	●	●	●			None	113
[15]	C	2007	●	●		●		habits, sanctions, information quality, rewards	240
[16]	C	2009	●	●	●			perceived security protection mechanism	176
[4]	C	2012	●	●	●			perceived vulnerability, perceived severity, response efficacy, response cost	124
[8]	C	2012	●	●	●			none	148
[17]	V	2011	●	●				identity match	306
[18]	C	2010	●	●				detection probability, sanction severity, security risk, perceived benefits	246
[19]	C	2010	●					none	275
[20]	C	2010			●			vulnerability, perceived severity, rewards, response efficacy, response cost	210
[21]	V	2004				●		self-defence intention	162
[22]	C	2005					●	perceptions of information security climate	104
[23]	C	2011					●	deterrent certainty, deterrent severity, legitimacy, value congruence,	602

To offer a more complete review and be able to include all results obtained, the regression coefficients were also synthesised. All studies used linear regression models to test the modelled relationships and, consequently, reported the regression coefficients. However, using simple mean values for regression coefficients is only meaningful if the regression models they come from are sufficiently similar to avoid the bias due to multicollinearity, i.e., if two correlated variables are included as predictors in a regression model, their regression coefficients will be different than if each of them were included in separate models. Many of the regression models included additional variables and relationships that are not included in the TPB, and many lacked variables of the TPB. For instance, the model used by Herath and Rao [12] includes variables drawn from deterrence theory [24] and social control theory [25]. Thus, there is an apparent risk of bias due to differences in the regression models.

The importance of differences between regression models is, however, unclear [26]. The use of mean values is considered reasonable for models with low numbers of variables and relationships, such as those included in this review [26]. Consequently, although the mean values of regression coefficients are less reliable than the mean values of the correlation coefficients, they are meaningful indicators of the strength of the relationships and serve as a complement to the correlation coefficients.

The regression coefficients and correlation coefficients were aggregated as unweighted mean values and mean values weighted by sample size. The correlation coefficients were rescaled via the Fisher transformation before the mean values were calculated. No dramatic differences existed between these aggregates (cf. Table 2, Table 3, and Table 4). We will therefore only address the unweighted means in the discussions.

A potential issue in systematic reviews is the publication bias, i.e., the general tendency to publish significant and positive results more often than insignificant or negative results. A Funnel plot was created over the studies sample size and correlation coefficients. The studies did not appear to be biased because large samples (i.e., those with small variance) are close to the average correlation coefficients and studies with small samples (i.e., those with large variance) have more varied results.

3.3 Identification of Possible Explanations for Divergent Results

There are a great number of possible reasons to expect that the included studies have attained different results. For instance, the samples are from different cultures, the measurement instruments (questions) differ among the studies, and the actual behaviours studied differ to some extent. All the applications, tests, and reviews made of the TPB provide a considerable amount of knowledge concerning the theory in general and how it performs under different conditions. To identify factors that are known to influence or bias the results when the TPB is applied, overviews and meta-analyses [3, 5–7, 27–35] of the theory were reviewed. There is additional relevant literature that postulates factors of relevance to TPB applications. However, the authors believe that the reviewed literature sufficed to identify the most established factors. How these factors were treated in the studies was assessed using the information available in the reviewed papers (e.g., concerning how the questions were formulated).

4 The Explanation Offered by the Theory of Planned Behaviour

Attempts to answer the two research questions are provided below. Section 4.1 attempts to answer the first research question, i.e., how well the theory explains information security policy compliance and violation. Section 4.2 tries to answer the second research question, i.e., whether divergent results can be explained in a reasonable manner.

4.1 How Well Does the Theory of Planned Behaviour Explain Information Security Policy Compliance and Violation?

The TPB proposes that three variables (ATN, SN, and PBC) determine intentions and that intentions and PBC determine actual behaviour. Thus, it should be possible to explain the variance in intentions and actual behaviour with these variables.

Table 2 includes the regression and correlation coefficients for the antecedents of intentions; Table 3 includes the antecedents of behaviour. The last three rows of Table 2 provide the unweighted and sample-weighted means for the regression coefficients and the correlation coefficients in addition to the combined sample size (N) for the studies that include the corresponding coefficient.

Table 2. Regression coefficients and correlation coefficients for the antecedents to intentions

Study	Regression coefficients			Correlations coefficients		
	ATT	SN	PBC	ATT	SN	PBC
[9, 10]	0.12	0.73	0.15	0.29	0.82	0.54
[11]	Unav.	0.45	0.17	0.51	0.59	0.40
[12]	0.07	0.31	0.17	0.38	0.59	0.51
[13]	0.25	0.29	0.22	0.48	0.49	0.40
[14]	0.20	0.47	0.15	0.49	0.61	0.22
[15]	0.54	0.25	-	Unav.	Unav.	-
[16]	0.18	0.02	0.43	0.36	0.21	0.49
[4]	0.48	0.19	0.17	0.69	0.50	0.32
[8]	0.20	0.37	0.36	0.30	0.60	0.60
[17]	0.67	0.22	-	0.61	0.53	-
[18]	0.34	-0.09	-	0.37	-0.04	-
[19]	0.64	-	-	Unav.	-	-
[20]	-	-	0.34	-	-	0.47
Unweighted mean	0.34	0.29	0.24	0.48	0.47	0.43
Sample-weighted mean	0.34	0.29	0.24	0.48	0.52	0.45
Number of respondents (N)	2510	2912	2570	2900	2900	2452

Table 3. Regression coefficients and correlation coefficients for the antecedents to behaviour

Study	Regression coefficients		Correlation coefficients	
	INT	PBC	INT	PBC
[9, 10]	0.35	0.22	0.47	0.40
[11]	0.40	Unav.	0.85	0.42
[21]	0.29	-	Unav.	-
[15]	0.87	-	-	Unav.
[22]	-	0.33	-	0.40
[23]	-	0.19	-	0.23
Unweighted mean	0.48	0.25	0.85	0.35
Sample-weighted mean	0.46	0.21	0.83	0.35
Number of respondents (N)	1173	812	1011	1717

Table 4. Explained variance in intentions

Study	Consequence	R^2
[9, 10]	Compliance	0.71
[12]	Compliance	0.41
[13]	Compliance	0.35
[14]	Violation	0.43
[16]	Compliance	0.26
[4]	Compliance	0.60
[8]	Compliance	0.51
Unweighted mean		0.47
Sample-weighted mean		0.42
Number of respondents (N)		1443

Eight studies measured intentions and all its antecedents according to the TPB. Table 4 presents the explained variance (coefficient of determination, R^2) for seven of these studies. The values are calculated based on the cross-correlation matrixes reported from the studies (the correlation between predictors is missing in [11]).

The ability of the TPB to explain information security policy compliance and violation is perhaps best judged by considering how well the TPB explains behaviours in general (i.e., behaviours in other fields). In the meta analysis by Armitage and Conner [29], which covered a total of 154 studies based on the TPB, the mean explained variance in intentions was 0.39. Rivis and Sheeran [33] were able to explain variance of 0.39 in data from 5,810 samples. In a recent meta-analysis of 237 prospective studies regarding health behaviours, McEachan et al. [31] found that the theory, on average, explained variance of 0.44. The explained variance in information security policy compliance and violation intentions suggests that the efficacy of the TPB is similar for information security intentions/behaviours and intentions/behaviours in general. The magnitude of the regression coefficients also supports this conclusion. The median regression coefficients reported in [36] for 30 different behaviours (ATT=0.26, SN=0.36, and PBC=0.29), the mean regression coefficients reported in [33] (ATT=0.40, SN=0.16, and PBC=0.11), and the mean regressions coefficients reported in [37] for 23 studies of condom use (ATT=0.47, SN=0.21, and PBC=0.20) are of the same magnitude as the means in Table 2.

Only Cox [9, 10] and Siponen et al. [11] included both antecedents to behaviour and cross correlations and thereby enable calculation of the explained variance in behaviour. The explained variance (R^2) in behaviour reported in [9] is 0.25, and the explained variance offered by [11] is 0.31. These results can be compared with the result of Armitage and Conner [29] and McEachan et al. [31] (R^2 of 0.27 and 0.19). The mean values of the correlations found (I=0.85 and PBC=0.35) should be compared with those found in the broader reviews of [29] (I=0.47 and PBC=0.18) and [31] (I=0.43 and PBC=0.31). Overall, the influence of both Intentions and PBC on behaviour appears to be stronger for information security policy compliance and violation than what is reported in broader reviews.

4.2 When Divergent Results Are Reported, Can a Reasonable Explanation Be Made?

The aim of this section is to answer the following question: *when divergent results are reported, can a reasonable explanation be made?* In general, one should expect

that the errors of results produced with surveys are caused by the measurement instrument (i.e., the questionnaire), the sampling method (i.e., the sampling frame and responses), the internal validity of the model (in this case, the TPB), and the statistical conclusion errors [38].

A general reflection is that statistical conclusion errors appear unlikely considering that all surveys have more respondents than the recommended minimum according to [38]. However, there are several other possible explanations. As mentioned in section 3.3, this paper does not aspire to be exhaustive with regard to observing divergent results and analysing possible causes for them. It only aspires to cover some of the more obvious divergences and the most frequently discussed causes for such divergent results when the TPB is used.

Table 5 lists seven observations of results that diverge together with a possible cause for this divergence and a schematic analysis to assess whether this cause contributes to the observed divergence.

Table 5. Observed divergent results and attempts to explain them

Observation	Possible cause	Analysis
In some studies, PBC has little effect on intentions.	The behaviour is more volitional in the studies in which PBC has little effect [6].	Likely. The study investigating PBC and violation intention (which is arguably more volitional than compliance) has the lowest regression coefficient of 0.15 (the mean of the regression coefficient for compliance intention is 0.25). The correlation coefficients point in the same direction, with 0.22 for violation vs. 0.46 for compliance.
In some studies, the effects of ATT and SN seem small.	The theory is used for beliefs concerning an object or goal and not behaviour with an "action element" [6].	Likely. When the questions clearly concern behaviour (in [8–10, 14, 17, 19]), the unweighted mean correlation coefficients (ATT=0.43 and SN=0.66) are greater than when the questions concern the goal or state "compliance" (in [11–13, 18]) (ATT=0.41 and SN=0.37). The regression coefficients have the same tendency, (ATT=0.37 and SN=0.45) vs. (ATT=0.22 and SN=0.24).
In some studies, the SN is comparably important.	Violation (i.e., risky behaviour) is modelled instead of compliance (healthy behaviour). [33, 39]	Likely. SN has a stronger mean correlation in the two studies of violation (r=0.57) than in the other studies that report correlations (r=0.47). Also, the mean regression coefficient is greater for violation (β=0.35) than for compliance (β=0.30).
The influence of antecedents on security policy compliance is high compared with other behaviours (e.g., health-related).	Self-reports, rather than objective observations or predictions of future behaviour, are used to measure behaviour. Or/and the predicted behaviour is measured at the same occasion, not on a future occasion. [6]	Likely. All studies used self-reports of behaviour, and all studies collected these self-reports at the same time that the other variables were assessed. Thus, relative to the average application of TPB, the importance of intention and PBC may be inflated in the present studies because of how behaviour was measured.

Table 5. *(Continued)*

Varying regression coefficients for TPB variables.	The regression coefficients are weakened because of multicollinearity and inclusion of many variables. The regression coefficients are inflated because of multicollinearity and because TPB variables are omitted from the model.	Likely. Large regression coefficients are reported by studies with few variables ([17, 19]). However, studies with correlated variables (e.g., habits in [15]) also report large regression coefficients. Furthermore, neither [13] nor [14] included additional variables, but they produced comparably small regression coefficients.
In some studies, PBC has little effect on intentions and behaviour.	Self-efficacy is measured, and this operationalisation excludes external sources [30] or perceived autonomy [6].	Possible. Studies that used PBC (i.e., [8–10, 14, 16]) yielded greater coefficients on intentions than studies that used self-efficacy, (β=0.27 and r=0.47) vs. (β=0.21 and r=0.42). However, for regression coefficients, PBC seems to have less influence on behaviour than self-efficacy.
In some studies, the antecedents of intentions seem less important	The "principle of compatibility" is not fulfilled, i.e., the action, target, context and time should be the same when all variables are measured [6, 32, 35, 40]	Unlikely. In [4], a mix of questions regarding general security behaviour and compliance behaviour is used; in [9, 10], following rules and taking precautions are mixed; and in [12], technology questions are mixed with questions regarding compliance behaviour. Their unweighted correlation coefficients (ATT=0.47, SN=0.66, and PBC=0.46) are even greater than the correlation coefficients of those with compatible questions (ATT=0.47, SN=0.48, and PBC=0.43). The regression coefficients point in different directions.

5 Discussion

As indicated above, it is non-trivial to interpret the results of studies related to the TPB or its variables. Validity issues associated with the analyses are discussed in section 5. Section 5.2 presents recommendations for decision makers concerned with information security management. Section 5.3 offers recommendations for security researchers.

5.1 Issues When Interpreting the Puzzle Left by Mixed Models and Adaptations

It is fair to say that the TPB has not been the focus of quantitative studies on information security policy compliance and violation despite its immense popularity in the behaviour sciences. This review was only able to identify 15 quantitative surveys that investigated one or more variables included in the TPB. Two studies (namely [9, 10] and [11]) included all the TPB variables, and other (potentially correlated) variables are included in most of the tested regression models.

Furthermore, many of the studies did not follow the guidelines, caveats, and recommendations regarding how the TPB should be applied and tested (e.g., concerning the measurement instruments), most likely because the TPB was not the focus of these studies. Fishbein and Ajzen [6] find that "*[e]ven though virtually hundreds of studies have tested variations of our theory, we were able to find only relatively few*

that contained all the elements required for a complete and valid test". Our conclusion is that this also applies to the studies that apply the TPB to information security policy compliance and violation. In our view, no study followed all the guidelines completely.

The implication of these two factors (incomplete models and incompliance with guidelines) is that the results should be interpreted cautiously. When other variables are mixed with the TPB variables, the regression coefficients can be influenced. When departures are made from established guidelines, caveats, and recommendations, it should be expected that this theory's efficacy will be influenced. In Table 5, some other possible explanations for differences in the results were explored, but no crystal clear explanations could be found. A larger sample of studies regarding the TPB and differences related to individuals' security behaviours (e.g., sampling differences) may explain the divergent results better.

5.2 Recommendations for Practitioners and Decision Makers

The TPB is one of the most-researched theories in the behavioural sciences. However, despite its value to and use in other domains (e.g., dieting, drug use, exercise, and marketing) it has not been widely proposed or used as a basis for ideas on how security behaviour should be influenced or controlled. Bits and pieces of the theory are used, and ideas coupled to the TPB can be found in the practitioner-oriented security literature. For instance, NIST's handbook about computer security [41] explains that "*changing attitudes is just one step toward changing behaviour*". However, it is surprisingly difficult to find references to the theory by name or cases in which the whole theory (i.e., all the variables and relationships in it) has been used within the practitioner-oriented information security literature (textbooks, white papers, and guidelines, for example). Despite this lack of references, the authors' experiences suggest that decision makers in the information security field often make predictions following the reasoning of the TPB, but they are presumably unaware of the fact that the TPB has formalised their reasoning.

Although it uses a small number of predictor variables, the TPB has a considerable ability to explain human intentions and behaviour compared with its alternatives [6]. The results of this study indicate that the TPB is approximately as meaningful for information security behaviour as it is for behaviours on average. Thus, it is reasonable to expect that decision-making and interventions (e.g., education programs) would benefit from using the TPB as a basis, as decision-making and interventions in other domains already do.

5.3 Recommendations for Researchers and for Future Work

The TPB is a theory with impressive merits, and the results of this review clearly demonstrate that it is valid for the behaviours related to information security policy compliance and violation. Our opinion is that researchers should consider conducting studies focusing explicitly on the TPB to further explore and establish its efficacy for predicting and explaining information security behaviour before mixing multiple

theories (and essentially creating new theories). Studies regarding the TPB can aim at establishing the relative importance of its variables, identifying its explanatory power under different circumstances and for different behaviours, and exploring extensions that are of particular relevance to inform security behaviour.

To correctly appraise the relevance, accuracy, and importance of the TPB and its variables, researchers should attempt to follow the provided guidelines, caveats, and recommendations. For instance, clear guidelines concerning the design of questionnaires are provided on Azjen's website [28], and the relevance of many theoretical ideas are discussed in [6]. These ideas may offer inspiration for research regarding the circumstances and behaviour-types that are relevant for exploration.

The originators of the theory are (and have been) open to include additional variables in their theoretical framework if the proposed addition is (1) behaviour-specific, (2) possible to conceive as a causal factor of behaviour, (3) conceptually different from existing predictors, (4) applicable to a wide range of behaviours studied by social scientists, and (5) explains a sufficient amount of additional variance [6, 7]. Several additions have been proposed and dismissed on the basis of these requirements (see [6, 7]). For instance, habits are not considered to fulfil (2) because past behaviour (which is used to measure habit) is not itself a causal factor [3]. Whereas many proposals have been dismissed on fair grounds, there may be extensions or adaptations that are especially suitable and meaningful for information security behaviours. Thus, extensions that comply with all requirements except for (4) may be relevant for the security community to explore. For instance, meaningful and promising ideas for extensions can be sought in literature regarding security economics and the human aspects of information security.

6 Conclusions

This review sought the answer to two research questions by synthesising the reports from 16 empirical studies that address the TPB or its variables in relation to information security policy compliance and violation. The answer to the first research question is that the TPB has approximately the same explanatory power for information security policy compliance and violation as it has for behaviours on average. Approximately 0.4 of the variance in intentions can be explained, and the correlations and regression coefficients for variables that influence behaviour are also similar to those found in other domains. The answer to the second research question is that some potential explanations for why the results of the identified studies diverge can be found. However, many of the differences in the results are left unexplained.

Acknowledgments. The authors would like to thank the following researchers for responding to our inquiries: Prof. Merril Warkentin, Dr. Allen Johnston, Dr. Sang M. Lee, Dr. Sang-Gun Lee, Prof. Mikko Siponen and, in particular, Dr. Seppo Pahnila. This research is sponsored by the Swedish Civil Contingencies Agency (MSB).

References

1. ISO/IEC: Information technology – Security techniques – Information security management measurements, ISO/IEC 27004, Geneva, Switzerland (2009)
2. Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J.: Variables influencing information security policy compliance: a systematic review of quantitative studies. Under review
3. Ajzen, I.: The theory of planned behavior. Organizational Behavior and Human Decision Processes 50, 179–211 (1991)
4. Ifinedo, P.: Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers and Security, 83–95 (2012)
5. Fishbein, M.: A theory of reasoned action: Some applications and implications (1979)
6. Fishbein, M., Ajzen, I.: Predicting and Changing Behavior: The Reasoned Action Approach. Psychology Press, New York (2010)
7. Ajzen, I.: The theory of planned behaviour: reactions and reflections. Psychology & Health 26, 1113–1127 (2011)
8. Hu, Q., Dinev, T., Hart, P., Cooke, D.: Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Sciences 43, 615–660 (2012)
9. Cox, J.: Information systems user security: A structured model of the knowing–doing gap. Computers in Human Behavior 28, 1849–1858 (2012)
10. Cox, J.: Organizational narcissism as a factor in information security: A structured model of the user knowing-doing gap (2012)
11. Siponen, M., Pahnila, S., Mahmood, A.: Compliance with Information Security Policies: An Empirical Investigation. Computer 43, 64–71 (2010)
12. Herath, T., Rao, H.R.: Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems 18, 106–125 (2009)
13. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly: Management Information Systems 34, 523–548 (2010)
14. Dugo, T.M.: The insider threat to organizational information security: a sturctural model and empirical test (2007), http://etd.auburn.edu/etd/handle/10415/1345
15. Pahnila, S., Siponen, M., Mahmood, A.: Employees' behavior towards IS security policy compliance. In: Proceedings of the Annual Hawaii International Conference on System Sciences, Big Island, HI, p. 10 (2007)
16. Zhang, J., Reithel, B.J., Li, H.: Impact of perceived technical protection on security behaviors. Information Management and Computer Security 17, 330–340 (2009)
17. Guo, K.H., Yuan, Y., Archer, N.P., Connelly, C.E.: Understanding nonmalicious security violations in the workplace: A composite behavior model. Journal of Management Information Systems 28, 203–236 (2011)
18. Li, H., Zhang, J., Sarathy, R.: Understanding compliance with internet use policy from the perspective of rational choice theory. Decision Support Systems 48, 635–645 (2010)
19. Johnston, A.C., Warkentin, M.: The Influence of Perceived Source Credibility on End User Attitudes and Intentions to Comply with Recommended IT Actions. Journal of Organizational and End User Computing 22, 1–21 (2010)

20. Vance, A.: Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. Why do employees violate is security policies? Insights from multiple theoretical perspectives. pp. 93–110. Faculty of Science, Department of Information Processing Science, University of Oulu, Oulu, Finland (2010)
21. Lee, S.M., Lee, S.-G., Yoo, S.: An integrative model of computer abuse based on social control and general deterrence theories. Information & Management 41, 707–718 (2004)
22. Chan, M., Woon, I.: Perceptions of information security in the workplace: linking information security climate to compliant behavior. Journal of Information Privacy and Security 1, 18–41 (2005)
23. Son, J.-Y.: Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information and Management 48, 296–302 (2011)
24. Gibbs, J.P.: Crime, Punishment, and Deterrence, New York (1975)
25. Hirschi, T.: Causes of Delinquency. Unveristy of California Press, Berkeley (1969)
26. Becker, B.J., Wu, M.-J.: The Synthesis of Regression Slopes in Meta-Analysis. Statistical Science 22, 414–429 (2007)
27. Ajzen, I.: The theory of planned behavior. Organizational Behavior and Human Decision Processes 50, 179–211 (1991)
28. Ajzen, I.: Theory of Planned Behavior, http://people.umass.edu/aizen/tpb.html
29. Armitage, C.J., Conner, M.: Efficacy of the Theory of Planned Behaviour: a meta-analytic review. The British Journal of Social Psychology / the British Psychological Society 40, 471–499 (2001)
30. Conner, M., Armitage, C.J.: Extending the Theory of Planned Behavior: A Review and Avenues for Further Research. Journal of Applied Social Psychology 28, 1429–1464 (1998)
31. McEachan, R.R.C., Conner, M., Taylor, N.J., Lawton, R.J.: Prospective prediction of health-related behaviours with the Theory of Planned Behaviour: a meta-analysis. Health Psychology Review 5, 97–144 (2011)
32. Montano, D.E., Kasprzyk, D.: Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. In: Glanz, K., Rimer, B., Viswanath, K. (eds.) Health Behavior and Health Education: Theory Research, and Practice, pp. 68–96. United States of America (2008)
33. Rivis, A., Sheeran, P.: Descriptive Norms as an Additional Predictor in the Theory of Planned. Current Psycology: Developmental, Learning, Personality, Scoial 22, 218–233 (2003)
34. Sheppard, B., Hartwick, J., Warshaw, P.: The theory of reasoned action: A meta-analysis of past research with recommendations for modifications and future research. Journal of Consumer Research 15, 325–343 (1988)
35. Trafimow, D.: Distinctions Pertaining to Fishbein and Ajzen's Theory of Reasoned Action. In: Ajzen, I., Albarracin, D., Hornik, R. (eds.) Prediction and Change of Health Behavior: Applying the Reasoned Action Approach, Erlbaum, Hillsdale (2007)
36. Sheeran, P., Trafimow, D., Finlay, K., Norman, P.: Evidence that the type of person affects the strength of the perceived behavioural control-intention relationship. The British Journal of Social Psychology / the British Psychological Society 41, 253–270 (2002)
37. Albarracín, D., Johnson, B.T., Fishbein, M., Muellerleile, P.A.: Theories of reasoned action and planned behavior as models of condom use: a meta-analysis. Psychological Bulletin 127, 142–161 (2001)

38. Malhotra, M., Grover, V.: An assessment of survey research in POM: from constructs to theory. Journal of Operations Management 16, 407–425 (1998)
39. Hooker, K., Kaus, C.R.: Health-related possible selves in young and middle adulthood. Psychology and Aging 9, 126–133 (1994)
40. Ajzen, I., Albarracin, D.: Predicting and Changing Behavior. In: Ajzen, I., Albarracin, D., Hornik, R. (eds.) Prediction and Change of Health Behavior: Applying the Reasoned Action Approach. Erlbaum, Hillsdale (2007)
41. NIST: An introduction to computer security: The NIST Handbook. Nist Special Publications. 800 (1995)