MEASURING COMPLIANCE WITH SPECIFIC POLICY CONTENTS – THE SRPC- AND SRPCC-SCALES FOR A MORE DETAILED MEASUREMENT OF POSITIVE POLICY COMPLIANCE

Research in Progress

Kurowski, Sebastian, Fraunhofer Institute of Industrial Engineering, Competence Team Identity Management, Stuttgart, Germany, sebastian.kurowsk@iao.fraunhofer.de

Abstract

Research on information security policy compliance provides insights on the factors that facilitate security related human behaviour. Since humans provide the end of every technological use chain, this research provides an important building block of every organizational security architecture. Research on this topic can be divided into research on policy compliant behaviour (positive policy compliance) and research on policy deviant behaviour (negative policy compliance). However, a previous meta-study that was the first to test available measurement instruments of positive policy compliance for response biases remained inconclusive on the truthfulness of self-reported policy compliance. This contribution provides a new measurement instrument that builds upon the scenario-based questioning approach found in most negative policy compliance research, while enabling scenario-independent measurement of positive policy compliance and provided response consistency. The instrument was validated by conducting a pre-test (n = 8) in a research department and yields a promising internal validity with Cronbach alphas of .911 for the policy compliance instrument and .961 for the policy knowledge consistency instrument. The instrument is being applied in a larger survey that aims at determining the reliability of measured policy compliance of the instruments currently used in positive policy compliance research.

Keywords: Policy Compliance, Information Security, Human Behaviour, Response Bias

1 Introduction

Understanding human adherence or deviance to information security policies is a key element for future security architectures. Human behaviour is an important antecedent for attacks on organization and private information systems (Johnston et al., 2016), with 34.8% of german corporations reporting social engineering as a main cause of industry espionage (Corporate Trust, 2014), and human error being one of three root causes for data breaches (Ponemon Institute, 2016). Therefore, several studies both on factors of policy deviance (in the following referred to as negative policy compliance) (Bansal and Shin, 2016; Chu et al., 2015; D'Arcy et al., 2014; Shepherd and Mejias, 2016; Siponen et al., 2014; Vance et al., 2014; Vance and Siponen, 2012) and on factors of policy compliance (in the following referred to as positive policy compliance) have been conducted. Most of the surveys on negative policy compliance employ scenario-based questioning. These minimally invasive measurement method does not require the individual to admit a bad truth, but rather measures the familiarity and identification of an individual with a certain scenario. Positive policy compliance on the other side, mostly employs self-reporting questionnaires. Such questionnaires can be easily scaled, e.g. by using online surveys, and provide the interviewees with the flexibility to respond to the questionnaire when they wish to. Also, the anonymity of self-reporting questionnaires rules out the interviewer as a possible source of influence on the interviewee. As (Philip S. Brenner and DeLamater, 2016) put it: "it is relatively easier to admit a "bad" truth on a paper or computerized questionnaire than to a human interviewer" (Philip S. Brenner and DeLamater, 2016, p. 334).

Yet, this does not mean that the responses of self-reporting questionnaires are truthful. For instance, survey reports of church attendance and rates of exercise are found to be double the actual frequency, when self-reported (Philip S. Brenner and DeLamater, 2016; Philip S Brenner and DeLamater, 2016; Chase et al., 1983; Klesges et al., 1990; Rzewnicki et al., 2003). Current research on positive policy compliance largely indicates rather policy compliant individuals, with the mean self-reported policy compliance scoring in the upper quarter of the likert scales, and a variance that does not exceed the upper quarter of the likert scale (Kurowski and Dietrich, 2017). This however, contradicts the current research on positive policy compliance, since findings such as (Corporate Trust, 2014; Ponemon Institute, 2016) indicate policy deviant behaviour as a major cuase of data breaches. The quality of the studies on positive policy compliance can also be ruled out as an issue, since validity testing, defined and justified sample frames, sufficiently large response rates and partly estimations of non-response biases indicate a rather high quality of the existing body of knowledge (Malhotra and Grover, 1998; Sommestad et al., 2014).

The items that are used for capturing policy compliant behaviour are formulated in a rather general manner in the current literature. E.g. an item on policy compliant would ask whether an individual complies to the current information security policy. (Kurowski and Dietrich, 2017) however find, that responses to these rather general questions on policy compliance are likely to be either biased by social desirability, misjudgements or acquiescent response styles. Therefore this contribution introduces two scales that can be combined for a more detailed measurement of policy compliance. The scales address biases due to misjudgement, rooted in identity theory (Brenner et al., 2014; Philip S. Brenner and DeLamater, 2016). The scales are introduced throughout Section 3, which is followed by a brief validation in a small pretest throughout Section 4. Current ongoing research and shortcomings of the scales is discussed in Section 5. But first, a more detailed insight into the current body of indications of response biases in policy compliance, and the identity theory based causation of the biases is introduced in the next Section 2.

2 Response Biases in Self-Reporting Questionnaires

Response biases are often caused by dispositional factors of the interviewee (Crowne and Marlowe, 1960) and by the interview setting itself (Myers, 2009). The role of the interview setting is often neglected in self-reporting questionnaires, since interviewees with such questionnaires may remain

anonymous, and can provide their answers without any external pressure. Still, (Philip S. Brenner and DeLamater, 2016) find that self-administered (e.g. web-based) questionnaires may indicate substantial bias due to social desirable responses. Using the identity theory (Stryker, 1980), (Philip S. Brenner and DeLamater, 2016) postulate that behaviour is "[...] encouraged by identity prominence; in short, we tend to perform identities that we value (Brenner et al., 2014)" (Philip S. Brenner and DeLamater, 2016, p. 338), and that even if an individual fails to perform the desired behaviour due to given circumstances, he or she may take the opportunity to "[...] perform the identity by simply answering a survey question in the affirmative" (Philip S. Brenner and DeLamater, 2016, p. 338). Furthermore, (Morren et al., 2012) indicate that the item wording itself may contribute to acquiescent response sets, in which either overly positive, or responses at the extreme end of a likert-scale occur (Kemmelmeier, 2016). This observable effect is shown in (Morren et al., 2012) as moderated by the cultural background of the respondents.

Current positive policy compliance research was investigated by (Kurowski and Dietrich, 2017) regarding possible response biases. Since respondents of the surveys in the current body of knowledge can surely not be contacted due to anonymity reasons, they used the moderating influence of culture on response biases by analysing the mean self-reported policy compliance along with its standard deviation, and the cultural background of the surveyed sample. They observed, that the mean self-reported policy compliance indicated values in the upper quartile of the likert scale. Additionally, the variance indicated by the measurement in existing positive policy compliance research showed a variance smaller than 1 point on the used likert scale. They also found significant positive correlations between the individualism and power distance indices (Hofstede and Hofstede, 2005) of the sample, and the self-reported mean policy compliance. However, these correlations both contradicted existing state-of-the-art on cultural influences on policy compliance (Dols and Silvius, 2010) and state-of-the-art on response biases (Harzing, 2006) (Kurowski and Dietrich, 2017).

This shows, that statements on the verification, rather than validation of current positive policy compliance research can be inconclusive at best. If biases exist however, they are obviously not indicated by cultural traits that can be attributed to the whole sample. A possible bias that would only be measurable on an individual level is provided by (Philip S. Brenner and DeLamater, 2016). Using identity theory (Brenner et al., 2014) postulate that behaviour is "[...] encouraged by identity prominence; in short, we tend to perform identities that we value (Brenner et al., 2014)" (Philip S. Brenner and DeLamater, 2016, p. 338), and that even if an individual fails to perform the desired behaviour due to given circumstances, he or she may take the opportunity to "[...] perform the identity by simply answering a survey question in the affirmative" (Philip S. Brenner and DeLamater, 2016, p. 338). In order to find out whether such individual conditions lead to a bias in self-reported policy compliance, a measurement instrument is introduced within the next section that goes beyond the rather general itemsets used in current positive policy compliance research.

A more differentiated view on policy compliance is provided by more detailed, and policy-content focused analysis of the responses. This way, we argue that the resulting values might be less subject to response biases due to individual identity prominence.

3 Measuring positive information security policy compliance

The previous section indicated that current research on positive information security policy compliance may be subject to acquiescent response styles. Especially striking is the significant correlation between individualism and mean self-reported policy compliance in the current empirical studies on the subject that hints towards acquiescent response styles biasing current results on information security policy compliance (Kurowski and Dietrich, 2017). Contributions on negative information security policy compliance often use scenario-based questioning, in order to measure policy deviance. The advantage of this method is the specificity of the question in place. Instead of asking for general policy compliance as it is the case in positive policy compliance research, deviance against a specific policy (e.g. using private USB sticks with their corporate device even though they are explicitly forbidden).

Assuming that the interviewee responds honestly, asking for behaviour in a specific scenario seems promising.

However, especially when coming to positive policy compliance research this approach would require the introduction of a scenario, and thus further complicate the layout of the self-reporting questionnaire. This would also potentially minimize return rates of self-reporting questionnaires. Another possibility would be to capture specific policy compliant behaviour by assuming symmetry between policy compliance and policy deviance. This approach would ask, whether a person would use private USB sticks with their corporate device, however the usefulness of this approach would require knowledge on the policy that a subject is governed under prior to the survey. This further complicates surveys with self-reporting questionnaires.

Knowledge of the policy however is surely one of the most important antecedents for policy compliance. If an individual does not know about the information security policies contents, it will not be able to comply, or comply only by chance. Therefore, the measurement instrument, that is proposed in this contribution, uses both items for measuring policy knowledge, and behaviour. By measuring policy knowledge, the approach can orient on scenario-based questions without the need to extensively introduce a scenario, or gather knowledge on the applied policies prior to the survey. By measuring policy knowledge and policy compliant behaviour, the measurement instrument provides two scales. The first scale indicates the self-reported policy compliance (SRPC) of an individual based on specific questions on the behaviour of the individual, and the contents of the policy. The second scale provides the consistency of the self-reported policy compliance by measuring the difference between the claimed knowledge of the policy contents and actually having read the policy. This scale is referred to as self-reported policy compliance consistency (SRPCC) scale in the following

Both the SRPCC and the PC scales can be used in combination in order to e.g. optimize the sample, or directly in quantitative analysis e.g. in regression analysis. The remainder of this section first introduces the questionnaire items for capturing the policy contents. The following section introduces the questionnaire items for capturing the individuals' behaviour. Then the scale for policy compliance and the scale for policy compliance reporting consistency are introduced, each with their analysis logic.

3.1 Questionnaire item development

Information security policies in organizations can have different contents and topics. For instance, one organization may employ policies that restrict the use of devices for private purposes, while other organizations may embrace private use of their devices. Therefore, a general list on policy contents is hard to provide.

Scenario	**Contribution(s)**	*"My organizations information security policy…"*
USB Usage	(D'Arcy et al., 2014), (Siponen and Vance, 2010)	*"…allows me to use a private USB stick with a computer at work."*
Document Transfer	(Siponen and Vance, 2010)	*"…allows me to transfer working documents or e-mails to a private mail account."*
Device Usage	(Shepherd and Mejias, 2016), (D'Arcy et al., 2014), (Cheng et al., 2014), (Cheng et al., 2013), (Li and Cheng, 2013), (Guo et al., 2011), (Siponen and Vance, 2010)	*"…allows me to use a company computer or mobile device for private purposes."* *"…allows me to disable security features (e.g. the antivirus) on my organizations devices."*
Software Installation	(Guo et al., 2011)	*"…allows me to install non-corporate software on a company computer or mobile device."* *"…does not require me to lock my computer when I leave my workstation."*
Password-related Behaviour	(Johnston et al., 2016), (D'Arcy et al., 2014), (Cheng et al., 2013), (Guo et al., 2011), (Siponen and Vance, 2010)	*"…allows me to share my password with other employees."* *"…allows me to use weak passwords with my devices (e.g. a birthday or the name of a family member)."* *"…allows me to write-down passwords."*
Information Sharing	(D'Arcy et al., 2014), (Cheng et al., 2013), (Kajtazi et al., 2013)	*"…allows me to share confidential information of my organization with friends outside my organization."* *"…allows me to share confidential information of my organization with experts outside my organization, that were not hired or do not collaborate with my organization, in order to get the job done."*

Table 1. Considered Scenarios and questionnaire items for Policy Contents of policy deviant research

However, existing research on policy deviant behaviour that use scenario-based techniques for capturing policy deviance may show which scenarios, and thus which policy contents may be relevance. Still, it is worthwhile to note that neither the SRPC nor the SRPCC scale depend on the provided set of questionnaire items on policy contents. The only limitation to the items, that both the SRPC and the SRPCC scales imply, is that for every questionnaire item on policy contents, there must be exactly one questionnaire item on policy compliant behaviour. The identified scenarios were consolidated from literature that was gathered by using a systematic literature research[1] (Cronin et al., 2008) that yielded 16 contributions on negative policy compliance[2].

Table 3 provides an overview on the considered contributions. Additionally, ***Table 3*** indicates the scenarios that were used within these contributions for measuring policy deviant behaviour. For each scenario that is used for measuring policy deviant behaviour, questions on the knowledge of policy contents on the scenario (in the following referred to as questions on policy knowledge) were included (see ***Table 3*** for an overview on the scenarios and the corresponding questionnaire items). When a scenario indicated different details in the literature, multiple questions on policy knowledge were included. One example are password-related behaviours, which can include sharing passwords, using weak passwords and writing passwords down (Interestingly, reusing passwords was not considered within the scenarios of the regarded literature).

Each of the policy knowlegde question was fitted with a behavioural question, which are in the following referred to as questions on policy compliant behaviour. For instance, the question on whether the organizations information security policy allows for the use of a private USB stick with a computer at work is accompanied by a question on whether the individual has ever used a private USB stick with a computer at work. The current version thus involves 11 questions on the contents of the organizations policy that an individual is associated with, along with 11 questions on the scenario-specific behaviour of the individual.

3.2 Scale for Policy Compliance

Each question on policy knowledge is accompanied by a question on policy compliant behaviour. E.g. if the questionnaire asks on policy knowledge on the usage of USB devices, a question on whether the an individual has acted accordingly is included. If one assumes, that response biases in self-reporting questionnaires on positive policy compliance prevail due to identity theory (Brenner et al., 2014; Philip S. Brenner and DeLamater, 2016; Stryker, 1980) then more detailed, scenario specific reporting, may be less biased as individuals are not able to answer the more specific question in the affirmative (Philip S. Brenner and DeLamater, 2016).

Therefore each policy knowledge question is considered along with the question on policy compliant behaviour. This way, it is possible to determine the behaviour of the individual in light of the organizations security policy with which the individual is associated with. Knowledge on the policy itself is gathered “on-the-fly”, through the items on policy knowledge.

---

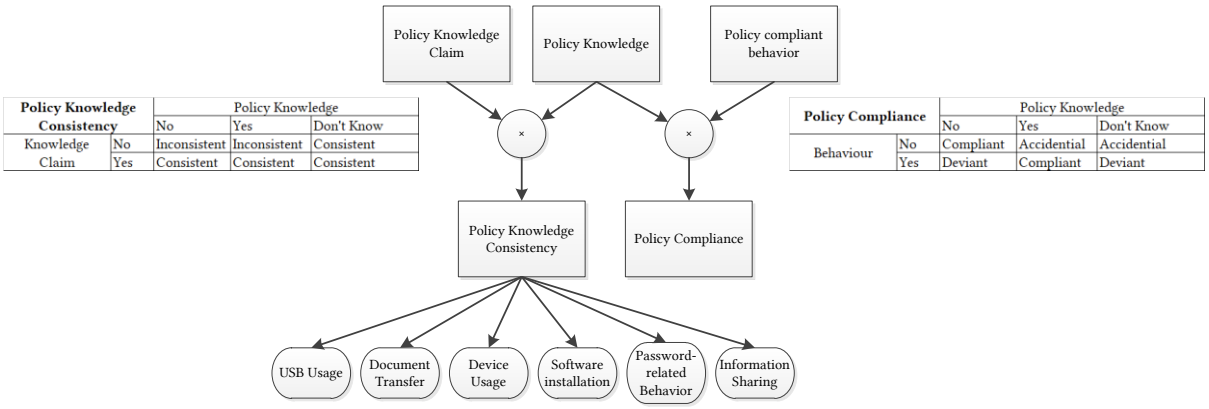
[1] The used literature database was Scopus (http://www.scopus.com). The used search term was: (it security OR information security OR it-security) AND (policy compliance OR security violation) AND (LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "ECON") OR LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "COMP"))

[2] The literature research resulted in 5.680 titles that were scanned for relevant contributions on negative and positive policy compliance. Relevant contributions were considered as any empirical examination that aims at discovering, validating or replicating factors that constitute policy deviant or compliant behaviour. 185 relevant abstracts were then examined for relevant contributions, resulting in 93 full-texts on the topic and finally 55 contributions of which 16 contributions focus on policy deviant behaviour.

The questions on policy knowledge ask for scenario specific rules of the organizations information security policy that the individual may or may not know about. Therefore, these questions must be answerable with "Yes", "No", or if the individual does not know, whether the policy contains a rule prohibiting an aspect with "Don't Know". Questions on policy compliant behaviour on the other hand ask the individual if a specific behaviour regarding one of the chosen scenarios has not been carried out (A typical question on policy compliant behaviour for instance would be "I am certain that I will comply with the information security policy of my organization").

Having gathered the contents of the policy via the questions on policy knowledge, along with the behaviour of the individual via the questions on policy compliant behaviour, the corresponding policy compliance can be determined by using a boolean table (see Figure 1). This results in three possible cases. If a policy does not contain a rule on a specific scenario, and the individual reports the described behaviour of the scenario, this would mean that the individual acts in due diligence and thus policy compliant. If the individual does not carry out a specific behaviour, and reports that the policy contains a rule prohibiting this behaviour, this as well indicates due diligence, and thus policy compliant.

There may be cases where the individual does not carry out a certain behaviour, but not due to the policy but e.g due to awareness of security issues associated with that behaviour (due care). These Cases are indicated as "Accidential" policy compliance in the boolean table of Figure 1. Finally, policy deviant behaviour is indicated, if an individual knows that the policy prohibits a certain behaviour, but still reports to carry out the behaviour. Also policy deviance is assumed to be the case, if behaviour is reported by the individual, in lack of knowledge on the policy itself in this regard. This would clearly be a case of a lack of individual due diligence and due care. Additionally since the questions on policy knowledge and policy compliant behaviour are all based in scenarios of current policy deviant research one may assume that this behaviour is usually associated with security issues. Therefore the case of not knowing the contents of the policy on a specific behaviour, but still reporting that behaviour is also considered a lack of individual due diligence and due care. Both cases show policy deviant behaviour in the resulting scale on self-reported policy compliance (SRPC).



Policy Knowledge Consistency		Policy Knowledge		
		No	Yes	Don't Know
Knowledge Claim	No	Inconsistent	Inconsistent	Consistent
	Yes	Consistent	Consistent	Consistent

Policy Compliance		Policy Knowledge		
		No	Yes	Don't Know
Behaviour	No	Compliant	Accidential	Accidential
	Yes	Deviant	Compliant	Deviant

Figure 1 Overview on the logic of the SRPC and SRPCC Scales

As mentioned throughout the previous Sections, verifiability of self-reported policy compliance is largely an issue. There are multiple influencing factors when researching individuals, and even with self-administered questionnaires many cases have indicated that reported values may in fact not be associated with the true behaviour of individuals (Philip S. Brenner and DeLamater, 2016; Philip S Brenner and DeLamater, 2016; Chase et al., 1983; Klesges et al., 1990; Rzewnicki et al., 2003). Therefore, true self-reported behaviour may only be truly verifiable if the same behaviour is also observed. However, this would completely diminish the advantage of a self-reporting questionnaire. Additionally, this observation would only be possible in controlled environments that may suffer from other biases, such as the hypothesis bias of survey subjects.

If however, self-reporting of policy compliant behaviour is subject to biases due to identity theory, as (Philip S Brenner and DeLamater, 2016) put it, and as previously introduced, measuring the difference

between the claim of having read the organizations policy, and knowing the policies contents may provide a value of consistency of the individuals reporting. Individuals that postulate a behaviour, while not acting on that behaviour in reality, may respond truthfully if asked whether he or she has actually read the policy. However, we assume that if an individual acts upon a self-formulated identity (Philip S Brenner and DeLamater, 2016), he or she may report knowledge on policy contents without actual knowledge of them. If this is the case, then the reported policy knowledge is subject to inconsistencies. This may also affect the possible truthfulness of the reported policy compliant behaviour, and indicate possible biases in the responses. Therefore the question on whether an individual has actually read the information security policy of his/her organization (in the following referred to as policy knowledge claim), is considered along with the reported policy knowledge by using a boolean table (see Figure 1). If an individual claims to not having read the organizations information security policy, any reported policy knowledge except for not knowing whether the policy contains a rule prohibiting a scenario-specific behaviour, indicates an inconsistency. This self-reported policy compliance consistency (SRPCC) provides an indication of truthfulness of the responses, and may be used for verifying the SRPC results throughout data analysis.

Using the mean value of the resulting SRPCC and SRPC values then results in the SRPC and SRPCC scale. The SRPC scale then indicates the degree of policy compliance of an individual. This scale should be analysed together with the SRPCC scale in order to determine the truthfulness of the individuals SRPC scale.

4 Validation of the SRPC and SRPCC scales

The SRPC and SRPCC scales were both embedded in a self-reporting questionnaire that is designed for verification of questionnaire items of current positive policy compliance research. The different questionnaire itemsets that are being used to compute the SRPC and SRPCC scales were distributed in the questionnaire. For instance, individuals were asked whether they have read their organizations security policy in the beginning of the questionnaire. Items on policy knowledge followed in the middle, after a few itemsets that are unrelated to the policy knowledge of the individual. Finally, items on policy compliant behaviour were put at the end of the questionnaire. This should hinder individuals in determining the relatedness of the three itemsets, and thus hinder altering the responses in light of their postulated identity. The questionnaire was pretested with a small sample consisting of researchers from a research organization. Unfortunately the sample remained relatively small, due to work council prohibitions (n=8). However, as the determination of cronbachs alpha should be rather invariant to the amount of interviewees we believe that the sample size provides only a rather small drawback regarding the statement of validity of the SRPC and SRPCC scales within this section. Existing literature suggests that the Cronbach alpha value should exceed at least 0.7 (Fornell and Larcker, 1981) in order for the scale to be reliable. Additionally, the item-total correlations are all above 0.39, with the majority being above 0.7, showing that the scale indicates strong psychometric properties (Diener et al., 1985). A first and small correlation analysis of the pretest sample showed weakly significant negative correlations (with a two-sided significance testing) between the policy compliance measured by the items gathered from the current literature on policy compliance research by (Kurowski and Dietrich, 2017) (see Section 2), and the SRPC (-.717, $p \leq .05$) and SRPCC scales (-.799, $p \leq .05$). This indicates that with higher consistency of measured policy knowledge, the individuals seem to indicate less policy compliance and vice versa. Additionally, the SRPC scale correlates positively, yet not significant with the SRPCC scale (.475). However, in light of the small sample size, these findings provide only an indication that the scale may work.

SRPC			**SRPCC**		
Item	**Cronbach's alpha**	**Item-total Correlation**	**Item**	**Cronbach's alpha**	**Item-total correlation**
PC01	.911	.886	PKC01	.961	.720
PC02		.781	PKC02		.992
PC03		.923	PKC03		.992

SRPC			SRPCC		
Item	**Cronbach's alpha**	**Item-total Correlation**	**Item**	**Cronbach's alpha**	**Item-total correlation**
PC04		.799	PKC04		.720
PC05		.395	PKC05		.720
PC06		.702	PKC06		.788
PC07		.749	PKC07		.788
PC08		.425	PKC08		.788
PC09		.398	PKC09		.992
PC10		.414	PKC10		.434
PC11		.922	PKC11		.992

Table 2 Internal validity of the scales and item-total correlation of the scale items

5 Conclusion

Both the SRPC and the SRPCC scales provide a promising approach for measuring policy compliance. The contribution has shown the internal validity, and the strong psychometric properties of the scales. Average variance extracted (AVE), as suggested by (Fornell and Larcker, 1981) however was not considered, at this would require a factor analysis which would not provide any promising results due to the low sample size of the pretest. The SRPC and SRPCC scales are currently used in a larger survey, which will also provide the AVE values. This survey also compares the scale of this contribution with existing itemsets for measuring self-reported policy compliance. This survey will also be used to finally assess the truthfulness of policy compliance measurements in current research, since (Kurowski and Dietrich, 2017) indicated in fact biases of the self-reported policy compliance. The more detailed, scenario-driven view on policy compliance in the SRPC scale puts the individual in front of more specific questions on their behaviour. Rather than asking an individual if he/she complies with the rules in general, our design is able to ask the individual whether he or she complies with a specific rule of the policy (e.g. do you use upload corporate information to your private mail account?). This comes close to asking an individual whether they would behave as described by a specific scenario, such as in scenario-based survey methods (e.g. the vignette method) (Taylor, 2005) that is commonly used in research on policy deviant behaviour. Since the questions of the SRPC scale gather knowledge of the policy on-the-fly, the questions on policy compliant behaviour can be fitted to the security policy of the individuals organization without actually knowing the policy. Of course this raises the question, whether the reported policy knowledge of the individual is in fact truthful. Therefore, the reported policy knowledge is considered along with the claim of having read the policy, which leads to the SRPCC scale. Individuals may score high on the SRPC scale, but a low score on the SRPCC scale indicates that most of the reported policy knowledge does not match the reported knowledge of the policy itself.

Of course, the SRPC and SRPCC scales may be subject to the same biases they are meant to avoid. Any individual, that postulates an identity but does not act accordingly due to any reason, may simply align the answers on policy knowledge, policy compliance, and on the claim of knowing the policy itself in such a way that it aligns with his or her identity. There is surely no rocket science to the scale, and any individual that puts some thinking in the process of filling out a questionnaire may figure out how the scale works. However, it puts more effort into the process. Sincere individuals may this way eventually stumble upon their own biases. Additionally, the items that are used to compute the scale must be dispersed in the questionnaire, in order to hinder the identification of the scale. Additionally, one may put a time limit on the questionnaire to pressure the individual and avoid him or her from thinking too much about the questions. However, this can result in individuals to choose response strategies (e.g. by providing more acquiescent responses) (Kemmelmeier, 2016) rather than truthfully answering the questions. In conclusion, the SRPC and SRPCC scales, as any self-reporting questionnaire, may be subject to biases. However, due to the more detailed questioning, the use of items that are dispersed within a questionnaire, and assessment of policy compliance and policy knowledge con-

sistency through the combination by boolean tables, it is harder to figure out the right response strategy, and it requires more consideration by the individual. We therefore believe, that the SRPC and SRPCC scale may provide more truthful responses, since they are not subject to biases by individual postulated identities (Philip S Brenner and DeLamater, 2016). Currently ongoing research will provide further insights into the truthfulness of both the SRPC and SRPCC scales, and currently used itemsets on positive policy compliance.

References

Bansal, G., Shin, S.I., 2016. Interaction effect of gender and neutralization techniques on information security policy compliance: An ethical perspective, in: AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems.

Brenner, Philip S., DeLamater, J., 2016. Lies, Damned Lies, and Survey Self-Reports? Identity as a Cause of Measurement Bias. Soc. Psychol. Q. 79, 333–354. https://doi.org/10.1177/0190272516628298

Brenner, Philip S, DeLamater, J., 2016. Measurement directiveness as a cause of response bias: Evidence from two survey experiments. Sociol. Methods Res. 45, 348–371.

Brenner, P.S., Serpe, R.T., Stryker, S., 2014. The causal ordering of prominence and salience in identity theory: An empirical examination. Soc. Psychol. Q. 77, 231–252.

Chase, D.R., Godbey, G.C., others, 1983. The accuracy of self-reported participation rates. Leis. Stud. 2, 231–235.

Cheng, L.., Li, Y.. b, Li, W.., Holm, E.., Zhai, Q.., 2013. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Comput. Secur. 39, 447–459. https://doi.org/10.1016/j.cose.2013.09.009

Cheng, L.., Li, W.., Zhai, Q.., Smyth, R.., 2014. Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. Comput. Hum. Behav. 38, 220–228. https://doi.org/10.1016/j.chb.2014.05.043

Chu, A.M.Y.., Chau, P.Y.K.., So, M.K.P.., 2015. Explaining the Misuse of Information Systems Resources in the Workplace: A Dual-Process Approach. J. Bus. Ethics 131, 209–225. https://doi.org/10.1007/s10551-014-2250-4

Corporate Trust, 2014. Studie: Industriespionage 2014 - Cybergeddon der deutschen Wirtschaft durch NSA & Co.? (Studie). Coprorate Trust Business Risk & Crisis Management GmbH, München.

Cronin, P., Ryan, F., Coughlan, M., 2008. Undertaking a literature review: a step-by-step approach. Br. J. Nurs. 17, 38.

Crowne, D.P., Marlowe, D., 1960. A new scale of social desirability independent of psychopathology. J. Consult. Psychol. 24, 349–354.

D'Arcy, J.., Herath, T.., Shoss, M.K.., 2014. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. J. Manag. Inf. Syst. 31, 285–318. https://doi.org/10.2753/MIS0742-1222310210

Diener, E., Emmons, R.A., Larsen, R.J., Griffin, S., 1985. The satisfaction with life scale. J. Pers. Assess. 49, 71–75.

Dols, T., Silvius, A.J.G., 2010. Exploring the Influence of National Cultures on Non-Compliance Behaviour. Commun. IIMA 3, 11–32.

Fornell, C., Larcker, D.F., 1981. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. J. Mark. Res. 18, 39–50.

Guo, K.H., Yuan, Y., Archer, N.P., Connelly, C.E., 2011. Understanding nonmalicious security violations in the workplace: a composite behavior model. J. Manag. Inf. Syst. 28, 203–236.

Harzing, A.-W., 2006. Response styles in cross-national survey research a 26-country study. Int. J. Cross Cult. Manag. 6, 243–266.

Hofstede, G.H., Hofstede, G.J., 2005. Cultures and organizations: software of the mind, Rev. and expanded 2nd ed. ed. McGraw-Hill, New York.

Johnston, A.C.., Warkentin, M.., McBride, M.., Carter, L.., 2016. Dispositional and situational factors: Influences on information security policy violations. Eur. J. Inf. Syst. 25, 231–251. https://doi.org/10.1057/ejis.2015.15

Kajtazi, M.., Cavusoglu, H.., Benbasat, I.., Haftor, D.., 2013. Assessing self-justification as an antecedent of noncompliance with information security policies, in: Proceedings of the 24th Australasian Conference on Information Systems.

Kemmelmeier, M., 2016. Cultural differences in survey responding: Issues and insights in the study of response biases. Int. J. Psychol. 51, 439–444.

Kim, J.., Park, E.H.., Baskerville, R.L.., 2016. A model of emotion and computer abuse. Inf. Manage. 53, 91–108. https://doi.org/10.1016/j.im.2015.09.003

Klesges, R.C., Eck, L.H., Mellon, M.W., Fulliton, W., Somes, G.W., Hanson, C.L., 1990. The accuracy of self-reports of physical activity. Med. Sci. Sports Exerc.

Kurowski, S., Dietrich, F., 2017. Response and Cultural Biases in Information Security Policy Compliance Research, in: Open Identity Summit 2017. Presented at the Open Identity Summit 2017, LNI, Karlstad, Sweden, pp. 13–24.

Li, W., Cheng, L., 2013. Effects of neutralization techniques and rational choice theory on internet abuse in the workplace, in: Proceedings - Pacific Asia Conference on Information Systems, PACIS 2013.

Lowry, P.B.., Posey, C.., Bennett, R. (B. J.., Roberts, T.L.., 2015. Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. Inf. Syst. J. 25, 193–273. https://doi.org/10.1111/isj.12063

Malhotra, M.K., Grover, V., 1998. An assessment of survey research in POM: from constructs to theory. J. Oper. Manag. 16, 407–425.

Morren, M., Gelissen, J.P., Vermunt, J.K., 2012. Response strategies and response styles in cross-cultural surveys. Cross-Cult. Res. 46, 255–279.

Myers, M., 2009. Qualitative research in business and management, 1st ed. Sage Publications Ltd, London.

Ponemon Institute, 2016. 2016 Cost of Data Breach Study: Global Analysis (Benchmark research sponsored by IBM). Ponemon Institute, IBM, Traverse City, Michigan, USA.

Rzewnicki, R., Auweele, Y.V., De Bourdeaudhuij, I., 2003. Addressing overreporting on the International Physical Activity Questionnaire (IPAQ) telephone survey with a population sample. Public Health Nutr. 6, 299–305.

Shepherd, M.M.., Mejias, R.J.., 2016. Nontechnical Deterrence Effects of Mild and Severe Internet Use Policy Reminders in Reducing Employee Internet Abuse. Int. J. Hum.-Comput. Interact. 32, 557–567. https://doi.org/10.1080/10447318.2016.1183862

Siponen, M.., Adam Mahmood, M.., Pahnila, S.., 2014. Employees' adherence to information security policies: An exploratory field study. Inf. Manage. 51, 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M.., Vance, A.., 2010. Neutralization: New insights into the problem of employee information systems security policy violations. MIS Q. Manag. Inf. Syst. 34, 487–502.

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

Stryker, S., 1980. Symbolic interactionism: A social structural version. Benjamin-Cummings Publishing Company.

Taylor, B.J., 2005. Factorial surveys: Using vignettes to study professional judgement. Br. J. Soc. Work 36, 1187–1207.

Vance, A.., Eargle, D.., Anderson, B.B.., Brock Kirwan, C.., 2014. Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). J. Assoc. Inf. Syst. 15, 679–722.

Vance, A.., Siponen, M.., 2012. IS security policy violations: A rational choice perspective. J. Organ. End User Comput. 24, 21–41. https://doi.org/10.4018/joeuc.2012010102

Annex

Contributions	**Summary**
(Shepherd and Mejias, 2016)	Quantitative research on the impact of reminders on acceptable use policies against Internet Abuse.
(Johnston et al., 2016)	Factorial Survey on dispositional and situational factors that constitute policy deviance. Used scenarios are on password related behaviour.
(Bansal and Shin, 2016)	Scenarios are used for identifying the moderating effect of different neutralization scenarios (6 different scenarios).
(Kim et al., 2016)	PLS modelling with different treatment conditions for abuse intention. Treatments included manipulation of freedom of movement, and manipulation of environment variables in a scenario where the subject is being mistreated by the company and seeks revenge.
(Chu et al., 2015)	PLS modelling of the factors that constitute IS resource misuse. No scenario techniques were used in this contribution.
(Lowry et al., 2015)	PLS modelling of the factors that constitute Reactive Computer Abuse. No scenario techniques were used in this contribution.
(D'Arcy et al., 2014)	PLS modelling of the factors that constitute a violation intention. Measurement was done with an online survey that randomly selected one out of five scenarios. The scenarios included password-sharing, password write-down, failure to logoff, USB copy and data leakage.
(Cheng et al., 2014)	PLS modelling of the factors that constitute the intention to use the internet for personal reasons at work.
(Vance et al., 2014)	EEG measurement to identify the impact of risk perception on security warning disregard.
(Cheng et al., 2013)	PLS modelling with hypothetical scenario method of the factors that constitute the information security policy violation intention. Four scenarios were used: copying sensitive data, workstation logout, sharing passwords, and reading confidential files.
(Kajtazi et al., 2013)	PLS modelling with hypothetical scenario method of the factors that constitute the willingness to engage in noncompliance behaviour. Only one scenario on sharing confidential information was used.
(Li and Cheng, 2013)	PLS modelling of the factors that constitute internet abuse intention. Internet abuse intention is measured by items that ask for the intention to use the internet for non-work related purposes.
(Vance and Siponen, 2012)	PLS modelling with hypothetical scenario method of the factors that constitute the intention to violate information systems security policies. Used scenarios included copying confidential information to a USB drive, failing to logout from a workstation and password sharing.
(Guo et al., 2011)	PLS modelling with hypothetical scenario method of the factors that constitute the intention for non-malicious security violations. Four scenarios were included: Writing-down passwords, using portable USB drives to carry sensitive business data, downloading and installing free software from the internet, using insecure public wireless connections.
(Siponen and Vance, 2010)	PLS modelling with hypothetical scenario method of the factors that constitute the intention to violate information systems security policies. The contributions uses three different scenarios, but also provides a survey on IS security policy violations that was used for scenario development. These violations include: failing to log-out of workstations, writing down passwords, sharing password, copying sensitive data to USB drives, revealing confidential information to outsiders, disabling security configurations, using laptops carelessly outside the company, sending confidential information unencrypted, creating easy-to-guess passwords.

Table 3. Considered Contributions on policy deviant behaviour