12-12-2021

Use of protection motivation theory in non-compliance research

Marcus Gerdin
Örebro University, Marcus.gerdin@oru.se

Åke Grönlund
Örebro University

Ella Kolkowska
Örebro University

Use of Protection Motivation Theory in Non-/compliance Research

Marcus Gerdin [1]
Örebro University
Örebro, Sweden

Åke Grönlund
Örebro University
Örebro, Sweden

Ella Kolkowska
Örebro University
Örebro, Sweden

ABSTRACT

There is a rich stream of research focusing on employee non-/compliance with information security policies. However, this stream suffers from inconsistent, even contradicting results and lack of theorical congruence. Attempts to explain such inconsistencies have included investigation of possible moderating effects of contextual variables. We further investigate these inconsistencies by analytically disentangling the consistency in the implementation of the four most used variables of Protection Motivation Theory—*Perceived severity*, *Perceived susceptibility*, *Response efficacy*, and *Self-efficacy*—across the research field. Specifically, we address the following research question; *what inconsistencies, if any, are there in the use of Protection motivation theory in non-/compliance research?*

We find that three of the variables analyzed have been ascribed more than one theoretical property across the seven studies reviewed, thereby making it problematic to fully understand their cause-and-effect relationships. That is, it is unclear which property that explains employees' intention to comply with IS policies, whether they have the same effects, or have an increased effect when applied in conjunction. This study contributes to the literature by proposing that

[1] Corresponding author. Marcus.gerdin@oru.se +4670 5951299

inconsistent results may not only be due to omitted moderating factors, but also to theoretical properties of key variables being inconsistently defined and measured.

Keywords: Protection Motivation Theory, PMT, Non-compliance, Inconsistent results, Variable properties, Consistent theory usage

1. INTRODUCTION

Research on employee non-/compliance with security policies has grown substantially from the first contributions in the early 1990s (Straub 1990). This research has not only brought about a more nuanced understanding of the complex phenomenon, but also resulted in a vast research landscape based on multiple theoretical perspectives, often behavioral theories borrowed from other research disciplines and tailored to the context of non-/compliance (Moody et al. 2018; Sommestad et al., 2014; Cram et al. 2017; 2019).

As the research field has matured, numerous literature reviews have been conducted, observing several problems regarding how research is carried out. For instance, Sommestad et al. (2014), Vance et al. (2012) and Cram et al. (2017; 2019) observed that there are several inconsistent, or even contradicting, research results and that there is a lack of theorical congruence. They found that relationships between the same set of variables have different directions and different effect sizes in different articles

Attempts to explain such inconsistencies include investigation of possible moderating effects inflicted by *external factors,* that is*,* contextual factors that can explain why directions and effect sizes differ between studies (Cram et al. 2019). However, even after such extensions, many inconsistencies remain (Cram et al. 2019). There is therefore a need to also consider *internal*

influencing factors, that is, how theories are used in different studies. In that vein, Sommestad et al. (2014) suggested two internal factors they believe could help explain the conflicting results: *differences in studies quality* and *differences among studies with respect to research method*. However, they did not test these internal factors as "*few studies included in this review overlap with each other with respect to the variable-relationship they measure*" (p 59). To test theory consistency between studies, we need a large sample of studies investigating the same relationship among variables. In this study, therefore, we set out to test theory consistency on a larger set of studies.

As suggested by a recent literature review (Cram et al. 2019), there is a limited number of what they refer to as, primary theoretical/conceptual bases. Specifically, they identify four theories which can be seen as representing the core of the field: Protection motivation theory (PMT), Theory of planned behavior (TPB), Rational choice theory (RCT) and Deterrence theory (DT). Out of these four theories, PMT, has been particularly discussed in terms of how it is used within the research field (Johnston et al. 2015; Haag et al. 2021).

Therefore, before investigating the entire spectrum of theories, we conduct this pilot study of PMT to identify if the problem of inconsistencies exists and, if so, the potential consequences of it. We draw on previous reviews, but rather than focusing on summing up what we know thus far in terms of empirical findings and examining external factors explaining inconsistencies, we focus on how the variables of PMT are used in non-/compliance research.

We also discuss their implications for future research in this area. In so doing, we draw upon Luft and Shield's (2003) highly influential paper in management accounting which compares definitions and applications of variables, and relations among variables. This offers the

opportunity for us to test the PMT theory consistency within the field and to enhance our understanding of the inconsistent study results. More specifically, this study asks,

What inconsistencies, if any, are there in the use of Protection motivation theory in non-/compliance research?

By inconsistencies we refer to definition and item measurements of variables.

We investigate that by categorizing the properties of each variable and analyzing the consistency across the selected studies. In so doing, we illustrate how the research field is currently studied as concerns the PMT variables. Based on these findings, we suggest interesting paths for future research.

2. PMT AND VARIABLES

PMT is defined in various ways. The original version, from psychology, includes a large number of variables but studies in compliance research typically draw on a smaller set (Haag et al. 2021). We have here considered as the "basis model" the one from Moody et al. (2018), which comprises the independent variables of *severity*, *susceptibility*, *response efficacy*, and *self-efficacy* and the dependent variable of *intention*, as Haag et al. (2021) found these variables to be, by a large extent, most frequently used in non-/compliance research.

2.1 Variables

A first observation is that studies based on PMT almost always add new variables, often taken from other behavioral theories, such as TPB. Previous reviews (Cram et al. 2017; 2019; Sommestad et al. 2014; Haag, Siponen and Liu 2021), however, have noted that these new variables oftentimes represent the same, or very similar, phenomena, only with different labels. Moreover, it has also been recognized that variables with the same name not necessarily represent the same phenomena. For example, the definition of the variable *reward* differs between Siponen

et al. (2015) and Vance et al. (2012). This means that the content of variables must be closely inspected, in order the fully understand the underlying cause-and-effect.

We map the cause-and-effect logic for each variable from PMT following the Luft and Shields (2003) description of good variable practice. Luft and Shields (2003) stress the importance of being precise in defining and operationalizing variables. They distinguish between what they call *practice defined variables,* and *theory defined variables,* based on the way variables are defined and the structure/arrangement of their properties. *Practice defined variables* draw upon the language of practitioners to describe that of interest. For example, practitioners may be interested in the effects of "security awareness training programs" and "information security policies" on employees' intention to comply with IS policies. While an advantage of this type of variable is that they make intuitive sense to most practitioners, a disadvantage is that they are typically broadly defined. A single variable often includes several properties, some of which may be irrelevant to the research question at hand. For example, a "security awareness program" may update employees on (1) the *severity* of IS threats, (2) the *vulnerability* of IS threats, and (3) the *skills required* to effectively deal with the threat (e.g., Hina Selvam & Lowry 2019), Such variables, containing multiple properties, can have different causes and effects (Luft and Shields 2003, p.188).

In contrast, *theory defined variables* are characterized by "well-defined, stable, unitary meanings making it possible to identify consistent cause-and- effect relations" (Luft & Shields 2003, p. 188). A theory defined variable contains only one property that is specifically tailored to a particular research question, and explains, or is explained by, variations in the property of another theory defined variable.

In conclusion, "a variable too broadly defined relative to the underlying theory generates noise in the cause– effect relation and makes it less likely that the effects specified in the theory will be detected, even when they exist. Too broad [of] a definition also makes it more likely that effects other than those specified in the theory will be detected and wrongly interpreted […]. In contrast, a variable too narrowly defined captures only part of the proposed cause–effect relation and also makes it less likely that the effects specified in theory will be detected, even when they exist" (Luft and Shields 2003, p. 189).

This line of reasoning is applicable also to the operationalization of variables into measurement instruments as there may be a discrepancy between what we claim/aim to measure (property of the variable, defined in our variable definition) and what we actually measure (e.g., items in a questionnaire). That is, a measurement instrument may contain items which only capture fragments of the proposed property or items which do not correspond well to the property or capture several properties (not in line with the variable definition), thereby increasing the risk of drawing invalid conclusions. Accordingly, we here not only look at variable definitions but also at how the variables are operationalized. This is done by comparing the measurement items with the variable description/properties.

With this in mind, it should be noted that even though a variable may originate from a known theory (in our case PMT), they can still contain characteristics of a p*ractice defined variable* in the study, depending on how the authors chose to define and measure it. Thus, *practice* and *theory defined variables* should be seen as two ends on a spectrum rather than two distinctive categories.

3. METHOD

As this is a pilot study and we wanted to identify possible discrepancies in the use of PMT –not necessarily finding *all* there may be – we selected seven articles using PMT. The selection was made from a set of 35 (PMT) articles that we found in a literature search covering the past 10 years. Because we looked for differences, we selected studies that had come to different conclusions. We also made sure to include different authors and different journals.

3.1 Coding and analysis

The coding process comprised two steps. The first included systematically extracting the same type of variable information from each study and from this, categorize each variable's inherent properties. In the second step we compared the studies.

Step 1, analyzing variables. Using a standardized form, based on Luft and Shields (2003), we extracted each variable definition from all studies, i.e., the word-by-word definition of each variable. Next, we extracted all questionnaire items used to measure the variable (only one article, Blythe and Coventry (2018), did not provide a full list of measure items).

From the variable definition and items, we categorized each variable's properties. For example, Ifinedo (2012) defined *Perceived vulnerability* as: "an individual's assessment of the probability of threatening events." (p. 84). From this definition we can draw that the property proposed (cause-and-effect) is linked to the *probability* of a threatening event. The same thing can be done for the questionnaire items. Using Ifinedo (2012) again, one item is designed as: "More and more serious information security threats are being faced by my organization" (p. 92), which also refers to probability of a threatening event. Thereby, the identified property (cause-and-effect) in this cause is probability (cause).

We focused on the "basic" PMT as defined by the Moody et al. (2018) which uses the variables *perceived severity, perceived vulnerability, response efficacy,* and *self-efficacy.* One reason for not including variables that other studies have used to amend the theory, such as *response cost* and/or *rewards*, is due to their limited usage (Haag et al. 2021). Another reason is that this is a pilot study only looking for the existence of inconsistencies and not aiming at identifying *all* consistencies there may be.

Step 2, comparing studies. Having identified properties for each variable from every study, we created variable-tables in which we grouped all properties found for each variable (e.g., see Table 1). From these tables it is easy to pinpoint discrepancies.

4. RESULT

We present the result by variable: perceived severity, perceived vulnerability, self-efficacy, and response efficacy.

4.1 Perceived Severity

The variable Perceived Severity was used in all the seven studies investigated, although in two instances under different names. Hooper and Blunt (2020) use the name "*Perceived impact*" and Menard, Bott and Crossler (2017) use "*Threat severity*", but from the variable description and the measurement items it is evident that all studies refer to the same core variable property, namely, to the *consequences* of a threat. Thus, the variable is defined in line with good variable practice in this small set of articles.

However, when dissecting the questionnaire items used to measure this variable, we find important, yet unacknowledged, nuances regarding the properties of consequences. Some studies

explore consequences related to the *organization* while others explore consequences related to the *individual* (examples in Table 1).

These differences are not present in the variable definitions. All studies either directly refer to *consequences for the organization* or do not clearly state who are affected by the consequences. Hence, the measurement items are not always in line with the variable definitions: we found several instances where the consequences are not connected to the organization but to the individual employee (see examples in Table 1). Thus, we have a potential problem insofar that some studies define the consequences as strictly organizational but in fact measure consequences for the individual. Moreover, it cannot be ruled out that this inconsistency leads to different cause-effect relations between this variable and others. For example, it may well be that perceived severity of a particular threat may be greater if the consequences are linked to the individual (e.g., in terms of job loss, public shaming, and/or risk of punishment from employer) than if the organization suffers the consequences (e.g., in terms of reputation and financial losses), or vice versa. Whether or not this is the case is an empirical question.

Table 1

Perceived Severity – Properties	**Illustrative examples of definition from studies**	**Illustrative examples of survey items from studies**
Perceived consequences for the **organization**	"Severity is the level of the potential impact of the threat (i.e., its severity and how severe the damage that it can cause). In our context, it refers to the severity of the IS security breach, and the possible negative event caused by the breach in an **organization**." (Vance et al. 2012) "perceived impact can be defined as an IT employee's perception of the **organizational** consequences of the threat. This includes the immediate impact, such as the loss of confidentiality, integrity and/or availability of the data stored in an information system, and the long-term effect on the business, such as reputational damage and legal or regulatory action." (Hooper et al. 2020)	"An information security breach in my **organisation** would be a serious problem for my organization." (Siponen et al. 2014) "The impact [on] my **organisation** would be _____ if a business-critical information system was unavailable for a prolonged period." (Hooper et al. 2020) "The impact on my **organisation** would be _____ if confidential information was disclosed to an unauthorised party." (Hooper et al. 2020)
Perceived consequences for the **individual**	No studies include individual consequences in their definitions of the variable Perceived Severity	"An information security breach in my organization would be a serious problem for **me**" (Siponen et al. 2014) "An information security breach in my

		organization would be a serious problem for **me**" (Vance et al. 2012) "If my work device were infected by malware, **I** could be severely disciplined" (Menard et al. 2017)
Mix of the identified properties above	"Perceived severity is "the negative consequences an **individual** associates with an event" (e.g., a security threat). For malware threats, this may be consequences towards employees' productivity, the functioning of their devices and their **organisation's** reputation." (Blythe and Coventry 2018)	

4.2 Perceived vulnerability

The variable *perceived vulnerability* was found in all seven studies although sometimes under slightly different labels, such as *threat susceptibility* (Menard et al. 2017) and *perceived susceptibility* (Blythe and Coventry 2018). Here, we find clear differences regarding both variable definitions and questionnaire items used. We can identify two distinct types of vulnerability, which may not necessarily have the same cause-effect relations to other variables.

The first type refers to the individual's perception of the *probability/likeliness* that a threat will occur if no countermeasures are being taken (examples in Table 2). The second type, however, refers to the individual's perception of how *vulnerable* the organization is to said threat (Table 2). To illustrate the importance of this difference, consider a bank employee who may very well feel that the bank is very *likely* to encounter security threats due to the nature of the business. However, the same employee may not necessarily feel that the organization is *vulnerable* to these threats, due to the sophisticated security systems the bank has in place. These two distinct properties of the 'Perceived vulnerability' variable may have different cause-and-effect relationships with other variables, and hence they should be investigated separately. In fact, as of today, we do not know whether it is the perceived likeliness/probability of a threat, or the

organization vulnerability to such threat the explain employees' intention to comply with IS-policies, or whether they have the same effects.

Table 2

Perceived Vulnerability – Properties	**Illustrative examples of definition from studies**	**Illustrative examples of survey items from studies**
Probability/likeliness of being exposed	"Perceived vulnerability, i.e., an individual's assessment of the **probability** of threatening events." (Ifinedo 2012) "Vulnerability is to the **probability** that an unwanted incident will happen if no actions are taken to prevent it." (Vance et al. 2012)	"I **could** be subjected to a serious information security threat." (Ifinedo 2012 "My organization **could** be subjected to a serious information security threat." (Ifinedo 2012) **"More and more** serious information security threats are being faced by my organization" (Ifinedo 2012)
Vulnerability	"With respect to safe computing in the organization, individuals who are of the view that they are **invulnerable** to security threats are more likely not adhere security measures at work." (Ifinedo 2012) "Threat susceptibility refers to the degree to which someone feels **vulnerable** to a particular threat." (Menard et al. 2017)	"It is _____ that a security incident will occur at my organisation that will result in a **business-critical information system being unavailable** for a prolonged period." (Hooper et al. 2020) "It is _____ that a security incident will occur at my organisation that will result in **confidential information being disclosed** to an unauthorised party" (Hooper et al. 2020) "It is _____ that a security incident will occur at my organisation that will result in the integrity of information stored in a system being compromised." (Hooper et al. 2020)

4.3 Self-efficacy

The variable self-efficacy was used in all seven studies, and in all cases labeled the same. However, an analysis of the definitions in different studies reveals two distinct properties. The first property refers to the individuals' *subjective judgement of /belief in* their ability to perform the expected security behavior while the second one refers to an actual *objective ability/capability/competence* of the individual to comply with the expected security behavior (examples in Table 3).

These two properties are not necessarily interchangeable. An employee may very well have high belief in her/his ability to undertake protective behavior, but still have limited actual ability or competence to do so may (and vice versa).

We also observe that researchers sometimes mix these two properties in their definitions as well as in their questionnaire items (Table 3). In some studies, the definition of the variable refers to one property and the measurement items refer to the other.

Table 3

Self-Efficacy – Properties	**Illustrative examples of definition from studies**	**Illustrative examples of survey items from studies**
Confidence/belief in its ability to performance expected security behavior	"Self-efficacy is the **confidence** an individual possesses in effectively performing the recommended response" (Menard et al. 2017)" "self-efficacy (the degree that he or she **believes** it is possible to implement the protective behavior)". --- "Self-efficacy in our study, refers to employees' belief that they can successfully comply with IS security policies, which should enhance compliance with policies and procedures" (Vance et al. 2012)	"I **believe** that I have the necessary skills to protect myself from information security violations." (Hina et al. 2019) "I **believe** that I have developed the capability to prevent people from getting my confidential information." (Hina et al. 2019)
(objective) Ability/capability /competence to follow expected security behavior	"self-efficacy emphasizes the individual's **capabilities and competence** to cope with the task or make a choice" (Blythe and Coventry 2018).	"Doing the opposite of what the [scenario character] did **would be difficult** for me to do." (Vance et al. 2012) "Doing the opposite of what the [scenario character] did **would be easy** for me to do." (Vance et al. 2012) "**It is easy** for me to perform the information security behaviour required by my organisation." (Hooper et al. 2020) "**It is difficult** for me to perform the information security behaviour required by my organisation." (Hooper et al. 2020)
Mix of above identified properties	"Self-efficacy can be defined as "an individual's **beliefs** about their competence to cope with a task and exercise influence over the events that affect their lives" (Bandura, 1977). In a security context, employees who have high **security-related capabilities** are presumed to be more likely to follow security practices as they are more effective in learning how to follow them and being able to perform the appropriate behaviour." (Blythe and Coventry 2018)	

	"Self-efficacy eth is factor emphasizes the **individual's ability** or **judgment** regarding his or her capabilities to cope with or perform the recommended behavior" (Ifinedo 2012) "a person's **belief** in their ability to perform a recommended behavior and effectively deal with a threat (e.g., **their skill and judgement abilities** for dealing with a security breach risks)" (Hina et al. 2019)	

4.4 Response Efficacy

The variable Response efficacy was used in all seven studies. This is the only variable consistently defined among all researchers, addressing only one theoretical property, namely the individual's perception of the effectiveness of recommended coping response (see Column 2 in Table 4). Also, all studies analyzed used questionnaire items which operationalize this particular property and they have done so in a consistent way (Table 4).

Table 4

Response Efficacy – Property	**Illustrative examples of definition from studies**	**Illustrative examples of survey items from studies**
Individuals' beliefs in effectiveness of the recommended response	"Response efficacy refers to an individual's **perception of how well the recommended response addresses the threat** at hand (e.g., follow security policy)" (Menard et al. 2017) "response efficacy (the belief in the **perceived benefits of the coping action** by removing the threat)" (Vance et al. 2012) "[…] one's judgment of how **effective a person believes a recommended response** will be should they follow it. In our context, for example, response efficacy would be an **employee's belief that following an organizationally recommended security procedure will actually prevent a threat** " (Hina et al. 2019)	"Complying with information security policies in our organization keep IS security breaches down" (Siponen et al. 2014) "Careful compliance with IS security policies helps to avoid IS security problems." (Vance et al. 2012) "In my institution, the available security measures to protect my work information from security violations are effective." (Hina et al. 2019)

5. DISCUSSION AND CONCLUSION

This study investigated *what inconsistencies, if any, are there in the use of Protection motivation theory in non-/compliance research?* "Inconsistencies" refers to description and item measurements of variables. We investigated seven studies using PMT to see if there is reason to

believe that differences in definitions and use of variables may be a reason for differences in research results.

We found that three out of four variables – perceived vulnerability, perceived severity, and self-efficacy – contained more than a single property, making it problematic to fully understand the cause-and-effect relationship proposed. Thus, we cannot know which property explains employees' intention to comply with IS policies, whether they have the same effects, or have an increased effect when applied in conjunction.

Even though we investigated a small number of studies, this shows that the use of PMT is not consistent across studies. Moreover, we discovered occurrences of inconsistent variable properties within individual studies. Thus, our study adds to the discussion about reasons behind the inconstant results plaguing the field of non-compliance research by showing that *property variance* is a potential explanatory factor. Thus, our result ties well into research in the likes of Cram et al. (2019) and Sommestad et al. (2014) as we identify potential factors which may be the cause for the inconsistent results within the non-/compliance research field. Indeed, we argue that our study is a first start to decipher an important piece of the jigsaw puzzle, that of examining theoretical congruence within a single study, as opposed to investigating external moderators which the previously authors chose to. Moreover, our study further contributes to the discussion about the use of the PMT in the non-/compliance research, as we in line with Johnston et al (2015) and Haag et al (2021) observe various implementations.

As our sample is small, there is of course a need to investigate to what extent this is a problem for the field in its entirety, including both the use of other theories and a larger set of PMT studies. As a final say however, as this study worked as an initial test of a research idea and targeted seven (out of 35 currently identified studies), we are planning to expand the number of

studies and make it into a full review. In the full review, we would be able to draw a more general conclusion on how consistent the PMT has been used, and better understand what if and how it may affect the problematic fact of inconsistent results.

REFERENCES

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, *87*, 87-97.

Cram, W. A., Proudfoot, J. G., & D'arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26*(6), 605-641.

Cram, W. A., D'arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525-554.

Hina, S., Selvam, D. D. D. P., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, *87*, 101594.

Hooper, V., & Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology*, *39*(8), 862-874.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework. *MIS quarterly*, *39*(1), 113-134.

Luft, J., & Shields, M. D. (2003). Mapping management accounting: graphics and guidelines for theory-consistent empirical research. *Accounting, organizations and society*, *28*(2-3), 169-249.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203-1230.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS quarterly*, *42*(1).

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2), 217-224.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii-xxiii.