What goes around comes around: an in-depth analysis of how respondents interpret ISP non-/compliance questionnaire items

Marcus Gerdin, Ella Kolkowska and Åke Grönlund
Department of Informatics, Örebro University, Örebro, Sweden

Received 7 December 2023
Revised 9 February 2024
Accepted 10 February 2024

Abstract

Purpose – Research on employee non-/compliance to information security policies suffers from inconsistent results and there is an ongoing discussion about the dominating survey research methodology and its potential effect on these results. This study aims to add to this discussion by investigating discrepancies between what the authors claim to measure (theoretical properties of variables) and what they actually measure (respondents' interpretations of the operationalized variables). This study asks: How well do respondents' interpretations of variables correspond to their theoretical definitions? What are the characteristics of any discrepancies between variable definitions and respondent interpretations?

Design/methodology/approach – This study is based on in-depth interviews with 17 respondents from the Swedish public sector to understand how they interpret questionnaire measurement items operationalizing the variables Perceived Severity from Protection Motivation Theory and Attitude from Theory of Planned Behavior.

Findings – The authors found that respondents' interpretations in many cases differ substantially from the theoretical definitions. Overall, the authors found four principal ways in which respondents interpreted measurement items – referred to as property contextualization, extension, alteration and oscillation – each implying more or less (dis)alignment with the intended theoretical properties of the two variables examined.

Originality/value – The qualitative method used proved vital to better understand respondents' interpretations which, in turn, is key for improving self-reporting measurement instruments. To the best of the authors' knowledge, this study is a first step toward understanding how precise and uniform definitions of variables' theoretical properties can be operationalized into effective measurement items.

Keywords Information security policy, Non-/compliance research, Validation of measurement instruments, Protection motivation theory, PMT, Theory of planned behavior, TPB

Paper type Research paper

1. Introduction

Due to the importance of employee knowledge and activities in safeguarding organizational information assets, extensive scholarly effort has focused on human aspects of information

The authors gratefully acknowledge the useful comments made by participants at the HAISA conference held in Canterbury 2023.

Information & Computer Security
Vol. 32 No. 4, 2024
pp. 459-476
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-12-2023-0240

security (Cram *et al.*, 2017; Cram *et al.*, 2019; Khan *et al.*, 2022; Moody *et al.*, 2018; Straub, 1990). The present study focuses on a rapidly growing subset of this research area, namely, on research investigating how and why employees comply, or not, with the organizational information security policies (ISPs) (D'Arcy and Lowry; 2019).

The dominant epistemological and ontological foundations in this ISP non-/compliance research are positivistic in nature (Khan *et al.*, 2022; Simons, 2021), implying that most of the studies within the field rely on quantitative survey data (Karlsson *et al.*, 2017; Khan *et al.*, 2022) based on theories of human behavior (Cram *et al.*, 2019). On these bases, our knowledge about ISP non-/compliance has been gradually improved as additional variables, serving both as predictors and moderators, have been incorporated in the theoretical models (Karljalainen *et al.*, 2019). Notwithstanding these advancements, however, recent literature overviews have noted that this stream of literature has so far produced inconsistent, even contradicting results (Cram *et al.*, 2019; Mou *et al.*, 2022).

It may not appear surprising that non-/compliance studies yield varying results across different contexts, as prior research has indicated that this type of employee behavior is context-dependent (Karlsson *et al.*, 2017; Siponen and Vance, 2014). This said, however, research shows that even after "controlling for" various contextual factors, many inconsistencies remain (Cram *et al.*, 2019). Accordingly, studies have called for research that investigates the extent to which such empirical inconsistencies are attributable to differences in conceptualizations and operationalizations of important theoretical variables (Sommestad *et al.*, 2014, 2015; see also MacKenzie *et al.*, 2011). This involves assessing to what extent theoretical variables are effectively operationalized into questionnaire items and ensuring that these items are interpreted by respondents in accordance with the theoretical properties as defined in the variables (Desimone and Le Floch, 2004; Luft and Shields, 2003; Mackenzie *et al.*, 2011).

Along these lines, for example, the review studies of Sommestad (2015) and Gerdin *et al.* (2021) noted several inconsistencies between variable definitions and measurement items within and across studies. And, empirically, Mou *et al.* (2022) and Cram *et al.* (2019) found significant differences in results between studies depending on how the content of ISPs had been operationalized into measurement instruments. Similarly, Siponen and Vance (2014) and Karlsson *et al.* (2017) highlighted the importance of developing measurement items that are tailored to the respondents' organizational context. Notwithstanding these insights, however, there are, to the best of our knowledge, no empirical studies that explores *how respondents actually interpret commonly used questionnaire measurement items in ISP non-/compliance research*. Hence, there is limited understanding of the extent to which respondents' interpretations of questionnaire items align with the theoretical properties of the variables in question.

Addressing this knowledge gap, we conducted an interview study enabling us to analyze in depth how respondents interpreted questionnaire measurement items depicting two key variables from the two most used theories in the field, Protection Motivation Theory (PMT) and Theory of Planned Behavior (TPB) (e.g. Boss *et al.*, 2015; Cram *et al.*, 2019; Haag *et al.*, 2021; Johnston *et al.*, 2015; Sommestad *et al.*, 2015). Specifically, drawing from influential papers discussing variable measurement and validation procedures (e.g. Boudreau *et al.*, 2001; Luft and Shields, 2003; MacKenzie *et al.*, 2011; Podsakoff *et al.*, 2016), we investigate whether there are any discrepancies between what we claim to measure – a theoretical property of the variable as stated in variable definitions – and what we actually measure in terms of respondents' interpretations. If there is a gap between the two, there is noise in the measurement as there is a high risk that we do not measure what we think we do.

Specifically, the study asks:

Q1. How well do respondents' interpretations of variable measurement items correspond to their theoretical definitions?

Q2. What are the characteristics of any discrepancies between variable definitions and respondent interpretations?

Arguably, this study not only contributes to the emerging literature on variable measurement and validation procedures within the ISP non-/compliance literature (Cram *et al.*, 2019; Karlsson *et al.*, 2017; Siponen and Vance, 2014) but also to the more general MIS literature on this topic (Boudreau *et al.*, 2001; Mackenzie *et al.*, 2011; Podsakoff *et al.*, 2016). Specifically, we do so by identifying four principal types of respondent interpretations – referred to as property contextualization, extension, alteration and oscillation – each implying more or less (dis)alignment with the intended theoretical properties of the two variables examined. And, through so doing, our study adds further insights on how to mitigate the problem of misalignment between what we claim to measure, and what we actually measure.

2. Related research

The research domain that investigates employee non-/compliance with policy requirements falls within the scope of behavioral information security research (Khan *et al.*, 2022; Liang *et al.*, 2023) and focuses on complex social phenomena that are usually challenging to quantify (Liang *et al.*, 2023). Despite these challenges, however, the field has predominantly used survey-based, quantitative methods (Khan *et al.*, 2022) to theorize, and empirically test, how compliance behavior – or the intention to comply – can be explained by various factors (Karjalainen *et al.*, 2019).

As detailed above, however, there is an emerging discussion about the validity of research methodologies, specifically, about the conceptualization of variables and measurement practices in the field (Chen *et al.*, 2021; Cram *et al.*, 2019; Karjalainen *et al.*, 2019). Although this debate may seem recent in the area of ISP non-/compliance, the validation of questionnaire-based measurement tools has been a longstanding topic of discussion in the behavioral MIS literature (Boudreau *et al.*, 2001; MacKenzie *et al.*, 2011; Straub, 1989) and other disciplines (Bennett *et al.*, 2011; Wikman, 2006). Considering that non-/compliance research, as a component of behavioral information security, shares similar challenges, insights from these related fields could significantly improve the validity and measurement practices in this research field.

The behavioral MIS literature suggests two main strategies to enhance methodological rigor in research. The first strategy, grounded in theoretical considerations, advocates for precise and uniform definitions of variables' theoretical properties to predicting and explaining causal relationships between them (Luft and Shields, 2003; MacKenzie *et al.*, 2011; Podsakoff *et al.*, 2016). A robust conceptual definition should precisely capture the essential properties that are common across occurrences of the phenomenon while distinguishing features unique to it (Luft and Shields, 2003). Such precision clarifies the concepts' intended meaning and prevents the misapplication of a term to disparate phenomena (Podsakoff *et al.*, 2016; Sartori, 1984). Therefore, theories and variables must be meticulously adapted to the unique aspects of the research subject.

In line with this strategy, various scholars have underlined the necessity of precise conceptualizations of non-/compliance study variables. For example, Chen *et al.* (2021) and Liang *et al.* (2023) stressed the importance of clearly defining the dependent variable, ISP non-/compliance behaviors. Similarly, Johnston *et al.* (2015) proposed a refined version of the PMT with variable properties customized to better suit the noncompliance context.

Karjalainen *et al.* (2019) underscored the need for a nuanced understanding of the evolving motivations and reasons behind employees' noncompliance because this makes conceptualizations better correspond to the studied reality. Hence, this line of research argues that methodological rigor can be improved by accurately specifying the theoretical properties of variables, tailored to the ISP non-/compliance context.

Differing from the first strategy, the second one takes the theoretical properties of variables as given and instead concentrates on their effective operationalization into questionnaire items (MacKenzie *et al.*, 2011). This necessitates that measurement tools not only undergo rigorous content validity checks but also be made relevant to the practical context to obtain useful results. Items that are ambiguous or contain unclear terminology should be clarified to guarantee clear understanding by respondents. Furthermore, items with complex sentence structures should be rephrased for greater specificity and conciseness (MacKenzie *et al.*, 2011).

Research has also stressed the importance of understanding the particular context in which respondents are situated. As effectively put by Desimone and Le Floch (2004, p. 4), "An important aspect of validity is that the respondent has a similar understanding of the questions as the survey designer; that the questions do not omit or misinterpret major ideas or miss important aspects of the phenomena being examined." And, in line with this, Siponen and Vance (2014) highlighted the importance of developing measurement items tailored to the intended respondents' organizational context to minimize the risk of measurement errors and to increase to possibility for researchers to draw correct conclusions about cause-and-effect relationships between variables. They also stressed the importance of testing and validating measurement instruments with target populations before the actual study. Arguably, neglecting this step could lead to an increased risk of misinterpretation, resulting in measurement items that only partially capture the intended theoretical property, capture content that does not correspond to the intended property, and/or capture several properties, some of which may not be in line with the theoretical definition (cf. Luft and Shields, 2003; see also Karlsson *et al.*, 2017; and *Li et al.*, 2021; for examples of non-/compliance research inspired by this strategy).

As will evident below, our interview study with respondents adds to the above-described stream of literature by providing in-depth insights into various types of respondent interpretations of measurement items. Before going into details, however, we shall briefly describe how we have collected and analyzed the empirical data.

3. Method

3.1 Selection of variables – perceived severity and attitude

This study analyzes the variables "Perceived Severity" from PMT and "Attitude" from TPB. Both theories have played central roles in prior studies on ISP non-/compliance research methodology, as evidenced by those conducted by Cram *et al.* (2019), Gerdin *et al.* (2023), Haag *et al.* (2021), Johnston *et al.* (2015), Mou *et al.* (2022) and Sommestad *et al.* (2015).

Guided by our research aim to analyze respondents' interpretations of questionnaire measurement instruments, we targeted variables with different levels of specificity in their definitions of theorical properties. The variable Perceived Severity has a high level of specificity and depict the perceived consequences of an information security threat for the individual and/or the organization (Gerdin *et al.*, 2021; Hooper *et al.*, 2020; Sommestad *et al.*, 2015). Conversely, the Attitude variable has a lower level of specificity when it comes to its theoretical property as per its variable definition. That is, while Attitude typically refers to one core property – attitude toward engaging in a specified behavior – the way in which authors define and measure this variable is very generic and does not provide any

information about the motive behind the attitude. In fact, a closer look at measurement items suggests very different motives. For example, Rajab and Eydgahi (2019) and Aurigemma and Mattson (2019) used measurement items implying that individuals' attitude can stem from their beliefs about the effectiveness of the prescribed behavior (cf. Response efficacy from PMT), whereas Ifinedo (2012) and Jalali *et al.* (2020) used items suggesting that individuals' attitudes stem from the potential benefits of following the prescribed behavior (cf. Response cost from PMT).

3.2 Data collection

We conducted semi-structured (Silverman, 2020) interviews with 17 professionals from Swedish public sector organizations of which 13 worked in municipal home care, 3 worked in the Swedish Transport Agency and 1 in the Agency of Digital Government. To ensure that the respondents could provide valuable insights based on their firsthand experiences (Silverman, 2020), all respondents selected handled classified information and were required to adhere to an information security policy in their respective organizations.

The selection of questionnaire items was based on previous studies, which have identified the abovementioned inconsistences in variable conceptualization and operationalization in the literature (Gerdin *et al.*, 2021; Sommestad *et al.*, 2015). For example, regarding the variable Perceived Severity, we incorporated a mix of items specifically related to whom the consequences of noncompliance were directed toward. Regarding the variable Attitude, our approach involved incorporating a diverse array of items each selected to capture variations in the motives underlying feelings and thoughts toward a given behavior. This served a dual purpose. First, it aimed to elucidate how, and to what extent, variations in wording influenced interpretations. This approach provided insights into the impact of different expressions on respondents' understanding and responses. Second, it aimed to mirror the reality of non-/compliance research, where there is a myriad of measurements used. Table 1 displays the full list of items, note that the items were translated from English to Swedish.

The interviewees were asked to think out loud and explain how they interpret the question, how they would have answered the question using a five-point Likert scale and the reason for choosing the specific number. The Likert scale was used to mimic quantitative research methods so as to make it possible for us to understand if and, if so, how different interpretations among the respondents cause different grading. When necessary, probing follow-up questions were asked. This gave us the opportunity to investigate evidence of the nature of the phenomena in question, including understanding contexts and situations in which the evidence emerges (Silverman, 2021). All items were taken from peer-reviewed articles published in academic journals.

Sixteen interviews were conducted online using Zoom or Microsoft Teams while one was conducted in person. For the first seven interviews, two researchers were present at the interviews, both of whom were familiar with the interview protocol. While one researcher was responsible for following the interview protocol the other was tasked to ask follow-up questions. This approach was used for the purpose of ensuring the researchers shared the understanding of the protocol. The subsequent ten interviews were conducted by one researcher, as the overall process was manageable by one researcher.

Each interview lasted about 1 h. We adopted an iterative approach whereby the interview protocol was modified (if needed) after each interview. During the first four interviews, minor modifications were made, including adjustments related to the translation of certain questions. The order in which the questions were posed was also changed slightly as respondents expressed that some questions seemed quite similar, and this modification

"Perceived Severity" items	
PS1	"Threats to the security of my organizations information are harmful" (Ifinedo, 2012)
PS2	"If my computerized data were temporarily not available, serious information security problems would result" (Barlette *et al.*, 2015)
PS3	"If my work device were infected by malware, it would be severe" (Blythe and Coventry, 2018)
PS4	"In terms of information security violations, attacks on my organization's information and information systems are severe" (Posey *et al.*, 2015)
PS5	"If my password was stolen, the consequences would be severe" (Johnston *et al.*, 2015)
PS6	"Threats to the security of my organization's information and information systems are severe" (Ma, 2022; Posey *et al.*, 2015)
PS7	"An information security breach in my organization would be a serious problem for my organization." (Siponen *et al.*, 2014)
PS8	"An information security breach in my organization would be a serious problem for me" (Vance *et al.*, 2012)
"Attitude" items	
A1	"I believe that it is useful for our organization to enforce its information security policies, practices, and technologies" (Jalali *et al.*, 2020; Hu *et al.*, 2012)
A2	"To me, complying with the requirements of my organizations information security policy/ measure is necessary" (Aigbefo *et al.*, 2022)
A3	"Following the organization's information system security policy is beneficial" (Ifinedo, 2012)
A4	"To adhere to the information security policies of my institution is an excellent idea" (Hina *et al.*, 2019)
A5	"The preventive measures available to me to stop people from gaining access to [my organization's] information are adequate" (Posey *et al.*, 2015)
A6	"My role/task is very beneficial to my company" (Kim and Kim, 2017)
A7	"Mandating [the] change of password is a good idea" (Bélanger *et al.*, 2017)

Table 1.
List of items and original studies

Notes: PS = perceived severity; A = attitude
Source: Created by authors

aimed to prevent their answers from being influenced by their previous responses. In the subsequent 13 interviews, no further changes were made.

3.3 Method for analysis

The coding process comprised of three steps and was conducted by two of the authors. Throughout the process, we conducted several joint coding workshops to make sure that we understood the respondents' interpretations similarly. In the later stages, the third author joined the discussions, contributing to the comprehensive analysis of the overall findings.

First, we transcribed, compiled and coded each interview separately. During the transcription and the subsequent readings, we identified numerous interesting words, phrases, terms and concepts, which we deemed important to understand the interpretation offered by the respondents (Bazeley, 2013).

Second, we re-read all transcripts and combined words, phrases, terms and concepts from each interview into categories representing similar ideas shared in the interpretation of each item among the respondents. This process consisted of comparisons of transcripts and subsequent analysis to over time detect patterns shared by the transcripts (Bazeley, 2013). This resulted in a set of categories representing different variable property-interpretations among the respondents.

Third, we formulated overarching labels that subsumed the previously identified categories on a more abstract level, representing a more aggregated analytical dimension of each category (Bazeley, 2013). This process involved all three authors. The focus here was to

see how well our overarching labels compared with the conceptualization of each variable as per the non-/compliance literature. To ensure confidence in our identified categories and subsequent labels, we continuously worked back and forth with the material, literature and the emerging tables. This process resulted in four types of overarching types of respondent interpretations, each of which will be described next. Note that preliminary results from the analysis were presented at the Human Aspects of Information Security and Assurance (HAISA, 2023) conference. The coding process thus involved two significant phases: an initial phase based on seven interviews, which was conducted before the conference, followed by a second phase that included an additional ten interviews. The latter phase was, among other things, based on the feedback received from the conference reviewers.

4. Results

We set out to investigate how the respondents interpreted questionnaire measurement items and whether their interpretations were in line with the theoretical conceptualization of the variable as suggested in ISP non-/compliance research literature (see Section 3.1).

Overall, we found four principal ways in which respondents interpretated measurement items, each implying more or less alignment with the intended theoretical properties of the two variables examined. These are the following:

- *Property contextualization*: Respondents make sense of vaguely formulated words or concepts used in the measurement items by relating them to their specific work context. Such property contextualization cause variation in interpretations among respondents, but their interpretations are still within the intended conceptual boundaries of the variable.
- *Property extension:* Respondents extend variable properties based on their understanding of their specific work context. These extended properties are close to, but still separate from, the theoretical conceptualization of the variable.
- *Property alteration:* Respondents alter the overall theoretical meaning of a variable, which make their interpretations more similar to other behavioral variables than the indented one.
- *Property oscillation:* Respondents oscillates between two or more logically reasonable responses for the same item ("one the one hand, [. . .]. On the other hand," [. . .]). These responses may align with the conceptualization of the variable, deviate from it or combine responses from within and outside of the conceptualization.

Below, the four types of respondent interpretations will be described separately for analytical reasons. In practice, however, they can overlap.

4.1 Property contextualization

This type of respondent interpretation refers to situations when they understand the general meaning of a measurement item. Because of unclear wordings, however, respondents seek to make sense of them, which causes variation in interpretations as respondents make sense of them by relating them to their specific work context. For example, as explained by one respondent, the statement" If my computerized data were temporarily not available, serious information security problems would result" (item PS 2) was not clear because "it depends on how temporary the break is. If it is a couple hours, then it is not a problem but if it is longer than that, there is definitely a problem." As a result of this unclarity, some respondents answered the question from a worst-case-scenario perspective – a long period of unavailability – while others had a normal "run-of-the-mill" scenario in mind where there

was just a very short interruption (see Table 2 for illustrative examples). These differences in interpretation made them rate the statement substantially differently on the five-point Likert scale.

Similarly, for the variable Attitude, respondents substituted measurement item words like "enforce" (item A 1) with "useful" and "necessary" with "beneficial" to align them more closely with their own work context. When asked about the rationale behind their reinterpretations, respondents referred to their organizational context, emphasizing sentiments such as "even if we desired to, we cannot compel our employees to adhere to that," or "I disagree with the notion of strongarming people to behave in a certain manner."

Property contextualization was found for both variables investigated. Table 2 displays more illustrative examples of this type of respondent interpretation.

4.2 Property extension

As mentioned above, respondent property extension refers to situations when respondents extend variable properties so that they better align with their specific work context. For example, for all measurement items related to Perceived Severity, all the respondents (working in municipalities) took the property "consequences" to refer to consequences for *the citizen/clients*, the people they serve in their role as a public organization (see Table 3 for illustrative examples). This is an extension from the conceptualization in the theories used in non-/compliance research, which typically refers to consequences related to either the *organization* or the *individual professional*. The reference to clients/citizens, however, is natural for a civil servant as privacy legislation (e.g. GDPR) is strict as it concerns clients in public services.

Property extension was only identified for the Perceived Severity items, but the frequency of this type of respondent interpretation was high.

4.3 Property alteration

This type of respondent interpretation refers to situations when they alter the intended theoretical property to the extent that it refers to another behavioral variable used in non-/compliance research. For example, one respondent's interpretation of the statement "An information security breach in my organization would be a serious problem for me" (item PS 8) was "These types of threats occur on a daily basis." That is, while the intended property of the measurement item was about the perceived *consequences* of a security breach, the respondent interpretation referred the *probability* of it to happen – a variable referred to as Perceived vulnerability in the ISP non-/compliance literature (see Table 5 for illustrative examples).

Similar examples of respondent property alteration could be found the Attitude variable. Here, the measurement items sought to capture feelings toward a prescribed information security behavior. However, when answering the questionnaire item, some respondents referred to the *ease or difficulty of performing the behavior of interest*, which is another commonly used variable in ISP non-/compliance literature referred to as Perceived behavior control. Table 5 provides further illustrative examples of this type of respondent interpretations.

4.4 Property oscillation

This type of respondent interpretation refers to situations where they oscillate between two or more incompatible interpretations of a measurement item. The measurement problem being such oscillations not only makes it difficult for respondents to provide *one* mark on a Likert scale but also to understand what such mark stands for.

Measurement item(s)	Interpretation (respondent)	Theory–interpretation disagreement
"If my computerized data were temporarily not available, serious information security problems would result" (Barlette *et al.*, 2015)	For me it depends on how temporary the break is. If it is a couple hours, then it is not a problem but if it is longer than that, well there is definitely a problem then. (Respondent 4, Item PS2)	In the respondent's context, the timeframe is important for the seriousness of threat, but this is unspecified in the questionnaire item. (Perceived Severity)
"An information security breach in my organization would be a serious problem for me" (Vance *et al.*, 2012)	It depends on what level in the organization the breach happens. (Respondent 4, item PS8)	The organizational level is important for the seriousness but is unspecified. (Perceived Severity and Attitude)
"My role/task is very beneficial to my company" (Kim and Kim, 2017)	I am very important in my unit, but not as important in the overall project, so it depends. (Respondent 9, Item A6)	
"Following the organization's information system security policy is beneficial" (Ifinedo, 2012)	I would say that it would be more relevant to use the word necessary instead of beneficial [[. . .]] I think the question should be rephrased (Respondent 15, Item A3)	Change connotation of word/s to fit narrative/ context (Attitude)

Note: Here, as in Tables 3–5, respondent quotes have been condensed due to space limitations
Source: Created by authors

Table 2.
Illustrative examples respondent property contextualization

Table 3.
Illustrative examples respondent property extension

Measurement item(s)	Interpretation (respondent)	Theory–interpretation disagreement
"If my password was stolen, the consequences would be severe" (Johnston *et al.*, 2015) "If my work device were infected by malware, it would be severe" (Blythe and Coventry, 2018)	For us who work within the health-care sector, everything is always serious. In the end, the clients can die or be injured. (Respondent 7 – Item PS5) Our mission is to always look out for the best interests of the citizens and care citizen/clients. So that nothing can happen to them, and that is what we must try to avoid. (Respondent 3 – Item PS3)	Respondents relate consequences to the citizens/clients rather than to the individual professional or the organization, which the statements implicitly suggest (Perceived Severity)

Source: Created by authors

Measurement item(s)	Interpretation (respondent)	Theory–interpretation disagreement
"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, it would be severe" (Blythe and Coventry, 2018)	It could be a school shooter and create chaos at the school, or perhaps share suicide clips to other students. (Respondent 2 – Item PS8) These types of threats occur on a daily basis. (Respondent 4 – item PS3)	Respondent refers to threats that are not related to information security Vulnerability and probability are theoretically conceived in the variable Perceived Vulnerability (PMT), not Perceived Severity
"To me, complying with the requirements of my organizations information security policy/measure is necessary" (Aigbefo *et al.*, 2022) "To adhere to the information security policies of my institution is an excellent idea" (Hina *et al.*, 2019)	My question is if it is even possible to comply with the policy? [. . .] I feel like the organization don't provide us the right conditions to do so. . . (Respondent 11 – Item A2) I don't think that the policy is good enough, nor possible to follow at the moment. (Respondent 11 – Item A4)	Ease or difficulty of performing the behavior of interest is theoretically conceived in the variable Perceived Behavior Control (TPB), not Attitude

Source: Created by authors

Table 4. Illustrative examples respondent property alteration

Table 5.
Illustrative examples respondent property oscillation

Measurement item(s)	Interpretation (respondent)	Theory–interpretation disagreement
"Following the organization's information system security policy is beneficial" (Ifinedo, 2012)	That depends, beneficial for whom? From a security perspective it is surely beneficial, but from the individual's perspective it can be terribly complicated to follow it in your daily work. (Respondent 11 – Item A3)	Different interpretations of the object of the statement – beneficial for the individual or the organization? (Attitude)
"Mandating [the] change of password is a good idea" (Bélanger *et al.*, 2017)	"Yes and no, I have two separate answers for this question [. . .] I, who have time and is technical sound can do it, but most of our workers rarely use the computers and don't have the knowledge to do it. . . (Respondent 3 - Item A7)	Easy for me and I can do it, but not for other coworkers whom I also consider in my answer (Attitude)
"If my computerized data were temporarily not available, serious information security problems would result" (Barlette *et al.*, 2015)	The word temporarily makes it difficult to interpret this question. . . What does it mean, five days or an hour (Respondent 2 – Item PS2)	In the respondent's context, the timeframe is important for the seriousness of threat, but this is unspecified in the questionnaire item. (Perceived Severity)

Source: Created by authors

For example, analyzing the statement "Following the organization's information system security policy is beneficial" (item A 3) one respondent explained that "it depends, beneficial for whom? From a security perspective it is surely beneficial, but from the individual's perspective it can be terribly complicated to follow it in your daily work."

Similarly, when considering how to grade a measurement item stating that "Mandating [the] change of password is a good idea" (item A 7), another respondent argued that:

> Yes, this is very important to do to counteract security problems in the case passwords have been leaked. However, there is also a risk associated with changing passwords often as people then tend to create short and insecure ones. [Hence], it is not always a good idea to mandate changes of passwords.

Table 5 provides further illustrative examples of this type of respondent interpretations.

5. Discussion

This study investigates how well respondents' interpretations of variables measurement items correspond with the theoretical definitions of them as well as the characteristics of any discrepancies. Overall, we found four general types of respondent interpretations, which affects the validity of the questionnaire measurement instruments in different ways.

Respondent property *contextualization* implies that while respondents understand the general meaning of measurement items, unclear wordings cause variations in interpretations as respondents seek to make sense by relating them to their own specific work context. On one hand, if not dealt with, this type of vague wordings may introduce noise in measurements, causing unnecessary differences in respondent interpretations of crucial theoretical properties. On the other hand, however, if these differences in interpretations are understood and accounted for by the researcher, we could potentially use this to draw more fine-tuned conclusions about ISP non-/compliance. For instance, we found that the timeframe and the level of the analysis (individual, departmental, organizational or external/supra-organizational) affected interpretations and ratings among respondents. Acknowledging this could provide a more nuanced understanding of the conceptual range and boundaries of a variable (MacKenzie *et al.*, 2011; Podsakoff *et al.*, 2016).

While different interpretations due to vague wordings may not be possible to eliminate, our findings indicate that unnecessary variation in respondent interpretations can be significantly reduced by measurement items being more precise in their wording to about key theoretical properties of variables. Our findings also stress the importance of closely adhering to Siponen and Vance, 2014 recommendation of contextualizing measurement instruments to better align with the respondents' work reality.

Respondent property *extension* refers to situations where theoretical properties are extended by respondents to better align with their specific work context. In similarity with the just-described type of respondent interpretation, this type of respondent interpretation can imply noisy measurements as such properties are close to, but still separate from, the theoretical conceptualizations of variables. [1] However, it can also be argued that this type of property extension offers an opportunity for researchers to increase the conceptual range and boundaries of a variable (Podsakoff *et al.*, 2016). Again, our study revealed that respondents stressed the importance of considering the consequences of security threats for their clients/citizens, a category previously overlooked in extant non-/compliance research whose dominating focus has been on the consequences of organizations and individuals (cf. Gerdin *et al.*, 2021; Sommestad *et al.*, 2014, 2015). And, because empirical evidence indicates that the effect on intention to comply with ISPs can vary depending on whether the focus is on the

organization or the individual (Sommestad *et al.*, 2015), future research should explore if similar effects can be found for clients/citizens or other external stakeholders.

As detailed above, our study also identifies a type of interpretation of measurement items referred to as respondent property *alteration*. Arguably, this is an important, yet largely unacknowledged, source of measurement error as respondents' interpretations implies that intended theoretical properties of variables are *replaced* by other properties consistent with other behavioral variables within the same theory. Hence, this type of interpretation has the potential to lead to invalid conclusions, particularly if it is widespread among respondents. After all, it implies that measurement items capture content that does not correspond with the intended property, and/or capture several properties, some of which are not in line with the conceptual definition (Luft and Shields, 2003; MacKenzie *et al.*, 2011).

Unlike the two former types of respondent interpretations (property contextualization and extension, respectively), the measurement error caused by this one cannot be addressed by more precise wording of properties and/or by aligning measurement items to the specific work context of respondents. After all, respondent property alteration typically arises because respondents simply misinterpret the intended theoretical property. This said, however, we stress the importance of adhering to sound guidelines for the operationalization of variables in future research so as to minimize the risk of such misunderstandings (cf. MacKenzie *et al.*, 2011; Podsakoff *et al.*, 2016; Siponen and Vance, 2014.

Finally, we identify a type of measurement item interpretation referred to as respondent property *oscillation*. Here, noisy measurements arise because theoretical properties allow for incompatible interpretations that leaves respondents hesitating between two or more logically reasonable responses. Arguably, also this type of "back-and-forth dynamic" is challenging from a measurement point of view. For example, it could be that respondents oscillate between marking 1 or 2 and 4 or 5 on the Likert scale depending on different pros and cons of the alternatives considered. But because self-reported measures require only one answer, there is no way of knowing the reasoning behind the final response. It could also be the case that respondents opt for a "middle-ground answer" (i.e. marking 3 on the Likert scale) based on the argument that this represents a neutral stance between the two incompatible interpretations. In both cases, we can expect noisy measurements as well as limited insights into respondents' viewpoints on the theoretical properties in question.

6. Conclusions and contributions

This study investigates how well respondents' interpretations of variable measurement instruments correspond to their theoretical definitions as well as the characteristics of any discrepancies between these. Overall, we conclude that:

- there are not only individual differences in interpretations but also, and more importantly, recurring patterns across respondents; and
- specifically, we found four principal ways in which respondents interpretated measurement items – referred to as respondent property *contextualization, extension, alteration* and *oscillation* – each implying more or less (dis)alignment with the intended theoretical properties of the two variables examined.

This study not only contributes to the emerging literature on variable measurement and validation procedures within the ISP non-/compliance literature (Cram *et al.*, 2019; Karlsson *et al.*, 2017; Siponen and Vance, 2014) but also to the more general MIS literature on this topic (Mackenzie *et al.*, 2011; Podsakoff *et al.*, 2016). It does so by adopting a rarely used research method in this research area – in-depth qualitative interviews – a method that enabled us to identify four important, yet largely unacknowledged, sources of

measurement error in questionnaire measurement instruments. Arguably, these in-depth insights into the respondents' perspective, and how this affects the interpretation of questionnaire measurement items, is difficult, even impossible, to capture by using conventional (statistics-based) methods for evaluating measurement validity typically used in the ISP non-/compliance literature. Hence, the potential benefits of this study are substantial, as the insights offered are valuable for further improving questionnaire measurement items in this rapidly expanding research area.

Note

1. Note, however, the possibility to identify respondent property extension largely depends on the level of specificity in defining the characteristics and properties of variables (cf. Section 3.1 above). Generally speaking, a more precise conceptualization, as is the case for the Perceived Severity variable, facilitates the identification of this type of respondent interpretations, whereas a more general conceptualization, being the case for the Attitude variable, works in the opposite direction (see also Luft and Shields, 2003; MacKenzie *et al.*, 2011; Podsakoff *et al.*, 2016).

References

Aigbefo, Q.A., Blount, Y. and Marrone, M. (2022), "The influence of hardiness and habit on security behaviour intention", *Behaviour and Information Technology*, Vol. 41 No. 6, pp. 1151-1170.

Aurigemma, S. and Mattson, T. (2019), "Generally speaking, context matters: making the case for a change from universal to particular ISP research", *Journal of the Association for Information Systems*, Vol. 20 No. 12, p. 7.

Barlette, Y., Gundolf, K. and Jaouen, A. (2015), "Toward a better understanding of SMB CEOs' information security behavior: insights from threat or coping appraisal", *Journal of Intelligence Studies in Business*, Vol. 5 No. 1, pp. 5-17.

Bazeley, P. (2013),*Qualitative Data Analysis Practical Strategies*, 2nd ed., Sage, London.

Bélanger, F., Collignon, S., Enget, K. and Negangard, E. (2017), "Determinants of early conformance with information security policies", *Information and Management*, Vol. 54 No. 7, pp. 887-901.

Bennett, C., Khangura, S., Brehaut, J.C., Graham, I.D., Moher, D., Potter, B.K. and M. Grimshaw, J. (2011), "Reporting guidelines for survey research: an analysis of published guidance and reporting practices", *PLoS Medicine*, Vol. 8 No. 8, p. e1001069.

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

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. and Polak, P. (2015), "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors", *MIS Quarterly*, Vol. 39 No. 4, pp. 837-864.

Boudreau, M.C., Gefen, D. and Straub, D.W. (2001), "Validation in information systems research: a state-of-the-art assessment", *MIS Quarterly*, Vol. 25 No. 1, pp. 1-16.

Chen, Y., Galletta, D.F., Lowry, P.B., Luo, X., Moody, G.D. and Willison, R. (2021), "Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model", *Information Systems Research*, Vol. 32 No. 3, pp. 1043-1065.

Cram, W.A., Proudfoot, J.G. and D'arcy, J. (2017), "Organizational information security policies: a review and research framework", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 605-641.

Cram, W.A., D'arcy, J. and Proudfoot, J.G. (2019), "Seeing the Forest and the trees: a meta-analysis of the antecedents to information security policy compliance", *MIS Quarterly*, Vol. 43 No. 2, pp. 525-554.

D'Arcy, J. and Lowry, P.B. (2019), "Cognitive-affective drivers of employees' daily compliance with information security policies: a multilevel, longitudinal study", *Information Systems Journal*, Vol. 29 No. 1, pp. 43-69.

Desimone, L.M. and Le Floch, K.C. (2004), "Are we asking the right questions? Using cognitive interviews to improve surveys in education research", *Educational Evaluation and Policy Analysis*, Vol. 26 No. 1, pp. 1-22.

Gerdin, M., Grönlund, Å. and Kolkowska, E. (2021), "Use of protection motivation theory in non-compliance research".

Gerdin, M., Grönlund, Å. and Kolkowska, E. (2023), "What goes around comes around; effects of unclear questionnaire items in information security research", *International Symposium on Human Aspects of Information Security and Assurance*, Springer Nature Switzerland, Cham, pp. 470-481.

Haag, S., Siponen, M. and Liu, F. (2021), "Protection motivation theory in information systems security research: a review of the past and a road map for the future", *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, Vol. 52 No. 2, pp. 25-67.

Hina, S., Selvam, D.D.D.P. and 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 and Security*, Vol. 87, p. 101594.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012), "Managing employee compliance with information security policies: the critical role of top management and organizational culture", *Decision Sciences*, Vol. 43 No. 4, pp. 615-660.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers and Security*, Vol. 31 No. 1, pp. 83-95.

Jalali, M.S., Bruckes, M., Westmattelmann, D. and Schewe, G. (2020), "Why employees (still) click on phishing links: investigation in hospitals", *Journal of Medical Internet Research*, Vol. 22 No. 1, p. e16775.

Johnston, A.C., Warkentin, M. and Siponen, M. (2015), "An enhanced fear appeal rhetorical framework", *MIS Quarterly*, Vol. 39 No. 1, pp. 113-134.

Karjalainen, M., Sarker, S. and Siponen, M. (2019), "Toward a theory of information systems security behaviors of organizational employees: a dialectical process perspective", *Information Systems Research*, Vol. 30 No. 2, pp. 687-704.

Karlsson, F., Karlsson, M. and Åström, J. (2017), "Measuring employees' compliance – the importance of value pluralism", *Information and Computer Security*, Vol. 25 No. 3, pp. 279-299.

Khan, N.F., Yaqoob, A., Khan, M.S. and Ikram, N. (2022), "The cybersecurity behavioral research: a tertiary study", *Computers and Security*, Vol. 120, p. 102826.

Kim, S.S. and Kim, Y.J. (2017), "The effect of compliance knowledge and compliance support systems on information security compliance behavior", *Journal of Knowledge Management*, Vol. 21 No. 4, pp. 986-1010.

Li, H., Luo, X.R. and Chen, Y. (2021), "Understanding information security policy violation from a situational action perspective", *Journal of the Association for Information Systems*, Vol. 22 No. 3, pp. 7398-7772.

Liang, N., Hirschheim, R., Luo, X. and Hollingsworth, H. (2023), "Identifying the idiosyncrasies of behavioral information security discourse and proposing future research directions: a foucauldian perspective", *Journal of Information Technology*, Vol. 38 No. 4, pp. 382-415.

Luft, J. and Shields, M.D. (2003), "Mapping management accounting: graphics and guidelines for theory-consistent empirical research", *Accounting, Organizations and Society*, Vol. 28 Nos 2/3, pp. 169-249.

Ma, X. (2022), "Is professionals' information security behaviors in Chinese IT organizations for information security protection", *Information Processing and Management*, Vol. 59 No. 1, p. 102744.

MacKenzie, S.B., Podsakoff, P.M. and Podsakoff, N.P. (2011), "Variable measurement and validation procedures in MIS and behavioral research: integrating new and existing techniques", *MIS Quarterly*, Vol. 35 No. 2, pp. 293-334.

Moody, G.D., Siponen, M. and Pahnila, S. (2018), "Toward a unified model of information security policy compliance", *MIS Quarterly*, Vol. 42 No. 1, pp. 285-A22.

Mou, J., Cohen, J.F., Bhattacherjee, A. and Kim, J. (2022), "A test of protection motivation theory in the information security literature: a meta-analytic structural equation modeling approach", *Journal of the Association for Information Systems*, Vol. 23 No. 1, pp. 196-236.

Podsakoff, P.M., MacKenzie, S.B. and Podsakoff, N.P. (2016), "Recommendations for creating better concept definitions in the organizational, behavioral, and social sciences", *Organizational Research Methods*, Vol. 19 No. 2, pp. 159-203.

Posey, C., Roberts, T.L. and Lowry, P.B. (2015), "The impact of organizational commitment on insiders' motivation to protect organizational information assets", *Journal of Management Information Systems*, Vol. 32 No. 4, pp. 179-214.

Rajab, M. and Eydgahi, A. (2019), "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education", *Computers and Security*, Vol. 80, pp. 211-223.

Sartori, G. (1984), "Guidelines for concept analysis", in Sartori G. (Ed.), *Social Science Concepts: A Systematic Analysis*, Sage Publications, Beverly Hills, CA, pp. 15-85.

Silverman, D. (2020), *Interpreting Qualitative Data*, 6th ed., SAGE, UK.

Silverman, D. (2021), *Qualitative Research*, 5th ed., SAGE, UK.

Simon, T. (2021), "Revolution and stability in the study of the human factor in the security of information systems field: a systematic literature review over 30 years of publication", In 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), *IEEE*, pp. 1-8.

Siponen, M. and Vance, A. (2014), "Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations", *European Journal of Information Systems*, Vol. 23 No. 3, pp. 289-305.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2014), "Employees' adherence to information security policies: an exploratory field study", *Information and Management*, Vol. 51 No. 2, pp. 217-224.

Sommestad, T., Karlzén, H. and Hallberg, J. (2015), "The sufficiency of the theory of planned behavior for explaining information security policy compliance", *Information and Computer Security*, Vol. 23 No. 2, pp. 200-217.

Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014), "Variables influencing information security policy compliance: a systematic review of quantitative studies", *Information Management and Computer Security*, Vol. 22 No. 1, pp. 42-75.

Straub, D.W. (1989), "Validating instruments in MIS research", *MIS Quarterly*, Vol. 13 No. 2, pp. 147-169.

Straub, D.W., Jr (1990), "Effective IS security: an empirical study", *Information Systems Research*, Vol. 1 No. 3, pp. 255-276.

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating is security compliance: insights from habit and protection motivation theory", *Information and Management*, Vol. 49 Nos 3/4, pp. 190-198.

Wikman, A. (2006), "Reliability, validity and true values in surveys", *Social Indicators Research*, Vol. 78 No. 1, pp. 85-110.

Further reading

Burns, A.J., Posey, C., Roberts, T.L. and Lowry, P.B. (2017), "Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals", *Computers in Human Behavior*, Vol. 68, pp. 190-209.

Hooper, V. and Blunt, C. (2020), "Factors influencing the information security behaviour of IT employees", *Behaviour and Information Technology*, Vol. 39 No. 8, pp. 862-874.

Prentice-Dunn, S. and Rogers, R.W. (1986), "Protection motivation theory and preventive health: beyond the health belief model", *Health Education Research*, Vol. 1 No. 3, pp. 153-161.

Rogers, R.W. (1975), "A protection motivation theory of fear appeals and attitude change1", *The Journal of Psychology*, Vol. 91 No. 1, pp. 93-114.

Rogers, R.W. (1983), "Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation", *Social Psychology: A Source Book*, Guilford Press, New York, pp. 153-176.

Vrhovec, S. and Mihelič, A. (2021), "Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation", *Computers and Security*, Vol. 106, p. 102309.

Corresponding author

Marcus Gerdin can be contacted at: Marcus.gerdin@oru.se