Culture Matters - A Cross Cultural Examination of Information Security Behavior Theories

Sebastian Hengstler[1]

[1] Chair of Information Security and Compliance, University of Goettingen, Germany
s.hengstler@stud.uni-goettingen.de

Abstract. Ensuring information security is an international problem and poses particular challenges for international companies. Research proposes various solutions for ensuring information security based on several theories such as the deterrence theory or the protection motivation theory. What is currently missing is a comparison of these theories in an intercultural context to test their comparability and different effectiveness. In our study, we empirically tested the theories and determined their comparability with invariance testing and predictive power between Germany, India and the USA using a SEM approach. Our results show differences in the effectiveness of the theoretical models across the three cultures. The results provide initial insights into the use of the theories in an international context and offer a practical approach to design culture-specific security measures

Keywords: Information Security Policy Compliance Behavior, Cross-cultural research, Deterrence Theory, Protection Motivation Theory

1 Introduction

With the increasing relevance of information security for ensuring successful business in the digital age, the need for effective measures to ensure secure employee behavior within organizations is growing [1]. As a basis for ensuring security behavior, companies define information security policies (ISP). ISPs are defined as “a set of formalized procedures, guidelines, roles and responsibilities to which employees are required to adhere to safeguard and use properly the information and technology resources of their organizations [2]”. Research on ISP compliance behavior (ISPCB) has already been developed a variety of contextualized theories to explain employee behavior, mainly using theories from other disciplines such as sociology, psychology, criminology or health care [3]. These approaches provide detailed insights into how ISPCB can be explained and influenced positively or negatively and helps in practice to design effective security measures [4].

However, the results of current research still highlight some less considered problems such as the analysis of cultural differences in ISPCB [5, 6]. This becomes particularly relevant when internationally operating companies want to define their security measures and use them in their heterogeneous cultural environment [7].

16th International Conference on Wirtschaftsinformatik,
March 2021, Essen, Germany

Existing research partially considers this problem when analyzing ISPCB [3, 8]. Previous research shows, for example, that the effectiveness of established measures to ensure information security can vary from one national culture to another [7]. Other culture-related studies analyze the cultural differences in information security attitudes and behavior of employees [9].

Thus, there is still a need for the examination of aspects that have not yet been taken into account to a sufficient extent. First, the current research describes that only a limited set of cultures have been analyzed at the national level for differences in terms of ISPCB [5, 10]. Second, existing approaches either do not use theories to describe cultural differences regarding ISPCB in their basic form or consider specific contexts, such as different security offenses [8, 11]. An analysis of theoretical mechanisms in a general ISPCB context offer the possibility of better comparability and more specific use of the results with existing and future research [12]. Currently, we cannot say whether current analyzed theories in ISPCB research differ in their predictive power and mechanisms in different countries because there is no common level of comparability. Therefore, the aim of this study is to investigate whether the predictive power of established theories and their mechanisms differ in different national cultures.

Our study addresses the mentioned gaps as follows. Using two of the most widely used theories in ISPCB research, the Deterrence Theory (DT) [8] and the Protection Motivation Theory (PMT) [13] we collected, analyzed and compared data sets with different cultural values from Germany, the USA and India using an SEM-PLS approach. We use the two theories mentioned above because they have different perspectives on ISPCB [3]. Our analysis comprises of three aspects. First, we conduct invariance testing to validate that the measurement instruments measure the same theoretical construct across our cultures. Second, there is an established tradition in information systems research in general, of comparing research models that have been developed and tested in earlier work [14]. Thus, we follow this approach and compare the predictive power and the mechanisms of the two theories [15]. We test for statistical differences between the explained variance in ISPCB using a Multi Group Analysis.

The rest of the paper is structured as follows. In the second section, we look at the cultural dimensions that are the basis for our cross-cultural comparison and describe the analyzed theories DT and PMT. We then develop the research model and present the explorative hypotheses underlying this study in the third section. Subsequently, the results of the study are presented. The study concludes with a discussion, limitations, contributions and an outlook on further research potentials.

2 Theoretical Background

2.1 The Concept of National Culture

The factor culture is an essential dimension that shapes an individual’s behavior and can be described as a summary of ideologies, beliefs, basic assumptions, shared norms and values, that have an influence on the collective will [16]. Existing research on information security and culture indicates a wide range of studies in which the influence of theoretical mechanisms on ISPCB are analyzed, based on national cultural differences. To apply these cultural differences, Hofstede's cultural dimensions provide a solid base for a comparison and are a widely used approach in information security research [9]. The dimensions consist of the constructs power distance (PD), uncertainty avoidance (UA), individualism/collectivism (COL), Masculinity/Femininity (MAS) and long-term orientation (LO). Power distance determines the degree to which people accept and expect that power is distributed unequally. Uncertainty Avoidance defines the degree to which people feel uncomfortable with uncertainty and ambiguity. Individualism is defined as a preference of individuals to take care of only themselves and their families. Collectivism is the opposite. Masculinity and Femininity can be related to tough vs. Tender cultures. According to Hofstede (2011) Masculinity represents values ass heroism, material rewards or success. Femininity is related to the preference for cooperation, modesty and quality of life. This orientation defines the degree to which long term values and traditions are balanced in contrast to thrift encouragement and efforts in modern solutions [17]. We used Hofstede’s cultural dimensions for two reasons. First, the dimensions have been rigorously developed and provide definitions for different cultural dimensions. Second, their application allows us to better integrate our theoretical findings in this stream of literature [7].

Table 1. Comparison of Cultural Dimensions between Nations

Cultural Dimension	**Country Score**		
	Germany	USA	India
Power Distance	35	40	77
Uncertainty Avoidance	65	46	40
Collectivism	67	91	48
Masculinity/Femininity	66	62	56
Long Term Orientation	31	29	61

We selected these three nations Germany, India and USA because, they have different values in Hofstede's cultural dimensions and thus, form a good basis for analyzing cultural differences at the national level. Table 1 shows that India has a higher value for PD than Germany or the USA, which means in the Indian culture it is more likely to accept the unequal distribution of power than in the national culture of Germany or the USA. Uncertainty avoidance differs more between Germany and the USA and India, which shows that in German culture uncertainty and ambiguity are described as more uncomfortable than in the U.S. and India. The COL dimension is strongest for the USA and lowest for India. It shows that the national culture of the U.S.A has a strong bias for collective action in society instead of emphasizing individualism. The dimension MAS shows similarly high values in all three cultures. LO is more pronounced in India than in the USA or Germany and shows that Indian culture emphasizes long-term values and traditions instead of thrift encouragement and efforts in modern solutions. Overall, the three national cultures show a good distribution in the characteristics of the cultural dimensions according to Hofstede and are therefore well suited for carrying out an intercultural comparison at the national level.

2.2 Deterrence Theory in Information Security Research

The DT has its origin in criminology and has been widely used in information security research [8]. The theory states that individuals will choose to commit an offence, if the benefits outweigh the underlying penalties. The DT further describes that the trade-off between benefits and the expected penalty can be further divided in different mechanisms, namely sanction certainty, sanction severity and sanction celerity [11]. When considering the DT in existing information security literature, a wide range of uses can be identified. The application of the original form of DT concentrates on the usage of formal sanctions to explain ISPCB, while other research additionally includes more informal consequences, such as informal sanctions like guilt and shame. Formal sanction severity is described as the formal expected amount of a penalty when a policy violation is committed, such as a fine or a warning, while an example for informal sanction severity could the loss of reputation among colleagues and superiors or shame. Formal sanction certainty describes the perceived probability of being formally punished if one is caught for an ISP non-compliant behavior, while informal sanction certainty describes probability of being informally punished by the social environment (e.g. at the workplace) [3]. Sanction celerity describes the velocity a person is punished if a crime was committed [18].

Both formal and informal sanction certainty and sanction celerity find empirical support in various contexts of information security research [19]. Since sanction severity and sanction celerity are considered as the two main components of deterrence theory, since celerity has received less empirical support in information security research so far, we only considered formal and informal sanction severity and sanction celerity in our research model [11].

2.3 Protection Motivation Theory in Information Security Research

The PMT has its origins in healthcare research. The theory states that a person, when confronted with a threat, cognitively weighs the threat and a possible related protective measure [20]. After assessing the threat and potential countermeasures to cope with it, the individual decides to adopt an adaptive or non-adaptive behavior. Adaptive behaviors are recommended responses designed to protect against a threat, whereas non-adaptive responses involve behaviors in which the threat recipient avoids implementing a recommended response. PMT assumes that the susceptibility to threats and the severity of the threat have a positive effect on a person's behavior and adaptation. Similarly, in its adapted form, the PMT contains further constructs used to constitute the protection motivation, such as response effectiveness, self-efficacy to comply and response costs, which have a direct influence on behavior [21]. Response cost describe the perceived extrinsic or intrinsic personal costs of performing the suggested adaptive behavior in terms of time, money or effort. Response efficacy is described as the perceived effectiveness of the behavior in mitigating or avoiding the perceived violation. Self-efficacy is defined as the confidence an individual possesses in effectively performing a recommended response and to complying with given ISP’s. Severity is defined as the perceptions of the seriousness of an information security violation. Susceptibility refers to the degree to which someone feels vulnerable to a specific violation of ISP's [13].

The constructs of the PMT find broad empirical support in information security research. Menard et al. (2017) analyze the impact of PMT on the individual motivation of information technology users. Johnston and Warkentin (2010) developed their fear-appeal model based on the PMT in order to convey the effectiveness of an antispyware software [22]. Moody et al. (2018) show that PMT constructs such as response efficacy, severity and susceptibility have an indirect effect on behavior [3]. However, current information security research lacks on studies on the relationship between PMT constructs and national culture [13, 20]. We, therefore, used the explained theoretical constructs of the PMT for our cross-cultural analysis.

3 Research Approach

3.1 Hypotheses development and Research Design

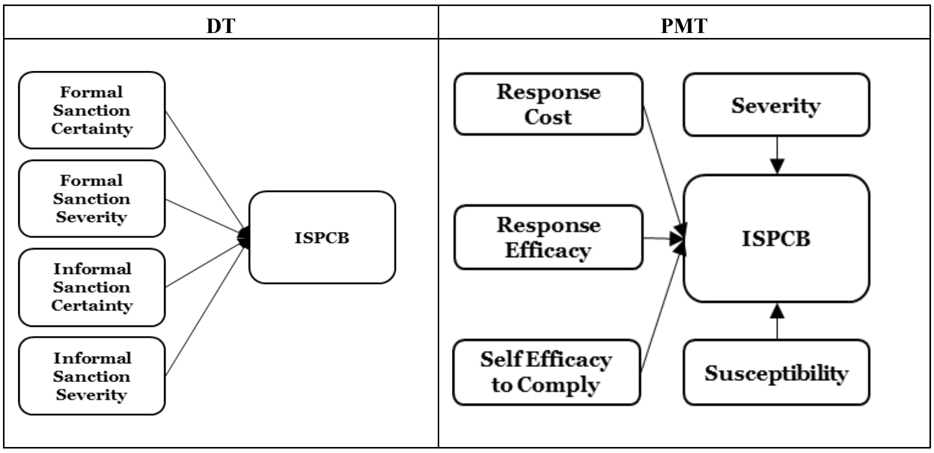
The hypotheses of a research project serve to answer the underlying research questions. However, in order to answer our research questions, we need to operationalize the theories we have introduced earlier in our study. The construct definitions from the DT and PMT were used to transfer the theories into a structural model displayed in Figure 1. This becomes necessary because the results of the structural model are needed to determine the effect strengths of the respective theory components on ISPCB. They are used to determine the predictive power of the theories for ISPCB. We furthermore analyze different effect sizes between the constructs along different cultures to identify significant differences as it has been shown that differences in cultural values can have an influence on behavior [17]. We draw on this argumentation and propose the following hypotheses:

H1: The predictive power of DT and the model's mechanisms differ across cultures.

H2: The predictive power of PMT and the model's mechanisms differ across cultures.

We conducted an empirical cross-cultural study to examine our underlying hypotheses. The operationalization of their variables follows a context-independent approach, measuring general ISPCB in order to make more generalized statements about the effectiveness of the theories and to compare their explanatory power throughout the culture samples [12]. For the measurement of behavior, the items of D'Arcy and Lowry (2019) were used and generalized for our study. Furthermore, we used 7-point Likert scales for our questionnaires. The items for formal and informal sanction severity and -certainty of the DT (3 items each) were adapted by Moody et al. (2018) and rephrased for our study [3]. The items used for the constructs response cost and response efficacy of the PMT were adapted by Floyd et al. (2000) (4 items each). Self-efficacy, severity and susceptibility were taken from Menard et al. (2017) and adapted (3 items each) [13, 20]. The used questions per item are listed in the appendix.

Figure 1. Research Models of DT and PMT.



We used an SEM approach and the partial least squares (PLS) method to test the theoretical models, because it has fewer sample size requirements and is characterized by excellent prediction [24]. We performed a cross-model comparison by using a multi-group analysis (MGA) to look for significant differences in the mean differences of the explained variance of our models across our samples as well as in the path coefficients of the analyzed theories (Welch-Satterthwait test) [25].

3.2 Data collection, Sample Characteristics and Common-Method Bias

A pilot study was conducted by sending the survey to five academic experts for review. A test run was then started with 60 participants for each sample, where at least 30 results per sample were complete and valid. The crowdsourcing platforms Amazon Mechanical Turk and Clickworker were used to collect the data, taking into account the quality criteria for using crowd working platforms, defined by Lowry et al. (2016) [26]. Only participants with their cultural background and origin from the respective sample (USA, India, Germany) were able to participate in our study. Their job acceptance rate on the platform must have been higher than 90%, and a certification of English language skills must be registered on the platform. We only selected participants which were employed, worked at least partially with a computer in their job and whose organization had an ISP. Additional attention checks were built into the study (e.g., requests to select a specific response) to avoid systematic response patterns. Participants were paid $1.65 for successful and conscientious participation in the study. In total, 767 people participated in the German survey, 623 in the survey within the USA and 481 people in the Indian survey. After applying the used quality criteria, the resulting samples consist of 422 (57%) valid responses collected in Germany, 263 (42%) in the USA and 252 (52%) in India. Demographic characteristics of the respondents were adapted from Hovav and D'Arcy (2012). The average age in all three countries is between 30 and 35 years. In all three countries, the proportion of men is higher than 60%. The majority of the participants work in a company with more than 1000 employees.

To carry out the common method bias test, we used the marker variable technique [27] and chose the respondent's outside activities as the theoretically unrelated marker variable [23]. The highest variance that the marker shares with another construct is less than 0.05. In addition, the path coefficients between the constructs showed no significant size changes (> 0.01 and not significant). In conclusion, the result suggests that there is no evidence of a common method bias in our study.

4 Data Analysis and Results

4.1 Measurement Models and Invariance Testing

To check our data for reliability, common quality criteria for reflective measurement models in IS research were applied to our study [28]. We used individual item reliability, composite construct reliability (CR), and average variance extracted (AVE) as indicators of convergent validity for our models. The factor loadings of the items for the DT and PMT model were all above 0.70, which indicates sufficient item reliability [29] (see appendix). The CR is higher than 0.70 for every variable used in each model, and the AVE is higher than 0.5 [28]. We furthermore used the Fornell and Larcker criterion to confirm discriminant validity by showing that for each model, the AVE for each construct is higher than the variance shared with other constructs (see square root AVEs as bold numbers in Table 2). [30, 31]. In summary, our results indicate that our measurement model is acceptable and reliable.

Table 2. Inter-construct correlations, construct reliability, and average variance extracted of Deterrence Theory Model.

Samples and Items		CR	AVE	FSC	FSS	ISC	ISS	ISPCB
Germany	**FSC**	0.884	0.719	**0.848**				
	FSS	0.917	0.786	0.581	**0.887**			
	ISC	0.913	0.778	0.468	0.496	**0.882**		
	ISS	0.919	0.79	0.409	0.551	0.649	**0.889**	
	ISPCB	0.938	0.834	0.347	0.318	0.428	0.378	**0.913**
USA	**FSC**	0.85	0.654	**0.809**				
	FSS	0.87	0.693	0.618	**0.832**			
	ISC	0.903	0.757	0.404	0.447	**0.87**		
	ISS	0.881	0.713	0.366	0.451	0.667	**0.844**	
	ISPCB	0.918	0.789	0.399	0.373	0.394	0.491	**0.888**

India	**FSC**	0.808	0.585	**0.765**					
	FSS	0.823	0.608	0.5	**0.78**				
	ISC	0.841	0.639	0.344	0.359	**0.799**			
	ISS	0.801	0.576	0.408	0.624	0.507	**0.759**		
	ISPCB	0.823	0.609	0.453	0.433	0.357	0.475	**0.78**	
Samples and Items		**CR**	**AVE**	**RC**	**REF**	**SEF**	**SEV**	**SUS**	**ICB**
Germany	**RC**	0.866	0.624	**0.79**					
	REF	0.906	0.708	-0.015	**0.842**				
	SEF	0.931	0.819	-0.167	0.328	**0.905**			
	SEV	0.918	0.788	0.155	0.197	0.095	**0.888**		
	SUS	0.944	0.85	-0.084	0.346	0.400	0.339	**0.922**	
	ISCPB	0.866	0.624	-0.162	0.333	0.495	0.074	0.467	**0.913**
USA	**RC**	0.926	0.759	**0.871**					
	RE	0.887	0.664	-0.199	**0.815**				
	SEF	0.916	0.784	-0.237	0.499	**0.885**			
	SEV	0.915	0.781	0.414	0.088	-0.003	**0.884**		
	SUS	0.905	0.761	-0.082	0.476	0.500	0.131	**0.872**	
	ISPCB	0.918	0.789	-0.263	0.597	0.603	-0.009	0.539	**0.888**
India	**RC**	0.87	0.628	**0.792**					
	REF	0.805	0.509	0.35	**0.714**				
	SEF	0.81	0.588	0.138	0.47	**0.767**			
	SEV	0.841	0.64	0.395	0.437	0.395	**0.8**		
	SUS	0.787	0.553	0.234	0.516	0.531	0.402	**0.743**	
	ISPCB	0.824	0.609	0.161	0.543	0.698	0.331	0.606	**0.781**

Notes (also for following tables): **FSC** = Formal Sanction Certainty. **FSS** = Formal Sanction Severity. **ISC** = Informal Sanction Certainty. **ISS** = Informal Sanction Severity. **RC** = Response Cost. **REF** = Response Efficacy. **SEF** = Self Efficacy. **SEV** = Severity. **SUS** = Susceptibility. The bold numbers on the leading diagonal are the square root of the AVE. *significant at 0.1; ** significant at 0.05; *** significant at 0.01.

Additionally, we tested for configural and metric measurement invariance. This step is necessary to create the ability to further analyze differences in the predictive power of the theories in a cross cultural manner [32]. Only if the charges of the similar items are invariant across groups, differences in the item scores can be meaningfully compared to the extent that they indicate similar group differences in the underlying construct [33]. To measure invariance, we performed a MGA and tested the differences in item loadings for all models between the three samples. We were not able to find significant differences between the item loadings of our samples and thus show metric invariance and comparability of our results.

4.2 Testing Theoretical Mechanisms across Cultures

We have tested the previously introduced path models with the PLS algorithm for estimating the structural model. We used the bootstrapping method to determine the significance of the path coefficients with 5000 bootstrap samples [28]. An overview of our significance levels of the individual path coefficients for all three models is given in Table 3.

Table 3. Structural Models of DT and PMT Research Model.

Model Path	Germany	USA	India	Germany / USA	Germany / India	USA / India
	Path Coefficients			**Significant Effect Differences**		
Deterrence Theory						
FSC -> ISPC	0.150***	0.211***	0.252***	NS	NS	NS
FSC -> ISPCB	0.018	0.052	0.124*	NS	NS	NS
ISC -> ISPCB	0.196***	0.058	0.105	S*	NS	NS
ISS -> ISPCB	0.164***	0.372***	0.213***	S*	NS	NS
Protection Motivation Theory						
RC -> ISPCB	-0.049	-0.086*	-0.011	NS	NS	NS
REF -> ISPCB	0.149***	0.307***	0.207***	S*	NS	S**
SEF -> ISPCB	0.324***	0.296***	0.467***	NS	S*	S*
SEV -> ISPCB	-0.062	-0.033	-0.049	NS	NS	NS
SUS -> ISPCB	0.279***	0.220***	0.279***	NS	NS	NS

While formal sanction certainty and informal sanction severity have a significant impact in all three models, formal sanction severity only applies to India and informal sanction certainty only to Germany. The mechanisms of PMT are almost equally applicable to all three cultures. While response efficacy, self-efficacy and susceptibility are applicable in all three models and severity has no significant effect in all of them, response cost is only significantly applied in the USA model.

We additionally identified some significant effects of our control variables (see appendix). Age has a significant effect on ISPCB in at least one of the samples for each theory. The company size and industry only have an influence in the DT model. Education affects at least one sample for each theory. For gender, only one significant effect can be found in the PMT model.

4.3 Comparing the Predictive Power across Cultures

In order to determine the predictive power of the theories and then compare them, we first considered the path coefficients of the individual models and determined whether significant differences exist in their height [25]. In the second step we compared the explained variance and also investigated whether significant differences exist. As analyzed in the previous chapter, different significances can be identified in the path coefficients of the DT models. However, it can be observed that only significant path differences can be identified in the informal sanctions. For example, ISC in the USA model is significantly higher than in the German model (significant at 0.1). The same difference can be found for ISS. The PMT model was tested using five different constructs. Response efficacy has a significant effect on ISPCB in all three models, whereas the effect in the USA is significantly higher than in Germany and India. There is a significant effect of self-efficacy on ISPCB in all models where the path coefficient in the Indian is significantly higher as in the USA and German one (significant at 0.1).

When interpreting the explained variance, the acceptable values depend on the research context [29]. In general, a proportion of the explained variance of an endogenous variable is considered low up to 0.32, moderate from 0.33 and substantial from 0.67. The R² adjusted in the DT model is in the medium range for the USA (0.350) and India (0.327), for the German sample slightly below the 0.32 limit at 0.291. However, the MGA showed that the difference between Germany and USA and Germany and India is significant (significant at 0.05). For the PMT models, all R² adjusted are in the medium range, whereas only the value for Germany is below 0.4 (0.358) and significantly different compared to the USA (0.520) and Indian (0.580) sample (significant at 0.05). The R² adjusted values for the PMT and DT model are above average [8]. The differences in the R² values may result from the different operationalisation of the theories, as we use basic models or have no further context-specific extensions in our models. Along the investigated theories we can see that there are significant differences in the path coefficients of the theories as well as in the R² of the models.

5 Discussion

5.1 Implications for Research and Practice

Our results show implications for research as well as for practice. The main purpose of this analysis was to empirically evaluate and compare the predictive power of the DT and PMT along three different national cultures. The results of the analysis provide different insights into the cultural differences when applying the theories and show interesting theoretical contributions. First, by applying configural and metric invariance between our cultural samples, we can show that our used models and items of the DT and PMT are understood in the same way across different cultures [33]. These results are the basic prerequisite for a comparison of the theories between the national cultures. Secondly, we were able to show that there are differences in the predictive power of DT and PMT mechanisms. We could show for our context that the theories have a small to medium-strong explanatory power. Significant differences along the cultures exist in the DT model between USA and Germany. In addition, we were able to show in our study that the PMT constructs response efficacy and self-efficacy explains the ISPCB significantly better in India and the USA than in Germany. Furthermore, our results show different effects for the effectiveness of formal sanctions in the USA than in existing research [7]. Our results provide important information on the effectiveness of models on ISPCB in order to define what types of measures are appropriate to ensure ISPCB in an international context. These findings indicate that ISPCB research needs to consider cultural differences in the use of DT and PMT. Our results provide a basis for more specific investigation, such as analysing the effects of individual cultural dimensions on the mechanisms of the theories analysed. Finally, we can contribute to a broader consideration of intercultural comparisons between more than two nations since we integrated national samples such as Germany and India which were previously less considered in cross-cultural research of ISPCB [6].

Practitioners can also benefit from the conclusions of our results. Our findings underline the relevance of a cultural differentiation of measures for the management of security breaches. Overall, in the future, it will be important to consider cultural differences when using security measures to positively influence ISPCB. Companies should pay attention to the fact that the measures work differently in different international locations. They should be designed with a culture-specific mode of operation in mind. An example of such differences is the use of sanctions. While our results show that the severity of an expected formal punishment in different cultures tends to be less effective ISPCB, the sole high probability that a formal punishment is to be expected is comparatively more effective.

5.2 Limitations and Future Research

For an adequate interpretation of our results, the following limitations of the study should be considered. On the one hand, we measured general ISPCB and did not specifically refer to one or more contexts. The general validity of our results cannot be proven by the fact that cultural differences can be context specific. Future research can take up this aspect and examine our results as a starting point for cultural differences in specific ISPCB contexts. Secondly, in order to compare different cultures, we have used three example cultures, which differ in their cultural dimensions according to [17]. Thus, our results are limited to the cultures we selected. In order to find out more about the differences between cultures, we need to involve further culture samples and take a closer look at the direct influences of cultural dimensions on specific behaviour. Furthermore, we could not consider the problem of a cultural shift in detail. For example, our samples from the different countries could be influenced by the individual cultural values of each subject. In order to obtain a detailed consideration of cultural values on the studied theoretical constructs and ISPCB, future studies should also measure culture on an individual level and investigate it in terms of its influence on ISPCB. [7]. Third, moderating factors could only partially be addressed in our work. More detailed differences and the involvement or deepening of other factors, such as an industry-specific investigation or an analysis based on different educational backgrounds, will be subjected to future research.

6 Conclusion

Studies on the analysis of ISPCB often show the need to consider their results from different cultural perspectives. However, existing studies in this area rarely take an empirical approach, look at given problems from different theoretical lenses and put the results into context. This study is the first to empirically test and compare three prominent theories that are often used to explain ISPCB. Furthermore, we were able to identify different types of effects in different cultures and that their effect strength can vary. Interestingly, both strong similarities and differences can be identified across theories. Other interesting aspects are constant effects along the three cultures analyzed, such as attitude or susceptibility as an effective factor for explaining ISPCB. Our results give a first impression of cultural differences in the effectiveness of different theoretical models and provide a starting point for the design and implementation of ISP's in an international environment. In summary, future research on ISPCB and culture should be based on these results when deciding for or against a theoretical lens and should conduct more specific analyses.

References

1. Barlow, J.B., Warkentin, M., Ormond, D., Dennis, A.R.: Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. Journal of the Association for Information Systems 19 (2018)
2. Lowry, P.B., Moody, G.D.: Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Info Systems J 25, 433–463 (2015)
3. Moody, G.D., Siponen, M., Pahnila, S.: Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly 42, 285–311 (2018)
4. Willison, R., Warkentin, M., Johnston, A.C.: Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives. Info Systems J 28, 266–293 (2018)
5. Cram, W.A., D'Arcy, J., Proudfoot, J.G.: Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. MISQ 43, 525–554 (2019)
6. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Computers & Security 32, 90–101 (2013)
7. Hovav, A., D'Arcy, J.: Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. Information & Management 49, 99–110 (2012)
8. Trang, S., Brendel, B.: A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. Inf Syst Front 21, 1265–1284 (2019)
9. Connolly, L.Y., Lang, M., Wall, D.S.: Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees. Information Systems Management 36, 306–322 (2019)
10. Chen, Y., Zahedi, F.M.: Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. MISQ 40, 205–222 (2016)
11. D'Arcy, J., Herath, T.: A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems 20, 643–658 (2011)

12. Aurigemma, S., Mattson, T.: Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research. Journal of the Association for Information Systems (2019)
13. Menard, P., Bott, G.J., Crossler, R.E.: User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. Journal of Management Information Systems 34, 1203–1230 (2017)
14. Srite, Karahanna: The Role of Espoused National Cultural Values in Technology Acceptance. MISQ 30, 679 (2006)
15. Brown, S.A., Venkatesh, V., Hoehle, H.: Technology adoption decisions in the household: A seven-model comparison. J Assn Inf Sci Tec 66, 1933–1949 (2015)
16. Leidner, D.F., Kayworth, T.: Review: a review of culture in information systems research: toward a theory of information technology culture conflict. MIS Quarterly 30 (2006)
17. Hofstede, G.: Culture's consequences. Comparing values, behaviors, institutions, and organizations across nations. Sage Publ, Thousand Oaks, Calif. (2011)
18. Vance, A., Siponen, M.T., Straub, D.W.: Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Information & Management 57, 103212 (2020)
19. Willison, R., Lowry, P.B., Paternoster, R.: A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence to Inspire New Directions in Behavioral and Organizational Security Research. JAIS, 1187–1216 (2018)
20. Floyd, D.L., Prentice-Dunn, S., Rogers, R.W.: A Meta-Analysis of Research on Protection Motivation Theory. Journal of Applied Social Psychology 30, 407–429 (2000)
21. M. Warkentin, N. Malimage, K. Malimage: Impact of Protection Motivation and Deterrence on IS Security Policy Compliance: A Multi-Cultural View. In: WISP 2012 (2012)
22. Johnston, Warkentin: Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly 34, 549 (2010)
23. D'Arcy, J., Lowry, P.B.: Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Info Systems J 29, 43–69 (2019)
24. Ringle, S., Straub, S.: Editor's Comments: A Critical Look at the Use of PLS-SEM in "MIS Quarterly". MIS Quarterly 36, iii (2012)
25. Rocha Flores, W., Antonsen, E., Ekstedt, M.: Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security 43, 90–110 (2014)
26. Lowry, P.B., D’Arcy, J., Hammer, B., Moody, G.D.: “Cargo Cult” science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. The Journal of Strategic Information Systems 25, 232–240 (2016)
27. Lindell, M.K., Whitney, D.J.: Accounting for common method variance in cross-sectional research designs. Journal of Applied Psychology 86, 114–121 (2001)
28. Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M.: A primer on partial least squares structural equation modeling (PLS-SEM). SAGE, Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne (2017)

29. Hair, J.F.: A primer on partial least squares structural equation modeling (PLS-SEM). Sage Publ, Los Angeles (2014)
30. Chin, W.: Issues and Opinion on Structural Equation Modeling. MIS Quarterly 22 (1998)
31. Fornell, C., Larcker, D.F.: Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research 18, 39 (1981)
32. Steelman, Z.R., Hammer, B.I., Limayem, M.: Data Collection in the Digital Age: Innovative Alternatives to Student Samples. MISQ 38, 355–378 (2014)
33. Henseler, J., Ringle, C.M., Sarstedt, M.: Testing measurement invariance of composites using partial least squares. International Marketing Review 33, 405–431 (2016)

Appendix

Table 4. Analyzed Control Variables.

Control Variables	**Deterrence Theory**			**Protection Motivation Theory**		
	Germany	USA	India	Germany	USA	India
Age	0.269***	0.138***	0.099*	0.057*	0.096**	0.029
Company Size	0.102***	0.008	0.037	0.013	-0.02	-0.017
Education	0.035	-0.138***	-0.061	0.099***	0.034	0.011
Gender	0.059	0.036	-0.026	0.065*	0.037	0.067*
Industry	0.120***	0.144***	0.132***	0.032	0.033	-0.031
Job Position	0.012	-0.033	0.024	-0.071	0.044	0.035

Table 5. Used Items.

Construct	Item
Formal Sanction Severity	1. How much of a problem would it create in your life if you violated the company information security policy? 2. How much of a problem would it be if you received severe sanctions if you violated the company information security policy? 3. How much of a problem would it create in your life if you were formally sanctioned if you violated the company information security policy?
Formal Sanction Certainty	1. What is the chance that you would be formally sanctioned (punished) if management learned that you had violated company information security policies? 2. I would receive corporate sanctions if I violated company ISP procedures. 3. What is the chance that you would be warned if management learned you had violated company information security procedures?
Informal Sanction Severity	1. It would create a problem in my life if my career was adversely affected for not complying with ISP procedures regularly. 2. It would create a problem in my life if I lost the respect and good opinion of my colleagues for not following ISP procedures regularly.

	3. It would create a problem in my life if I lost the respect of my manager for not complying with ISP procedures regularly.
Information Sanction Certainty	1. How likely is it that you would lose the respect and good opinion of your business associates for violating company information security procedures? 2. How likely is it that you would jeopardize your promotion prospects if management learned that you had violated company information security procedures? 3. How likely is it that you would lose the respect and good opinion of your manager for violating company information security policies?
Response Cost	1. Complying with information security procedures would be time consuming. 2. Complying with information security procedures would take work time. 3. Complying with information security procedures makes my work more difficult. 4. Complying with information security procedures inconveniences my work.
Response Efficacy	1. Complying with information security procedures in our organization keeps information security breaches down. 2. If I were to comply with information security procedures, IS security breaches would be scarce. 3. If I were to do the opposite to what Mattila did, it would keep IS security breaches down. 4. If I were to do the opposite to what Mattila did, IS security breaches would be minimal.
Self-Efficacy to Comply	I have the necessary ... to fulfil the requirements of the ISP (skills, knowledge, competencies).
Severity	An information security breach in my organization would be serious / severe / significant.
Susceptibility	1. My information and technology resources are at risk for becoming attacked. 2. It is likely that my information and technology will become compromised. 3. It is possible that my information and technology resources will become compromised.
ISPCB	1. I complied with the requirements of the ISP. 2. I protected information and technology resources according to the requirements of the ISP. 3. I carried out my responsibilities prescribed in the ISP when I used information and technology.