Response and Cultural Biases in Information Security Policy Compliance Research

Sebastian Kurowski[1], Fabina Dietrich[1]

Abstract: This contribution tries to shed light on whether current information security policy compliance research is affected by response (such as social desirability) or cultural biases. Based upon the hypothesis that response biases may be subject to information processing of the questionnaire item by the respondent, a classification of questionnaire items of 17 surveys is provided. Furthermore, the Individualism and Power Distance indices are gathered for the survey samples. Correlation analysis reveals that the Power Distance index correlates negatively, while Individualism correlates positively with the mean self-reported policy compliance. These findings support previous findings on the role of Power Distance and contradict the influence of response and social desirability biases on self-reported information security policy compliance.

Keywords: Policy Compliance, Information Security, Information Security Management, Culture, Human Behaviour

1   Introduction

Human behaviour has long been identified as an important antecedent for attacks on organizational and private IT systems [Jo16]. E.g. when it comes to industry espionage 38.4% of German corporations report social engineering as the main act of industry espionage [Co14], and [Po16] identifies human error as one of three root causes for data breaches, causing the disclosure of data in 25% of reported cases. Respectively both studies aiming at identifying factors that lead to noncompliance, e.g. [BS16], [Ch15b], [Da14], [Sh16], [Si14], [Va14], [VS12], and those aiming at factors that foster compliance to information security policy compliance exist. The following focuses on the latter, which are referred to as studies on positive policy compliance. One widely distributed measurement tool used within these studies are self-administered questionnaires. This measurement tool is widely known to be subject to response biases. E.g. [HV16] find that questionnaires can be subject to response biases due to the cultural background of the respondent in interview situations, and [Ke16] even find cultural differences in the response style, when using completely self-administered questionnaires, where no interviewer is used. In this context, the vast majority of acquiescent responses in self-reported positive policy compliance raise the question of response biases: If one assumes that the information security policies of an organization

[1] Institute for Labour Science and Technology Management, University of Stuttgart, Competence Team
Identity Management, Allmandring 35, Stuttgart, 70565, {prename}.{surname}@iat.uni-stuttgart.de
Annex at: https://www.researchgate.net/publication/318208966_Annex_to_the_Contribution_
Response_and_Cultural_Biases_in_Information_Security_Policy_Compliance_Research

are in fact efficient mechanisms which prescribe protecting behaviour, this contradicts the previously mentioned findings of [Co14], [Po16] that indicate misbehaviour as a major cause of data breaches and industry espionage. Even the quality of the surveys can largely be ruled out as a cause of this contradiction: existing surveys on positive policy compliance widely employ validity testing, defined and justified sample frames, sufficiently large response rates, and partly even estimate the non-response bias, indicating a rather high quality according to [MG98], [So14].

This contribution therefore tries to shed light on whether response biases impact the self-reporting of the dependent variable in positive policy compliance. If this is the case, truthful correlations of independent variables with reported policy compliance may not be observable, while untruthful correlations may emerge. Providing a settled answer on this issue is therefore a key requirement for building upon the existing knowledge provided by the contributions on positive policy compliance. In order to provide this answer, this contribution conducts an analysis based on synthesized data that was kindly provided by the authors, or gathered from their respective contributions. Items are categorized and counted for the data synthesis. The impact of situational factors are analysed in terms of the question style (see Section 2), while dispositional factors are provided by the cultural dimension of Individualism versus Collectivism [Ho05], indicated by the country of origin of the used sample. Section 3 provides a description of the data synthesis, and analysis process, along with the analysis results and a critical discussion of the findings. This is followed by a conclusion of the findings and a brief introduction on future research in Section 4.

2   Situational and Dispositional Factors and Information Security Policy Compliance Research

Response Biases, such as those due to social desirability, are often seen both as a dispositional factor of the interviewee [CM60], and as a factor that is induced by the interview setting itself. As [Bd16a] put it: "it is relatively easier to admit a "bad" truth on a paper or computerized questionnaire than to a human interviewer" [Bd16a]. Still, [Bd16a] themselves find that self-administered (e.g. web-based) questionnaires may indicate substantial bias due to social desirable responses. E.g. survey reports of church attendance and rates of exercise are found to be double the actual frequency than the measurement of the criterion measure [BD16a], [BD16b], [Ch83], [Kl90], [Rz03]. Using identity theory [St80], [Bd16a] postulate that behaviour is "[...] encouraged by identity prominence; in short, we tend to perform identities that we value [Br14]" [Bd16a]. 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" [Bd16a]. Furthermore, [Mo12] 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 [Ke16]. This observable effect is shown in [Mo12] as moderated by the cultural background of the respondents.

For Security Policy Compliance Research, these findings are rather problematic. It means that research on policy compliant behaviour may build upon over-reported compliant behaviour, and thus yield possibly wrong conclusions. This opens up the consideration of dispositional and situational factors that may affect the response of the respondent. The following provides an overview on hypotheses on the impact of situational factors implied by the types of questions, and therefore the information processing of the individual. A review of the questionnaire items for the dependent variable of the considered surveys resulted in the classification, that is shown in the Annex (see Tab. 3 and Tab. 4 in the Annex), that distinguish between the dimensions of Protection vs. Adherence, Reporting of Specific vs. Unspecific Behaviour, and the Reporting of Intended vs. Actual Behaviour.

Protection versus Adherence: Information security is often perceived as something, which is done by the IT department, or generally by others in the organization [Ng09]. Even if users are aware of a security policy, they may not act accordingly [Ch15a]. Items that ask for protective actions by an individual may thus be elaborated more (H1a), than items that ask for adherence to a policy (H1b), resulting in a different impact on the self-reported policy compliance. Therefore, we assume that *an increase of Items on Protection Actions will decrease the Self-Reported Policy Compliance (H1a)*, and that *an increase of Items on Policy Adherence will increase the Self-Reported Policy Compliance (H1b)*.

Specific versus Unspecific Reporting: The considered surveys (see Section 3) indicated items on reported protective actions, reported adherence to policies, intended protective actions, and intended adherence to policy compliance. Hereby past observations indicate that the item wording may have an impact on the response [Ke16], [Mo12]. If an individual responds to an item, it is assumed to go through five stages which include "...interpreting the question, retrieving information, generating the judgement, mapping the judgement to the response scale and editing the response" [Mo12]. Past research has found an impact of dispositional factors, e.g. the generation of immigrants, or the general cultural background on given responses by individuals [Bl01], [Mo12]. [Ke16] comments the findings of [Mo12] by mentioning that "...although Dutch respondents explored the subtleties of a question or statement's phrasing, the Spanish respondents seized on the spontaneous affect they experienced when answering the same question." [Ke16]. While this indicates a response strategy which is largely influenced by the respondents' culture, it also indicates that the information processing of the survey item impacts the response to an item [Ke16]. The data synthesis originated items which referred to specific protective actions (e.g. actively getting updates on specific guidelines) and unspecific protective actions (e.g. protecting the organization). The same was the case for items that referred to adherence to policies. We assume, that asking about a specific action, or adherence to a specific rule requires more cognitive elaboration of the respondent, than asking about unspecific actions or policies. We therefore hypothesize that *an increase of Unspecific Items will increase the Self-Reported Policy Compliance (H2a)* and that *an increase of Specific Items will decrease the Self-Reported Policy Compliance (H2b)*. Analogously, *an Increase of Specific Items*

on Adherence will Increase the Self-Reported Policy Compliance (H3a), *An Increase of Unspecific Items on Adherence will Decrease the Self-Reported Policy Compliance (H3b)*, *An Increase of Specific Items on Protection Action will Increase the Self-Reported Policy Compliance (H4a)*, and *an Increase of Unspecific Items on Protection Action will Decrease the Self-Reported Policy Compliance (H4b)*.

Intention versus Actual Behaviour: [Bd16b] postulate that social desirability biases may result out of the respondents' identity, that is not acted upon due to any given circumstances. For policy compliance this reasoning could be applied by stating that respondents generally want to protect their organizations, and that respondents generally want to adhere to the organizations' information security policy. However, due to given circumstances such as the costs of adherence (e.g. the given work impediment), they may fail to do so. Still they may enact this identity if asked about their intentions. Therefore we hypothesize, that if a response or social desirability bias is given we would expect that the number of items on intended policy adherence or intended protective actions increases the self-reported policy compliance (H5a). Therefore, *an Increase of Items on Intention will Increase the Self-Reported Policy Compliance (H5a)*. On the other hand, asking for actual behaviour and not intentions may hinder the individual to enact the described identity, since the respondent elaborates not on its' intended actions, but on its' past behaviour. We therefore hypothesize that *an Increase of Items on Behaviour will Decrease the Self-Reported Policy Compliance (H5b)*.

Individualism versus Collectivism: Response Biases and Policy Compliance can be affected by dispositional factors, including character traits, such as the Big Five [Jo16], traits introduced by the individuals job [Ko11], or even the individuals work experience [HB15]. As our analysis focuses on the used samples, and not the individual respondents cultural traits as an important dispositional factor are highlighted, either as shaping character traits, or as directly impacting the individuals behaviour [Go16], [Ng09]. E.g. [Ah16] and [Ha16] discovered that (national) culture does have an influence on data sharing behavior in the world wide web. More specifically, a direct impact of the national culture of an employee has an effect on Compliance or Non-Compliance [DT10], [Sh12], [Wo08]. For instance, individuals from countries with a lower Power Distance Index (PDI[2]) seem to be more likely to violate policies [DT10]. Cultures with a high PDI indicate more respect for authority, and expectations for detailed instructions which are to be followed by the individuals [DT10], [Ho05], however at the same time low PDI scores indicate that leaders treat individuals with respect [Ho05] and empower subordinates [DT10]. On the other hand, high PDI scores are associated with acquiescent response styles [Ha06]. Therefore, a negative correlation between the PDI scores could be an indicator that the result is in fact due to the dispositional cultural trait of Power Distance. We thus assume that *an increase in PDI will decrease the self-reported policy compliance (H6a)*.

The Individualism Index (IDV[3]) of an individuals' culture seems to have an impact on

---

[2] Power Distance Index (PDI) – Acceptance of unequal distribution of power [Ho05]
[3] Individualism Index – Focus on the self over focus on others [Ho05]

information security policy compliance [DT10]. Individuals from countries with a high IDV tend to rather comply with the information security policy and are less likely to unintentionally share confidential information than in cultures with a low IDV. These differences may be due to different and noticeable divergent constructs of the self, of others, and the interdependence of both named aspects [MK91] which motivates individual behavior. The constructs of the self and of the others can influence and also determine the cognition, emotion and most important the motivation of every individual [MK91]. In individualistic cultures, people are rather self-contained and care primary about their self. Moreover the High IDV indicates that the ties between individuals are rather loose. The opposite, a Low IDV, shows that the individuals of those cultures see themselves as part of a group, the ties between the individuals are tight [FA11] and individuals "[…] are integrated into strongly cohesive in-groups, and group loyal lasts a lifetime"[DT10]. Furthermore cultures with a low IDV care more about personal contacts and relationships [DT10]. We assume that compliance with the organizations information security policy compliance will not be less important for an employee coming from a culture with a high IDV, than for individuals from a culture with a low IDV. On the other hand, individuals from cultures with a low IDV have a higher social pressure to e.g. stay long/longer at work, since it is important to the employee what work colleagues/superiors think about him/her. Also, an increase of the IDV is associated with a decrease in acquiescent responses [Ha06]. Therefore we hypothesize, that *an increase in IDV will decrease the self-reported Policy Compliance (H6b)*.

3   Analysis and Discussion

Survey Identification: In order to obtain the contribution included in the analysis of this contribution, a literature review was conducted by an approach similar to the meta-analysis of [So15a]. A literature database was used to obtain 5.680 titles. Assessment of titles took place regarding their focus on IT-Security Policy Compliance in general. This resulted in 185 abstracts, which were classified regarding their contents. Contributions which indicated opinion papers, technology contributions, home user research, security incident case studies, and literature driven taxonomies were removed. This resulted in 93 full-texts. These full-texts were analysed and all contributions that did not include empirical research on security policy compliance research were removed. Finally, this resulted in 55 studies on policy compliance and policy deviance research, and 29 studies which focus only on policy compliance research. This contribution builds upon a data set which is similar in size, than other meta-analysis with different research questions in the field of policy compliance (e.g. [So15a] also uses 29 surveys on policy compliant and policy deviant behaviour). We therefore assume to build our analysis upon a rather complete set of available surveys on policy compliant behaviour.

Data Collection: In order to provide an analysis of the possible influence of response biases and culture on self-reported policy compliant behaviour and intentions, the mean values, and the items of the dependent variable of the contributions were required. This

was however only the case for 10 of 29 contributions. Therefore, the authors of the contributions [Ab16], [AA15], [AM14], [BB13], [BK07], [Bu10], [HB15], [If16], [KB13], [Li14], [Pa13], [PH14], [RE16], [Sa15], [So15b], [WP13], [Wa11], [Ya16], [Yo13] were contacted and asked for either the used questionnaire items for the dependent variable in their survey, or the mean value of their dependent variable. The authors of [Ab16], [BB13], [Li14], [Pa13], [So15b] were able to provide the missing information. Additionally, the mean values of the questionnaire items of the dependent variable were given for [Bu10], [If16], [Sa15]. Since the authors of these contributions were not able to provide the mean value for the dependent variable, it was computed from the means of the questionnaire items. This finally resulted in a total amount of 18 contributions that were considered within this research. Some surveys additionally included the self-reported actual policy compliance along with the intended policy compliance (this is the case for the surveys [Pa13], [Po15], [Si14], [So15b]). Therefore, these surveys provided 2 different dependent variables. Also, [BB13] used a sample from two different countries (Ethiopia and USA). As the IDV and PDI of both countries vary drastically, 2 observations were included for this contribution. Both increased the total amount of observations used for preparation to 23.

Data Synthesis: Data Synthesis aimed at normalizing the mean values (1), classification of questionnaire items (2), normalization of questionnaire item class occurrence (3), and preparation of the Individualism and Power Distance indices of the observations (4). Mean values (1) were mostly retrieved with 7 point scales. However, in the case of [Ab16], [Hu12], [Li14], [Sa15] 5 point scales were used. Therefore the mean values of all contributions were normalized by using the scale range[4]. The questionnaire items (2) of the contributions were classified by using the categories shown in Annex. The item classes were built from the contributions, by considering first the distinction between specific and unspecific formulated items, then the distinction between items on adherence to a policy, or taking of a protection action, and finally the distinction between items on the intention of adherence or taking of a protection action, and the self-report of actual adherence or taking of a protection action. In order to enable a comparison of the items, the occurrence of the different item classes within the questionnaire of the considered surveys were normalized by using the amount of questionnaire items (3). Finally, the IDV and the PDI were obtained from [Ho05] for all contributions that indicated the country, in which their survey was taken. In the contributions [Hu12], [KH14], [Pa13], [Ya12] this indication was missing. However, the missing values were filled with the IDV and PDI of the country in which the authors were living in at the time of the contribution[5]. Additionally, the contribution [HK13] indicated, that a sample from Western Europe was obtained. However, as both the IDV and PDI drastically differ between the Western European countries [Ho05], the IDV and PDI of the authors country was taken as well. Finally, the IDV and the PDI index were normalized, by

---

[4] For the mean value m, the maximum scale value s_{max} and the minimum scale value s_{min} the normalized value $norm_m$ was achieved with $norm_m = (m - s_{min}) / (s_{max} - s_{min})$

[5] This requires the assumption that it is more likely, that researchers will be able to approach a sample from, or close to their cultural / national background, than those from other cultural / national backgrounds.

using maximum and minimum value of the data indicated in [Ho05]. This resulted in the data that is shown in the Annex.

3.1   Analysis of Response Bias Indications

The synthesized data (see Annex Tab. 2) was analysed by measuring the Pearson Correlation of the different category occurrences with the mean self-reported policy compliance of the survey. We refrained from using regressions due to the non-normality of the distribution of mean self-reported policy compliances in the surveys. Fig. 1 provides an overview on the result of the correlation analysis.
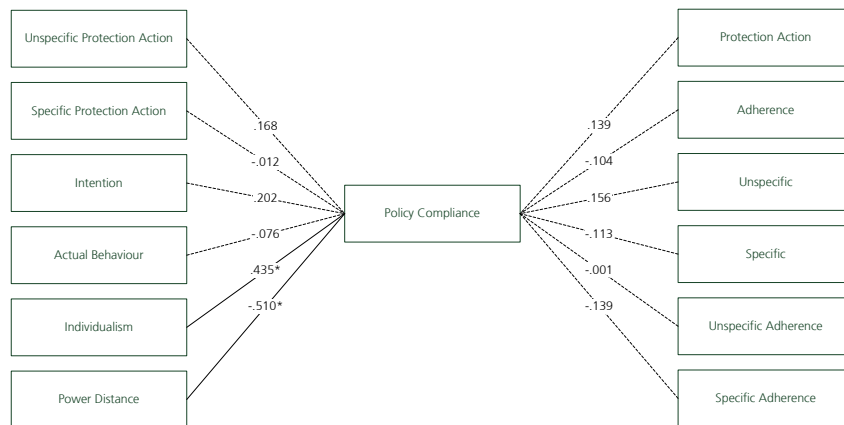

Fig. 1 Overview on the discovered correlations (* p ≤ .05, $^{n.s.}$ non significant)

Except for Individualism and Power Distance, all correlations show non-significant results. Therefore, the hypotheses H1 – H5 are rejected. Individualism shows a significant correlation with the self-reported mean policy compliance on a 95% level. However, an increase of the IDV of the sample increases the self-reported policy compliance. Therefore H6a, which hypothesized that increasing IDV would decrease the self-reported policy compliance, is rejected as well. The other significant correlation (p ≤ .05) occurs for PDI, which negatively correlates with policy compliance (-.510). This confirms past observations by [DT10] and thus H6b. All other correlations were non-significant. It is however interesting to observe, that except for items on protection action and adherence, all other effect directions were as expected. For instance, an increase in the amount of specific items decreases the reported policy compliance (-.113), which an increase of unspecific items also increases the reported policy compliance (.156). The same is given for items on Protection Action vs. items on Adherence, their unspecific and specific specialization, and items on Actual Behaviour vs. Intended Behaviour. Our findings are further discussed in the following Section 3.2.

3.2   Discussion of the Findings

The effect directions of the correlation of item classification with the mean self-reported policy compliance is supportive of the assumption that the response is influenced by social desirability due to the impact of the question style on the respondents information processing during the response [Ke16], or influenced by the enactment of an identity by the respondent [Bd16a]. However, any conclusions drawn by the item classification correlation must be regarded as being coincidentally. Significance testing of these correlations results in values between .100 and .600, indicating that these results are quite likely coincidental. Although the amount of cases is quite low (n = 23), it is reasonable to conclude that there is no effect of the question type on the self-reported policy compliance. When looking at the questionnaire items however, one may find that there is little distinguishability between the item classifications. For instance, a questionnaire item on unspecific adherence will ask for adherence of the information security policy, while an item on specific adherence will ask for adherence of the BYOD[6] information security policy. Our results indicate that these differences do not affect the amount of reported information security policy compliance. The significant and positive correlation of Individualism with the self-reported policy compliance is interesting, as it contradicts previous assumptions, regarding the impact of Collectivism on following policies and protecting an organization. This aligns well, with the findings of [Be06], [Ha06] who identify a negative correlation between the IDV and acquiescent responses. It indicates that the self-reported policy compliance is in fact not due to biases from cultural response strategies. Also [Be06] indicate a negative correlation ($p \leq .01$) of social desirability biases and the IDV. The significant and negative correlation of PDI with the self-reported policy compliance ($p \leq .05$) also contradicts the influence of response biases [Ha06] and social desirability biases [Be06] on the response. A positive correlation of the PDI would have indicated acquiescent responses [Be06]. The negative correlation however confirms the findings of [DT10] who also find a negative correlation of PDI with the self-reported policy compliance. The findings indicate that no situational factors that arise out of the questionnaire item layout affect the reported policy compliance. In conclusion, the correlation of the variations in mean self-reported policy compliance is well, yet not intuitively explained by Individualism and Power Distance. Those who are more focused on themselves, and loosely coupled with their environment, and those who are less likely to accept an uneven distribution of power are both more likely to report compliance with information security policies.

4   Conclusion

The wide use of self-administered questionnaires in information security policy compliance has so far not been subject to a revision of the questionnaire items, and critical examination of the items regarding response biases. This analysis closes this gap.

---

[6] Bring-Your-Own-Device

By classifying item questionnaire from positive policy compliance research, and by analysing the impact of the questionnaire item occurrence, and cultural traits of the individuals in the observed samples, this analysis was able to shed light on the impact of both factors on the responses. Non-significant correlations were identified for the questionnaire classes, rejecting the given hypotheses. However, the correlation directions were as hypothesized. Yet, the cultural traits of Individualism and Power Distance both significantly correlated with the mean self-reported information security policy compliance. This strongly contradicts the hypotheses of response and social desirability biases on the reported policy compliance. Of course, stronger conclusions cannot be drawn with the given sample size and methodology. However, it provides interesting indications, regarding the effect directions, and the impact of cultural traits on information security policy compliance. The latter might have been widely underestimated, and requires further research. Future research will also include the development of a questionnaire, to review the results of this preliminary analysis, and to identify the degree of explained variance provided by the cultural traits.

Acknowledgement and Annex

Bibliography

[Ab16]   Abed, J. et al.: Investigating continuous security compliance behavior: Insights from information systems continuance model. In: AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems. (2016).

[Ah16]   Ahn, T.K. et al.: Security property rights: A dilemma experiment in Austria, Maxico, Mongolia, South Korea and the United States. 143, 115–124 (2016).

[AA15]   Al-Mukahal, H.M., Alshare, K.: An examination of factors that influence the number of information security policy violations in Qatari organizations. Inf. Comput. Secur. 23, 1, 102–118 (2015).

[AM14]   Aurigemma, S.., Mattson, T..: Do it OR ELSE! exploring the effectiveness of deterrence on employee compliance with information security policies. In: 20th Americas Conference on Information Systems, AMCIS 2014. (2014).

[BS16]   Bansal, G.; Shin, S.I.: 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. (2016).

[Be06]   Bernardi, R.A.: Associations between Hofstede's Cultural Constructs and Social Desirability Response Bias. J. Bus. Ethics. 65, 1, 43–53 (2006).

[Bl01]   Bless, H. et al.: Personalized versus generalized benefits of stereotype disconfirmation: Trade-offs in the evaluation of atypical exemplars and their social groups. J. Exp. Soc. Psychol. 37, 5, 386–397 (2001).

[BB13]   Borena, B.., Bélanger, F..: Religiosity and information security policy compliance. In:

19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime. pp. 2848–2855 (2013).

[BK07]   Boss, S.R.., Kirsch, L.J..: The last line of defense: Motivating employees to follow corporate security guidelines. In: ICIS 2007 Proceedings - Twenty Eighth International Conference on Information Systems. (2007).

[Br14]   Brenner, P.S. et al.: The causal ordering of prominence and salience in identity theory: An empirical examination. Soc. Psychol. Q. 77, 3, 231–252 (2014).

[BD16a]   Brenner, P.S., DeLamater, J.: Lies, Damned Lies, and Survey Self-Reports? Identity as a Cause of Measurement Bias. Soc. Psychol. Q. 79, 4, 333–354 (2016).

[BD16b]   Brenner, P.S., DeLamater, J.: Measurement directiveness as a cause of response bias: Evidence from two survey experiments. Sociol. Methods Res. 45, 2, 348–371 (2016).

[Bu10]   Bulgurcu, B. et al.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. Manag. Inf. Syst. Q. 34, 3, 523–548 (2010).

[Ch83]   Chase, D.R. et al.: The accuracy of self-reported participation rates. Leis. Stud. 2, 2, 231–235 (1983).

[Ch15a]   Chen, Y.. et al.: Impacts of comprehensive information security programs on information security culture. J. Comput. Inf. Syst. 55, 3, 11–19 (2015).

[Ch15b]   Chu, A.M.Y.. et al.: Explaining the Misuse of Information Systems Resources in the Workplace: A Dual-Process Approach. J. Bus. Ethics. 131, 1, 209–225 (2015).

[Co14]   Corporate Trust: Studie: Industriespionage 2014 - Cybergeddon der deutschen Wirtschaft durch NSA & Co.? Coprorate Trust Business Risk & Crisis Management GmbH, München (2014).

[CM60]   Crowne, D.P., Marlowe, D.: A new scale of social desirability independent of psychopathology. J. Consult. Psychol. 24, 4, 349–354 (1960).

[Da14]   D'Arcy, J.. et al.: Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. J. Manag. Inf. Syst. 31, 2, 285–318 (2014).

[DT10]   Dols, T., Silvius, A.J.G.: Exploring the Influence of National Cultures on Non-Compliance Behaviour, (2010).

[FA11]   Fernando, S., Asai, T.: Human-related information security problems faced by British companies in economically rising countries. Presented at the Australian Information Security Management Conference , Perth 7.12 (2011).

[Go15]   Goo, J.. et al.: A path to successful management of employee security compliance: An empirical study of information security climate. IEEE Trans. Prof. Commun. 57, 4, 286–308 (2015).

[Go16]   Govender, S. et al.: The influence of national culture on information security culture. In: IST-Africa Week Conference, 2016. pp. 1–9 IIMC (2016).

[HK13]   Haeussinger, F.J., Kranz, J.J.: Information security awareness: Its antecedents and mediating effects on security compliant behavior. In: International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design. pp. 2222–2237 (2013).

[Ha16]   Halevi, T. et al.: Cultural and Psychological Factors in Cyber-Security. Presented at the iiWas , Singapore 30.11 (2016).

[Ha06]   Harzing, A.-W.: Response styles in cross-national survey research a 26-country study. Int. J. Cross Cult. Manag. 6, 2, 243–266 (2006).

[HV16]   He, J., Van de Vijver, F.J.: Response styles in factual items: Personal, contextual and cultural correlates. Int. J. Psychol. 51, 6, 445–452 (2016).

[Ho05]   Hofstede, G.H., Hofstede, G.J.: Cultures and organizations: software of the mind. McGraw-Hill, New York (2005).

[Hu12]   Hu, Q.. et al.: Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decis. Sci. 43, 4, 615–660 (2012).

[HB15]   Humaidi, N.., Balakrishnan, V..: The Moderating effect of working experience on health information system security policies compliance behaviour. Malays. J. Comput. Sci. 28, 2, 70–92 (2015).

[If16]   Ifinedo, P.: Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines? Inf. Syst. Manag. 33, 1, 30–41 (2016).

[If14]   Ifinedo, P.: Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Inf. Manage. 51, 1, 69–79 (2014).

[If12]   Ifinedo, P.: Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. 31, 1, 83–95 (2012).

[Jo16]   Johnston, A.C.. et al.: Dispositional and situational factors: Influences on information security policy violations. Eur. J. Inf. Syst. 25, 3, 231–251 (2016).

[KB13]   Kajtazi, M.., Bulgurcu, B..: Information security policy compliance: An empirical study on escalation of commitment. In: 19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime. pp. 2011–2020 (2013).

[Ke16]   Kemmelmeier, M.: Cultural differences in survey responding: Issues and insights in the study of response biases. Int. J. Psychol. 51, 6, 439–444 (2016).

[Kl90]   Klesges, R.C. et al.: The accuracy of self-reports of physical activity. Med. Sci. Sports Exerc. (1990).

[Ko11]   Kolkowska, E.: Security subcultures in an organization-exploring value conflicts. In: ECIS. (2011).

[KH14]   Kranz, J.J., Haeussinger, F.J.: Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior. In: 35th International Conference on Information Systems "Building a Better World Through Information Systems", ICIS 2014. (2014).

[Li14]   Li, H.. et al.: Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. Inf. Syst. J. 24, 6, 479–502. (2014).

[MG98]   Malhotra, M.K., Grover, V.: An assessment of survey research in POM: from constructs to theory. J. Oper. Manag. 16, 4, 407–425 (1998).

[MK91]   Markus, H.R., Kitayama, S.: Culture and the self: Implications for cognition, emotion, and motivation. Psychol. Rev. 98, 2, 224–253 (1991).

[Mo12]   Morren, M. et al.: Response strategies and response styles in cross-cultural surveys. Cross-Cult. Res. 46, 3, 255–279 (2012).

[Ng09]   Ngo, L. et al.: Assessing the level of I.T. security culture improvement: Results from three Australian SMEs. Presented at the November (2009).

[Pa13]   Pahnila, S.. et al.: Information security behavior: Towards multistage models. In: Proceedings - Pacific Asia Conference on Information Systems, PACIS 2013. (2013).

[Po16]   Ponemon Institute: 2016 Cost of Data Breach Study: Global Analysis. Ponemon Institute, IBM, Traverse City, Michigan, USA (2016).

[Po15]   Posey, C.. et al.: The impact of organizational commitment on insiders motivation to protect organizational information assets. J. Manag. Inf. Syst. 32, 4, 179–214 (2015).

[PH14]   Putri, F., Hovav, A.: Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. In: ECIS 2014 Proceedings - 22nd European Conference on Information Systems. (2014).

[RE16]   Rocha Flores, W., Ekstedt, M.: Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Comput. Secur. 59, 26–44 (2016).

[Rz03]   Rzewnicki, R. et al.: Addressing overreporting on the International Physical Activity Questionnaire (IPAQ) telephone survey with a population sample. Public Health Nutr. 6, 03, 299–305 (2003).

[Sa15]   Safa, N.S.. et al.: Information security conscious care behaviour formation in organizations. Comput. Secur. 53, 65–78 (2015).

[Sh12]   Shaaban, H., Conrad, M.: Democracy, culture and information security: a case study in Zanzibar. Inf. Manag. Comput. Secur. 2, 3, 191–201 (2012).

[Sh16]   Shepherd, M.M.., Mejias, R.J..: Nontechnical Deterrence Effects of Mild and Severe Internet Use Policy Reminders in Reducing Employee Internet Abuse. Int. J. Hum.-Comput. Interact. 32, 7, 557–567 (2016).

[Si14]   Siponen, M.. et al.: Employees' adherence to information security policies: An exploratory field study. Inf. Manage. 51, 2, 217–224 (2014).

[So15a] Sommestad, T. et al.: A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. Int. J. Inf. Secur. Priv. IJISP. 9, 1, 26–46 (2015).

[So15b] Sommestad, T. et al.: The sufficiency of the theory of planned behavior for explaining information security policy compliance. Inf. Comput. Secur. 23, 2, 200–217 (2015).

[So14]   Sommestad, T. et al.: Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf. Manag. Comput. Secur. 22, 1, 42–75 (2014).

[So11]   Son, J.-Y.: Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Inf. Manage. 48, 7, 296–302 (2011).

[St80]   Stryker, S.: Symbolic interactionism: A social structural version. Benjamin-Cummings Publishing Company (1980).

[Va14]   Vance, A.. et al.: Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). J. Assoc. Inf. Syst. 15, 679–722 (2014).

[VS12]   Vance, A.., Siponen, M..: IS security policy violations: A rational choice perspective. J. Organ. End User Comput. 24, 1, 21–41 (2012).

[WP13]   Wall, J.D., Palvia, P.: Control-related motivations and information security policy compliance: The effect of reflective and reactive autonomy. In: 19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime. pp. 894–902 (2013).

[Wa11]   Warkentin, M.. et al.: The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. Eur. J. Inf. Syst. 20, 3, 267–284 (2011).

[Wo08]   Workman, M. et al.: Security lapses and the omission of information security measures: A threat control model and empirical test. Comput. Hum. Behav. 24, 6, 2799–2816 (2008).

[Ya12]   Yang, X.. et al.: Cognitive elaboration on potential outcomes and its effects on employees' information security policy compliance intention-exploring the key antecedents. Lect. Notes Bus. Inf. Process. 108 LNBIP, 180–194 (2012).

[Ya16]   Yaokumah, W.. et al.: Towards modelling the impact of security policy on compliance. J. Inf. Technol. Res. 9, 2, 1–16 (2016).[Yo13]   Yoon, C., Kim, H.: Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. Inf. Technol. People. 26, 4, 401–419 (2013).