Transactions on Replication Research

Conceptual Replication DOI: 10.17705/1atrr.00067 ISSN 2473-3458

Toward a Unified Model of Information Security Policy Compliance: A Conceptual Replication Study

Miranda Kajtazi
Lund University School of Economics and Management, Department of Informatics, Sweden
miranda.kajtazi@ics.lu.se

Nicklas Holmberg
Lund University School of Economics and Management, Department of Informatics, Sweden
nicklas.holmberg@ics.lu.se

Saonee Sarker
McIntire School of Commerce, University of Virginia, USA
saonee@viginia.edu

Christina Keller
Lund University School of Economics and Management, Department of Informatics, Sweden
christina.keller@ics.lu.se

Björn Johansson
Department of Information Systems and Digitalization, Linköpings University, Sweden
bjorn.se. johansson@liu.se

Olgerta Tona
Department of Applied IT, University of Gothenburg, Sweden
olgerta.tona@ait.gu.se

Abstract:

Moody et al. (2018) presented a unified model of information security policy compliance (UMISPC) to explain information systems security (ISS) behaviors. The model was empirically tested against 3 main types of security-related behavior: USB practices, not locking computers appropriately, and password issues. In this study, we present a conceptual replication of Moody et al. (2018) in order to provide stronger empirical support. To this end, our study has empirically examined UMISPC through three types of ISS behaviors within a work environment in the European Union (EU), where General Data Protection Regulation (GDPR) is in force. The replication of the empirical study with the three scenarios is original. While the replication in general highlights the strength of UMISPC, the results also indicate some differences from the original study and show that there is still room for improving some of its theoretical concepts.

Keywords: Information Security Policy, Conceptual Replication, UMISPC, Compliance

The manuscript was received 1/15/2019 and was with the authors 6 months for 5 revisions.

Introduction

It is well-acknowledged that data is one of the key assets of an organization (Johnson et al., 2015). Recent digitization processes have led organizations to gain a reputation for data insecurity, which in turn forces them to proactively prioritize security (Ritter and Pedersen, 2019). A large factor contributing to this reputation comes from data breaches that unfold due to 1) internal negligence or mistakes, 2) complicated information security policies (ISPs) that are difficult to interpret, and 3) lack of proper enforcement and compliance. Specifically, ISPs have become a part of organizational security processes for more than a decade (D'Arcy et al., 2009). Current information systems (IS) research acknowledges that organizational employees rarely comply with ISPs (Puhakainan and Siponen, 2010), a problem that still remains evident today (Moody et al., 2018). Consequently, much of recent IS research has focused on understanding why employees engage in "insecure information security actions" (Moody et al., 2018, p. 286), and a number of competing theoretical models have been proposed and empirically validated to address this (see Moody et al. (2018) for a review of this literature). To provide a more synthesized and unified understanding of ISP compliance (or lack thereof), Moody et al. (2018) recently presented the Unified Model of Information Security Policy Compliance (UMISPC).

While this new model is comprehensive and makes important contributions, we believe that owing to more recent security compliance-related policies that have been introduced in Europe (and not addressed by Moody et al. (2018)), there is an opportunity for replication to help build a cumulative body of knowledge on this topic. Specifically, we refer to the General Data Protection Regulation (GDPR)[1] introduced by the European Union (EU) in May 2018, known as the strongest developed rule on data protection in the world. There are views that GDPR has already made drastic changes in how data is stored, processed and distributed, however, its effects remain to be witnessed scientifically. GDPR has a large applicable context and applies to any organization holding or processing personal data of EU citizens. Consequently, it targets organizations that operate not only within EU but also outside its borders (e.g. Google, Facebook etc.). We argue that much like other ISPs, the success of GDPR will depend on how employees and their organizations comply with it and whether the (so far) identified factors affecting compliance will hold in the context of GDPR. Recent literature suggests that since GDPR was introduced more as a "directive" than a "regulation," its interpretation and enforcement issues have been slightly open-ended (Adshead, 2016). At the same time, greater awareness of GDPR among the general population has also resulted in greater vigilance, and thereby potentially changing/impacting compliance behaviors. For example, Ooijen and Vrabec (2019) found in their study that just having the perception that GDPR provides more control to general consumers altered their behavior and decision-making. Thus, the aim of this study is to conduct a conceptual replication of Moody et al. (2018) with empirical support, post the introduction of GDPR. We believe that the dialectic of increased vigilance on one hand, and the interpretive flexibility offered by GDPR on the other, can potentially alter compliance behaviors within the EU and illuminate interesting deviations in the UMISPC model. Moody et al. (2018) tested their developed model using three different types of ISP violations and called upon future researchers to replicate their study using additional ISP violations to assess the applicability of their UMISPC model. Our replication study only seeks to respond to their first call by replicating the existing study. However, we recommend (and support) the expansion of other replication studies in the future by employing contextualized scenarios that target the effectiveness of not only GDPR but also other similar privacy laws that are emerging around the world (e.g., the California Consumer Privacy Act (CCPA)) in reference to compliance with security rules and regulations.

Original Model

The UMISPC was developed through three main steps: 1) a rigorous review of eleven different underlying theoretical models used in explaining ISP compliance; 2) empirically comparing the eleven different theories; and, finally 3) drawing on empirical and conceptual similarities (Moody et al., 2018, p. 286) across the different theories. Table 1 lists the 11 theories and the model fit statistics presented in Moody et al. (2018).

[1] https://gdpr-info.eu

Table 1. Model Fit Statistics for the Original Theories in Moody et al. (2018)

Theory	RMSEA	CFI	TLI	CD
Neutralization techniques	0.103	0.726	0.687	1.000
Health belief model	0.087	0.864	0.837	1.000
Theory of reasoned action	0.053	0.944	0.956	1.000
Protection motivation theory	0.080	0.875	0.844	1.000
Theory of interpersonal behavior	0.077	0.724	0.798	1.000
Deterrence theory	0.115	0.655	0.607	1.000
Extended protection motivation theory (PMT2)	0.070	0.811	0.789	1.000
Theory of planned behavior	0.097	0.807	0.927	1.000
Theory of self-regulation	0.123	0.805	0.866	0.965
Extended parallel processing model	0.047	0.880	0.868	1.000
Control balance theory	0.118	0.802	0.849	1.000

RMSEA Root mean squared error of approximation (should be below .10); CFI Comparative fit index (should be above .90); TLI: Tucker-Lewis index (should be above .90); CD: Coefficient of determination (should be above .90)

The results of the three different steps followed by Moody et al. (2018) are presented in the original study under Figures 1, 2 and 3. Below, we present the refined and empirically tested model in Moody et al. (2018).

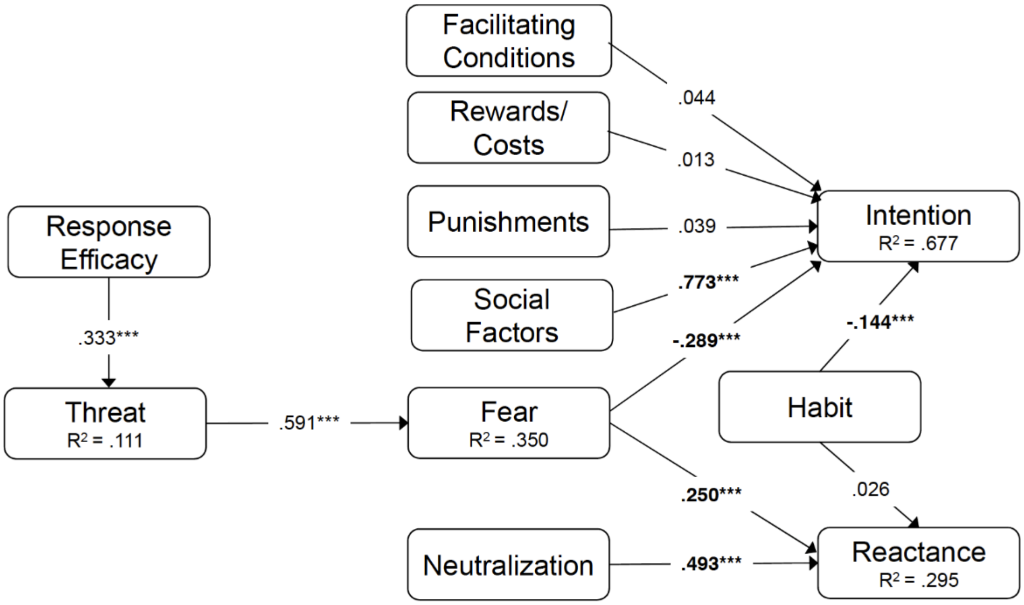

Figure 1. UMISPC Results as in the original study by Moody et al. (2018)

We also present the model that was refined by Moody et al. (2018) post the results from their model testing. In this replication study, we empirically test the refined model of Moody et al. (2018). In the upcoming sections, we present more details of the methodology and analysis.

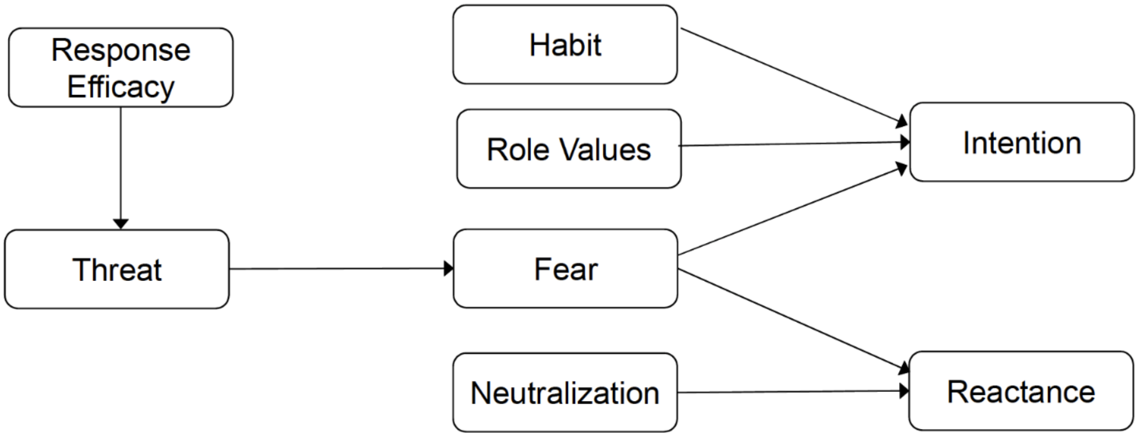

Figure 2. Refined UMISPC as in the original study by Moody et a. (2018) tested in the current replication study.

Among the three classical approaches to replication proposed by Dennis and Valacich (2014), our current study may be considered as a conceptual replication. In our study, we continue to test the same research question and hypotheses as proposed by Moody et al. (2018), with the same measurements, with only one alteration. Specifically, the analyses were conducted using the PLS-SEM based tool of SmartPLS 3.0 (Ringle et al., 2015), which was deemed appropriate to replicate the finalized model of UMISPC (see Figure 2). Next, we discuss our methodological approach.

Research Methodology

Given that our study involved a conceptual replication, we tested the final theoretical model named UMISPC with the use of the same measures, except for one alteration in the construct of Reactance. We eliminated one item from the measure of Reactance, because we believed that the wording of the items was not appropriate to the context. Furthermore, we have used a different method for analyses. We aimed to replicate the final model of UMISPC using SmartPLS 3.0.

The choice of our sample was a bit different from the original study. While Moody et al. (2018) used a more traditional sampling approach, but demographically with a diverse sample (employees obtained through a random selection from a large pool of alumni at a particular Finnish university), Bulgurcu et al. (2010) argue that an online panel offers a diversity of respondents and reduces the potential bias that could arise from a single organization. Therefore, we used an online panel for data collection, with a random sample from multiple companies (including small, medium, and large organizations) that are information-intensive. The majority fall under the GDPR regulation, with very few (ca. 17.5, residing and working outside EU such as under CPPA, although had clear links to the EU: they were originally European citizens and some work for companies that handle EU citizen data).

Demographics

Our sample targeted organizations that handle EU citizens' personal and/or organizational data. Moody et al. (2018) targeted alumni from a Finnish university, however, they did not inform the readers whether the alumni were working for a company that handles EU citizen data, where GDPR would have been enforced. Even if this was the case, GDPR only came into force May 2018, therefore, it would not have been possible for the original study to see any GDPR effects in time. In reference to GDPR, this study defines personal data as "any information relating to an identified or identifiable natural person ('data subject')".2

Table 2 presents our key demographics. A total of 402 useful responses were collected, with each scenario receiving almost the exact same number of responses. This was made possible with Qualtrics as the survey design tool. We analyzed the differences between the three samples collected for each scenario, and we separately analyzed the USB-drive scenario in further detail to check for inconsistencies and whether the

[2] https://gdpr-info.eu/art-4-gdpr

type of scenario affected the results. No difference was found in the results between the larger sample and that from one particular scenario. Moody et al., (2018, p. 303) also reported that "no systematic difference was found between the samples". We further tested for any variance with the general control variables, such as gender and within a specific scenario, however, we did not find any significant differences. The control variables: fear, habits, role values and neutralization were included in the model testing. While our initial belief was that country of residence and the specific workplace would affect views surrounding security, this was not reflected in the results. We however report this with caution, since the number of respondents in our sample was not enough for testing country-level differences.

The questionnaire was designed on Qualtrics, further distributed with the demographics presented in Table 2 by Prolific. We included a control for Nationality in Prolific to gather as many EU participants as possible. Each participant was reimbursed with a recommended amount, by Prolific, to respond to our survey. The distribution of the survey, with all the three scenarios, was evenly made amongst the participants, thus we had an even distribution of our respondents.

Table 2. Demographics

	Number of Respondents	**Percentage of Respondents**
Gender		
Female	209	51.35
Male	195	47.81
Other	3	0.74
Age		
Under 20	2	0.49
21-30	119	29.24
31-40	158	38.82
41-50	74	18.18
51-60	43	10.57
Above 60	11	2.7
Country of Residence and Workplace		
Within EU	336	82.55
Outside EU	71	17.44
TOTAL	407	100

Retaining the Original Scenarios

Moody et al. (2018) introduced three scenarios to test their model. In this study, we have retained all three of the original scenarios: Scenario 1 – USB drive, Scenario 2 – workstation logout and Scenario 3 – passwords (presented in Appendix B). We consulted recent practitioner literature and news, GDPR policy documents (including details on Article 29), as well as research in the reference disciplines. This helped us to further understand the most common ISP compliance violations (e.g., the Oracle list). The specific scenarios (e.g., password sharing or unlocking computers) are still represented in such lists, confirming that scenarios of this nature have been re-used over the years (Siponen and Vance, 2010; Vance and Siponen, 2012) and may show better strength in confirming the replication as in the original study.

Data Analyses

The structural model of UMISPC (Moody et al., 2018) was tested using the component-based partial least squares (PLS) approach to structural equation modelling. Our choice of PLS was guided by recent literature within the IS discipline. The efficacy of PLS as an analysis technique have long been debated, with many arguing that PLS works better with small sample sizes (e.g., Chin 1998; Chin et al. 2003). In a more recent study, Goodhue, Lewis, and Thompson (2012) conducted a series of comparative analysis between PLS, regression, and Lisrel. They found all three techniques to be fairly equivalent in terms of accuracy, predictive power, and robustness across a range of criteria such as small sample size, non-normal data, and complex/simple models. However, they conclude by stating that in the context of a complex model and relatively smaller sample size "PLS had the smallest occurrence of false positives" (Goodhue et al. 2012, p. 998). They defined complex models as those with around seven constructs. Given that our model has the same number of constructs, and a moderate sample size of 409, in an effort to reduce false positives, we used the PLS technique for our analysis.

We first evaluated the psychometric properties of measurement scales following with a test of the hypotheses using the Smart-PLS software package (version 3.2.8) (Ringle et al., 2015). Whilst the original study depended on STATA's confirmatory factor analyses, with the intention to apply the model fit approach for selecting the fully fitted model, our intention was different. We aimed to test the fully fitted model, that of UMISPC, with the justification that the PLS approach allows us to examine the final model and its structural paths, by ignoring other covariance that is not explicitly stated in the model (Straub et al., 2004). We also deemed this approach suitable and reasonable for the purpose of replicating UMISPC, with which we predict its validity, rather than test it as a well-established theory. PLS is also regarded as more suitable when the purpose of the structural model is to predict (such as ours), rather than to test well-established theory. Moreover, it is suitable in terms of our sample size and residual distributions (e.g., Hair et al., 2017; Chin, 1998). In fact, we recognize that UMISPC can become a well-established theory. Therefore, we chose to test it in an exploratory fashion, by testing its strength in a new context.

UMISPC is built upon reflective constructs that we assessed by examining their convergent validity, individual item reliability, composite reliability, and discriminant validity of the measurement model (Barclay et al., 1995). Appendix A presents the analyses in Tables 3 to 7. Table 3 shows the descriptive statistics for the measurement items and item loadings, followed by standard deviations and t-statistics. Table 4 presents Cronbach's Alpha where the construct of reactance was shown to be under the threshold of 0.7 with 0.622, particularly because of our intention to test it on the basis of items 1, 2, 3, rather than items 2, 3, 4. This emphasized that item 1 was not reliable due to its wording, and therefore, we finally retained items 2 and 3 only. It is common to find problems for the Cronbach's Alpha with a number of items that are too few and are less Tau-equivalent reliable (Henseler et al., 2015). Composite Reliability and the Average Variance Extracted (AVE) values for all reflective constructs were greater than the minimum recommended value of 0.50 (Convergent Validity) and 0.75 (Composite Reliability) except for role values that showed to be just under the threshold in both cases. The values for all the constructs except for role values in the structural model of UMISPC reach good thresholds, demonstrating that those constructs have adequate reliability assessment scores (Internal Consistency and Scale Reliability) (Gefen et al., 2000). In this regard, we highly recommend that the construct of reactance should include items 2, 3 and 4. Since the measures of all other constructs had adequate reliability and validity assessments, all the measurement items of these constructs were fully tested in the structural model.

It is also important to notice that the scenario approach replicated from Moody et al. (2018) gave us confidence to rely on 407 responses and test the refined UMISPC model without being concerned about the three different contexts in the three scenarios, whether they present vast differences. According to Moody et al. (2018), if the three scenarios led them to receive different results, then the entire context with scenarios must be avoided and include direct behavior questions to test what influences the differences. Moreover, while we did not see major differences like Moody et al. (2018), we cannot conclude that such differences would not be visible if our response rate in PLS-SEM met the required minimum of ten responses/item to deem the results credible (Hair et al., 2011). In our study, we only present 407 responses in total that are divided into 3 scenarios, with approximately 135 responses/scenario, while we tested 34 items across 8 constructs.

Subsequently, we estimated the structural model and tested the research hypotheses. The results of the UMISPC model estimation are presented in Figure 3.

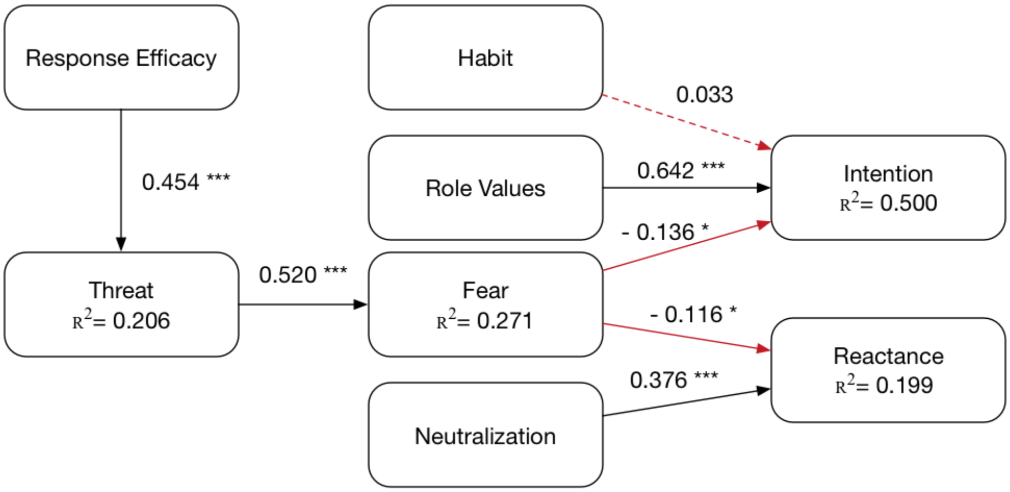

Figure 3. UMISPC Structural Model Testing

The data analysis was conducted by using a bootstrapping resampling method with 1000 resamples. The standardized path coefficients, which are based on two-tailed t-tests, show that all of the proposed hypotheses, except for habit->intention, are supported.

Furthermore, the results show that the independent variables explained approximately 50% of the variance of intentions. As predicted in the UMISPC, fear had a significant negative impact (p < .002) and role values had a significant positive impact (p < .001) on intentions. However, we did not find a significant relationship between habit and intentions. The results also show that fear had a significant negative impact on reactance (p < .041) while the original study showed a significant positive impact. The rest of the values are consistent with Moody et al. (2018). Table 3 presents the t-values.

Table 3. T-Statistics

Constructs	T Statistics (|O/STDEV|)	P Values	Consistent with Moody et al. (2018)
Fear -> Intention (-0.136*)	3.153	0.002	Yes
Fear -> Reactance (-0.116*)	2.048	0.041	No
Habit -> Intention (0.033)	0.7	0.484	No
Neutralization -> Reaction (0.376***)	7.052	p < .001	Yes
Response Efficacy -> Threat (0.454***)	11.039	p < .001	Yes
Threat -> Fear (0.520***)	12.9	p < .001	Yes
Role Values -> Intention (0.642***)	18.333	p < .001	Yes

Discussion of Results

This study is the first to validate the UMISPC model using a sample of respondents post implementation and routinization of GDPR in Europe. Our findings are in line with Moody et al.'s (2018) final model, but have a few notable differences. Of great importance is how further research in this direction can decompose the construct of role values that evolved with multiple theoretical fronts, with the aim to fine tune the low scores on Cronbach's Alpha, Composite Reliability and AVE.

Approximately 50% of the variance of intention was explained by the independent variables. In contrast to Moody et al. (2018), which found a significant negative impact of habit on intentions; this study did not find a significant relationship. While we highlighted the study's context within EU post-GDPR implementation, we have not re-designed this replication study with the aim to present any anticipated differences with Moody et al. (2018) as a result of GDPR. However, we have rather explored whether such differences are present by replicating the scenarios and testing the refined UMISPC. A relevant question to be asked then is if the introduction of GDPR has changed habits.

We further reflect on the constructs of fear, habits and reactance and their power to influence intentions and particularly on the relationship of our unsupported hypothesis of habits->intentions. Contrary to Moody et al. (2018), we found that fear has a significant negative impact on reactance. In response to our results, we consider that the construct of fear was found to be less effective in our study primarily because, within the EU context, it shows that penalties for such wrongdoings are not severe. For example, losing a job due to misconduct in response to ISP violation is not probable, particularly if such violation happens due to internal negligence or mistakes that both this study and the original study report. To support this argument, we reviewed the legal status of termination of employment relationship by the European Commission (see e.g., European Commission, 2006). It explicitly shows that employment in the EU is highly regulated and employees' rights are mature enough to allow employees for an open discussion with their employer in case of misconduct, particularly if that happens due to internal negligence or mistakes, overshadowing fear. In that continuum, GDPR has clear guidelines on how to report data breaches that would positively influence employees for disclosure, rather than try to cover actions that when discovered (often not if) can have greater consequences. It is important not to overlook Article 29 of GDPR in this context. Moody et al. (2018) suggests that the fear of security risks may not be as threatening as that of health risks, and thus sometimes, the effect of fear may not be that consistent or strong. Our results suggest a similar effect. Shen (2015) goes on to suggest that in the context of psychological reactance, when fear is aroused and then reduced, reactance may be mitigated. We also considered the fact that GDPR's data subject (also known as the individual user) holds the power of data. Hence, when individuals share private data with organizations, organizations are forced to be more vigilant in following the rights and freedom of data processors of the individual's data. In the context of our study, even if one viewed the violations in the scenarios as potentially problematic, the protections offered by the GDPR may have reduced those fears and thereby generated more muted reactions and consequently an inverse relationship between the two. More importantly, the enforcement of privacy laws that are emerging around the world (like GDPR and CCPA) have shown that organizations are encouraged to increase investments in cybersecurity (IBM Security, 2020), with the potential to turn around fear within an organizational context. This in turn has direct implications for exogenous factors, such as a higher gained trust among customers. When dealing with trust from the customer's perspective and organization's geographical operation, cultural properties are crucial for understanding why fear may no longer be a credible influential factor.

To further argue on the finding related to the construct of habit, Moody et al. (2018) suggest that habit is related to the complexity of ISP violation and that future research should look at the possibility for employees to become habitual non-compliers with ISPs. It could also be that in a post GDPR world, organizations increase investments for their governance of cybersecurity technologies (IBM Security, 2020) and as a result are capable of setting clearer cybersecurity agendas for how their employees should follow protocols owing to greater vigilance and awareness.

Furthermore, it might be more worthwhile for future research to re-examine the measures of fear and reactance. Given that some of the items of reactance did not demonstrate good psychometric properties, and the inconsistent results between fear and reactance, deeper look at the measures is warranted. Furthermore, from a methodological perspective, we report that testing items 1, 2 and 3 of reactance instead of items, 2, 3 and 4 as in the original study, shows that we only had support for items 2 and 3 and that item 4 would probably have shown support as well, while the wording of item 1 gave a reverse effect to respondents. Thus, further construct development of reactance by focusing on the wording of item 1 can have the potential to expand the measurements of reactance and strengthen it theoretically.

Limitations

This study is limited to respond only to the first call of Moody et al. (2018) through using the three different types of ISP violations; although, the elimination of one item of reactance can be considered a contextual limitation. Data collection was limited to an online panel primarily targeting organizations managing EU citizens' personal and/or organizational data (with only ca.17.5% operating outside the EU context). While this replication study intended to capture the relevance of the UMISPC model post GDPR, our arguments considered carefully the 17.5% of our respondents who reside and work outside of the EU, yet they had a clear connection to the EU.

Conclusion and Future Research

This study aims to conceptually replicate the UMISPC model by Moody et al., (2018). In contrast to the original study, this research is based on empirical data collected in organizations mostly operating in the EU context with the purpose of exploring and understanding any potential effects of GDPR. This study shows that the reliability of the UMISPC model generally holds strong with all but one hypothesis being supported. Future research supporting further advancements of UMISPC should be built around the constructs of: a) role values, where its multiple items drawn from a range of different theories, should be carefully reviewed; (b) fear, where its extreme fear- induced positioning did not have a major effect on our respondents thereby indicating that we are in need of a more universal view of fear that may apply in many contexts, including that of the EU; c) reactance, where its items downplay the role of the critical scenarios and stands at the other end of extreme compared to fear. Further, habit should be developed and theorized to actually find support that employees can be considered habitual non-compliers of organizational ISPs. The latter is significant because internal negligence or mistakes do not necessarily have to be habitual. Our analyses is the first step to testing UMISPC outside of its current scope, by using another kind of data collection that tends to highlight the importance of ISP violation in a mostly GDPR-related context (ca.17.5% of our respondents were outside EU), and also by applying another method for data analyses, PLS-SEM. Tackling ISP violation is an important first step in protecting organizations' most valuable asset, namely data, and we hope that our study contributes towards a cumulative understanding of the roadblocks to ISP compliance and noncompliance and provides more credibility to a theoretical framework such as UMISPC.

References

Adshead, D. (2016). Impact of EU-GDPR on local authorities in the UK. Masters Degree. Sheffield Hallam University.

Barclay, D., Higgins Ch., & Thompson, R. (1995). The partial least squares approach to causal modelling. *Technology Studies,* 2(2), 285-324.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.

Chin, W. W. (1998). Commentary: Issues and Opinion on Structural Equation Modeling. *MIS Quarterly*, 22(1), vii–xvii.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research*, *295*(2), 295-336.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, 14(2), 189-217.

Dennis, A. R., & Valacich, J. S. (2014). A replication manifesto. *AIS Transactions on Replication Research,* 1(1), 1-15.

European_Commission (2006). *Termination of employment relationships, Legal situation in the Member States of the European Union.* Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjUlZ6Q3_HnAhUDCewKHWcXAPgQFjAAegQIBRAB&url=https%3A%2F%2Fec.europa.eu%2Fsocial%2FBlobServlet%3FdocId%3D4623%26langId%3Den&usg=AOvVaw1blH-KgWg5pADrqNi4bgLJ.

Furedi, F. (2006). *Culture of Fear Revisited. Risk-taking and the Morality of Low Expectations* (4th ed.). London: Continuum.

Gefen, D., Straub, D. W., and Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems*, 4(1), 1-77.

Goodhue, D. L., Lewis, W., & Thompson, R. (2012). Does PLS have advantages for small sample size or non-normal data?. *MIS Quarterly*, 36(3), 981-1001.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *The Journal of Marketing Theory and Practice*, 19(2), 139-152.

Hair, J., Hollingsworth, C. L., Randolph, A. B., & Chong, A. Y. L. (2017). An updated and expanded assessment of PLS-SEM in information systems research. *Industrial Management & Data Systems*, 117(3), 442-458.

Henseler, J., Ringle, Ch. M., & Sarstedt, M. (2015) A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115-135.

IBM Security. (2020). Cost of a Data Breach Report. *Ponemon Institute and IBM Security*. Retrieved from https://www.ibm.com/security/data-breach.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), 285-311.

Puhakainen, P., & Siponen, M. (2010). Improving employee’s compliance through IS security training: An action research study. *MIS Quarterly*, 34(4), 757-778.

Ringle, C., Wende, S. and Will, A. (2015). SmartPLS 3. Boenningstedt: SmartPLS GmbH. http://www.smarpls.com

Ritter, T., & Pedersen, C. L. (2019). Digitization capability and the digitalization of business models in business-to-business firms: Past, present, and future. *Industrial Marketing Management*, 86, 180–190.

Shen, L. (2015). Antecedents to psychological reactance: The impact of threat, message frame, and choice. *Health communication*, *30*(10), 975-985.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly,* 34(3), 487-502.

Straub, D., Boudreau, M., & Gefen, D. (2004) Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, 13(1), 380-427.

Vance, A., & Siponen, M. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing,* 24(1), 21-41.

van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy*, 42**,** 91–107.

Vauntisjövari, T. (2006). Corporate social reporting in the European context and human resource disclosures: An analysis of Finnish companies. *Journal of Business Ethics*, 69, 331-354.

Wennberg, K., Pathak, S., & Autio, E. (2013). How culture moulds the effects of self-efficacy and fear of failure on entrepreneurship. *Entrepreneurship & Regional Development*, 25(9), 756-780.

Appendix A: Statistics

Table A1. General Statistics

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)
AppealHighLoy_1 <- Neutralization	0.895	0.896	0.018	50.927
Condemnation_3 <- Neutralization	0.895	0.896	0.012	72.562
DenialInjury_3 <- Neutralization	0.908	0.908	0.014	64.698
Fear_10 <- Fear	0.891	0.890	0.014	63.731
Fear_11 <- Fear	0.830	0.828	0.023	36.400
Fear_7 <- Fear	0.843	0.843	0.015	56.442
Habit_1 <- Habit	0.744	0.739	0.038	19.601
Habit_11 <- Habit	0.817	0.816	0.023	34.931
Habit_12 <- Habit	0.856	0.855	0.020	43.898
Habit_2 <- Habit	0.846	0.844	0.028	30.125
Habit_3 <- Habit	0.858	0.856	0.024	35.355
Habit_5 <- Habit	0.890	0.889	0.015	60.741
Habit_7 <- Habit	0.838	0.835	0.026	32.580
Habit_8 <- Habit	0.817	0.815	0.024	34.340
Intention_1 <- Intention_	0.978	0.978	0.005	203.176
Intention_2 <- Intention_	0.979	0.979	0.005	209.276
PercSeverity_3 <- Threat_	0.904	0.904	0.012	76.838
PerceivedVulnerab_1 <- Threat_	0.924	0.924	0.01	88.512
PerceivedVulnerab_2 <- Threat_	0.943	0.943	0.007	131.936
PerceivedVulnerab_3 <- Threat_	0.92	0.92	0.012	76.144
Reactance_2 <- Reaction	0.723	0.724	0.055	13.151
Reactance_3 <- Reaction	0.943	0.943	0.017	56.375
ResponseEfficacy_2 <- Response Efficacy	0.752	0.754	0.038	19.84
ResponseEfficacy_3 <- Response Efficacy	0.886	0.885	0.017	51.856
ResponseEfficacy_4 <- Response Efficacy	0.863	0.861	0.024	36.157
Roles_2 <- Role Values	0.661	0.66	0.036	18.345
Roles_3 <- Role Values	0.84	0.838	0.018	46.538
SelfControl_1 <- Role Values	0.485	0.484	0.056	8.623
SelfControl_2 <- Role Values	0.547	0.545	0.056	9.728
SelfControl_3 <- Role Values	0.318	0.314	0.066	4.853
Affect_1 <- Role Values	0.840	0.840	0.015	56.581
Affect_4 <- Role Values	0.744	0.742	0.030	25.010
MoralDefinitions_1 <- Role Values	-0.718	-0.716	0.031	23.244
PercBehavCtrl_2 <- Role Values	-0.229	-0.237	0.071	3.22

Table A2. Cronbach's Alpha, rho_A, Composite Reliability and AVE

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Fear	0.822	0.856	0.891	0.731
Habit	0.937	0.943	0.948	0.696
Intention_	0.956	0.956	0.978	0.958
Neutralization	0.882	0.884	0.927	0.809
Reaction	0.622	0.854	0.825	0.706
Response Efficacy_	0.781	0.788	0.874	0.699
Role Values_	0.574	0.864	0.693	0.401
Threat_	0.942	0.942	0.958	0.852

Table A3. Cross Loadings

	Fear	Habit	Intention	Neutralization	Reaction	Response Efficacy_	Role Values_	Threat_
Fear	1.000	0.332	-0.439	-0.505	-0.306	0.422	-0.488	0.52
Habit	0.332	1	-0.235	-0.383	-0.312	0.352	-0.347	0.299
Intention_	-0.439	-0.235	1	0.601	0.376	-0.367	0.697	-0.471
Neutralization	-0.505	-0.383	0.601	1	0.434	-0.433	0.724	-0.484
Reaction	-0.306	-0.312	0.376	0.434	1	-0.296	0.429	-0.377
Response Efficacy_	0.422	0.352	-0.367	-0.433	-0.296	1	-0.447	0.454
Role Values_	-0.488	-0.347	0.697	0.724	0.429	-0.447	1	-0.513
Threat_	0.52	0.299	-0.471	-0.484	-0.377	0.454	-0.513	1

Table A4. Latent Variable Correlations

	Fear	Habit	Intention	Neutralization	Reaction	Response Efficacy	Role Values	Threat
N_AppealHighLoy_1	-0.475	-0.33	0.58	0.895	0.371	-0.391	0.68	-0.465
N_Condemnation_3	-0.458	-0.376	0.478	0.895	0.414	-0.387	0.626	-0.414
N_DenialInjury_3	-0.432	-0.323	0.569	0.908	0.385	-0.39	0.652	-0.43
F_Fear_10	0.891	0.301	-0.33	-0.388	-0.218	0.309	-0.387	0.442
F_Fear_11	0.83	0.242	-0.27	-0.312	-0.143	0.245	-0.315	0.369
F_Fear_7	0.843	0.296	-0.474	-0.54	-0.367	0.472	-0.504	0.494
H_Habit_1	0.209	0.744	-0.153	-0.241	-0.199	0.292	-0.236	0.194
H_Habit_11	0.326	0.817	-0.221	-0.392	-0.295	0.28	-0.323	0.245
H_Habit_12	0.285	0.856	-0.207	-0.312	-0.28	0.281	-0.285	0.255
H_Habit_2	0.226	0.846	-0.176	-0.286	-0.248	0.273	-0.27	0.226
H_Habit_3	0.266	0.858	-0.206	-0.313	-0.254	0.292	-0.292	0.264
H_Habit_5	0.297	0.89	-0.225	-0.339	-0.25	0.326	-0.314	0.235
H_Habit_7	0.28	0.838	-0.178	-0.344	-0.316	0.3	-0.299	0.297
H_Habit_8	0.306	0.817	-0.186	-0.303	-0.234	0.305	-0.285	0.275
I_Intention_1	-0.413	-0.223	0.978	0.575	0.376	-0.353	0.679	-0.454
I_Intention_2	-0.445	-0.237	0.979	0.6	0.36	-0.365	0.685	-0.468
TH_PercBehavCtrl_2	0.085	0.089	-0.23	-0.204	-0.102	0.094	-0.229	0.084
TH_PercSeverity_3	0.465	0.258	-0.498	-0.507	-0.384	0.443	-0.529	0.904
TH_PerceivedVulnerab_1	0.479	0.273	-0.412	-0.404	-0.33	0.379	-0.429	0.924
TH_PerceivedVulnerab_2	0.487	0.282	-0.408	-0.445	-0.327	0.415	-0.454	0.943
TH_PerceivedVulnerab_3	0.49	0.288	-0.421	-0.428	-0.35	0.435	-0.479	0.92
R_Reactance_2	-0.175	-0.236	0.18	0.213	0.723	-0.11	0.239	-0.21
R_Reactance_3	-0.311	-0.29	0.399	0.458	0.943	-0.329	0.439	-0.386
RE_ResponseEfficacy_2	0.345	0.331	-0.266	-0.367	-0.245	0.752	-0.32	0.367
RE_ResponseEfficacy_3	0.405	0.301	-0.38	-0.403	-0.3	0.886	-0.447	0.414
RE_ResponseEfficacy_4	0.3	0.245	-0.262	-0.307	-0.187	0.863	-0.343	0.35
RV_Roles_2	-0.318	-0.184	0.425	0.445	0.242	-0.333	0.661	-0.344
RV_Roles_3	-0.455	-0.324	0.605	0.655	0.42	-0.385	0.84	-0.464
RV_SelfControl_1	-0.125	-0.147	0.29	0.206	0.155	-0.095	0.485	-0.106
RV_SelfControl_2	-0.192	-0.13	0.287	0.242	0.122	-0.121	0.547	-0.164
RV_SelfControl_3	-0.048	-0.15	0.204	0.114	0.036	-0.054	0.318	-0.062
RV_Affect_1	-0.452	-0.308	0.68	0.702	0.42	-0.429	0.84	-0.502
RV_Affect_4	-0.309	-0.273	0.448	0.552	0.307	-0.279	0.744	-0.305
RV_MoralDefinitions_1	0.456	0.241	-0.5	-0.557	-0.335	0.436	-0.718	0.502
	Fear	Habit	Intention	Neutralization	Reaction	Response Efficacy	Role Values	Threat

Appendix B: Scenarios

Scenario 1 – USB-drive

Pekka is a middle-level manager in a medium-sized company where he has worked for several years. Pekka is currently working on a sales report that requires the analysis of the company's customer database. This database contains customer names, phone numbers, credit card numbers, and purchase histories. Because of the sensitive nature of corporate data, the company has a strict policy prohibiting the copy of corporate data to unencrypted portable media, such as USB drives. However, Pekka will travel for several days and would like to analyze the corporate database on the road. Pekka expects that copying the data to the USB drive and taking it on the road could save the company a lot of time and money. The firm is experiencing growing sales and revenues in an industry that is economically deteriorating. He also knows that an employee was recently reprimanded for copying sensitive corporate data to a USB drive. Pekka copies the corporate database to his portable USB drive and takes it off company premises.

Scenario 2 – Workstation logout

Seija is a middle-level manager in a medium-sized company where she was recently hired. Her department uses an inventory procurement software application program to make inventory purchases. To ensure that only authorized individuals make inventory purchases, the company has a firm policy that employees must log out or lock their computer workstation when not in use. However, to make work more convenient, Seija's manager directs her to leave her user account logged-in for other employees to freely use. Seija expects that keeping her user account logged-in could save her company time. She also knows that keeping the workstation logged-in is a common practice in the industry and an employee recently was reprimanded for leaving the workstation logged-in. Seija leaves the workstation logged-in when she is finished.

Scenario 3 - Passwords

Hannu is a low-level manager in a small company where he was recently hired. His company has a strong policy that each computer workstation must be password-protected and that passwords are not to be shared. However, Hannu is on a business trip and one of his co-workers needs a file on his computer. Hannu expects that sharing his password could save his company a lot of time. He also knows that the firm has mandatory information security training. Hannu shares his password with his co-worker.

For a complete list of items included in the distributed survey, please refer to the original study by Moody et al. (2018).

About the Authors

Miranda Kajtazi is an Assistant Professor of Information Systems at the Department of Informatics, Lund University School of Economics and Management. She received her Ph.D. degree and Phil.Lic. Degree in Information Systems at Linnaeus University. Her research interest concerns one of the most crucial resources of our human, social and business affairs: information, with special focus on information systems security. Her work has been published in various outlets and she has recently received the Emerald Literati Award for her paper published in a special issue of *Information and Computer Security*. She is a Senior Associate at the Swedish MIT Research School as well as a member of IFIP WG 9.2.

Nicklas Holmberg is Senior Lecturer, Ph.D., in Information Systems and Head of Department at the Department of Informatics at Lund School of Economics and Management. Nicklas' research focus is on Process and Service Design and Development for decision making automation and service orientation. Senior Associate at MIT Research School, eGovernment Member, IBM GWC/WUG Member, IBM Client Reference Member, IBM Customer Partner Program Member, IBM Smarter Planet Reference Member and a Microsoft Certified Technology Specialist (MCTS).

Saonee Sarker is the Senior Associate Dean and Rolls Royce Commonwealth Commerce Professor at the McIntire School of Commerce in the University of Virginia. She is currently also a Visiting Professor at Lund University, Sweden. Her research focuses on globally distributed software development teams, Green IS and smart electricity, IT-enabled innovation, and Healthcare IT, and more recently on AI and its implications in organizations. Her publications have appeared in outlets such as *MIS Quarterly, Information Systems Research, Journal of Management Information Systems, Journal of the Association of Information Systems, Decision Sciences Journal, European Journal of Information Systems, and MIS Quarterly Executive,* among others. She currently serves as a Senior Editor of MIS Quarterly.

Christina Keller is a Professor in Information Systems at the Department of Informatics at Lund School of Economics and Management since 2019. She received her PhD in Economic Information Systems from the Department of Management & Engineering at Linköping University, Sweden. From 2008 to 2018, she worked Jönköping International Business School, Sweden. Her research interests include online learning, design science research and information systems in health care. She is a Program Director of the Master Program in Information Systems at Lund University. Since 2017, she is the dean of the Swedish Research School of Management and IT.

Björn Johansson is an Associate Professor in Information Systems at Department of Management and Engineering Division of Information Systems and Digitalization, Linköping University, Sweden. Previously he worked as Associate Professor at School of Economics and Management, Lund University 2009-2019 and as Post Doc at Center for Applied ICT at Copenhagen Business School 2007-2009. He received his PhD in Information Systems Development from the Department of Management & Engineering at Linköping University, Sweden in 2007. He is a member of the IFIP Working Groups IFIP 8.6 and IFIP 8.9., and the Swedish National Research School Management and IT (MIT). Johansson is Program Manager of the Master program IT and Management at Linköping University.

Olgerta Tona is an assistant professor at the department of Applied IT, University of Gothenburg and a research affiliate at the Swedish Center for Digital Innovation (SCDI). She received her Ph.D. in information systems from Lund University and was awarded the Börje Langeforspriset by Svenska Informationssystem Akademin for the best Ph.D thesis. Her research interests include business intelligence and analytics, personal data digitalization, and societal implications of algorithmic decision-making.