2020

A Conceptual Replication of the Unified Model of Information Security Policy Compliance

Diana K. Young
Trinity University, dyoung1@trinity.edu

D. Carpenter

A. McLeod

Transactions on Replication Research

Conceptual Replication DOI: 10.17705/1atrr.00050 ISSN 2473-3458

A Conceptual Replication of the Unified Model of Information Security Policy Compliance

Diana K. Young
Finance and Decision Science, Trinity University
dyoung1@trinity.edu

Darrell Carpenter
Information Systems and Cyber Security, Longwood University
carpenterdr@longwood.edu

Alexander J. McLeod
Health Information Management, Texas State University San Marcos
am@txstate.edu

Abstract:

Conceptual replications offer robust tests of theory by subjecting the relational notions of a scientific model to evaluation using alternate instruments, treatments, and subject pools. This study performs a conceptual replication of Moody, Siponen, and Pahnila's 2018 empirical analysis that integrated elements of eleven theoretical models to produce the unified model of information security policy compliance (UMISPC). This replication employed a substantially more parsimonious instrument, using modestly revised treatment scenarios targeted toward a U.S. audience of 218 IT professionals as opposed to the Finnish graduate students used in the original study. Our results indicate that UMISPC is robust across variations in instruments and subject pools. The replicated model explained approximately two thirds of the variance in information systems security policy compliance intentions across both studies. In contrast, competing models such as the theory of planned behavior and extended protection motivation theory exhibited large changes in explanatory power when the instrument and subject pool were modified. This suggests that UMIPSC may be a superior theoretical model for consistently evaluating security policy compliance behavioral intentions among varied populations. Our results also indicate that the theoretical model is capable of detecting and integrating a wide range of behavioral antecedents that may have differing levels of influence among various populations.

Keywords: information systems security, unified theory, survey

The manuscript was received 09/12/2019 and was with the authors 7 months for 2 revisions.

1 Introduction

Numerous researchers have sought to identify factors that motivate employees to comply with information security policies (Bulgurcu et al., 2010; Herath & Rao, 2009; Moody et al., 2018; Schneier, 2011; Siponen & Baskerville, 2018). Between 2009 and 2019, over 4,700 articles discussing the topic were published and of those 143 focused specifically on factors that affect employees' compliance behavior[1]. However, the individual articles were based on a wide range of theoretical perspectives from disciplines including criminology, psychology, social psychology, and health. As Moody, Siponen, and Pahnila (2018) noted, this has resulted "in a jungle of competing behavioral models that may not be easily compared" (p. 286) and does little to clarify the field's collective understanding of security policy compliance behavior.

Conceptual replications provide a robust method for testing the bounds of applicability for previously validated theoretical models. Such replications can determine whether the theoretical underpinnings of a model will hold in varied experimental conditions such as altered instrumentation and variations in the subject pool. In the current study, we test the (Moody et al., 2018) unified model of information security policy compliance (UMISPC) to determines its applicability to information technology (IT) professionals. Previous research suggests that information security professionals evaluate security risks differently than other groups of organizational insiders (Posey et al., 2014). More specifically, technology experts tend to make probabilistic security risk determinations while lay persons tend to be influenced by emotional reactions to threats and their potential impacts (Peters et al., 2006; Ponemon, 2014). Additionally, while lay people may be less informed regarding substantive risk issues, they tend to consider a much wider array of risk factors than IT professionals (Posey et al., 2014). Finally, IT professionals tend to have higher self-efficacy than lay persons with regard to their ability to appropriately respond to IT security threats.

Moody et al.'s (2018) original study examined UMISPC via a sample of Finnish graduate students which approximated the population of lay people within organizations. Our study considered the model's applicability to IT professionals who are expected to have differing underlying motivations based on their greater understanding of risk factors, higher self-efficacy, and reduced reliance on emotional reactions during risk calculations.

Moody et al. (2018) identified 11 information security policy compliance models that have been widely discussed in the literature including: 1) the theory of neutralization, 2) the health belief model, 3) the theory of reasoned action, 4) protection motivation theory, 5) theory of interpersonal behavior (TIB), 6) deterrence theory and rational choice theory, 7) extended protection motivation theory (EPMT), 8) theory of planned behavior, 9) theory of self-regulation, 10) extended parallel processing model, and 11) control balance theory. They then conducted a multi-phase examination of the eleven models to develop UMISPC, which includes components of the other models. The authors then empirically tested UMISPC using responses from Finnish graduate students (Figure 1).

Moody et al. (2018) later reduced the model by eliminating non-significant paths (rewards/costs, punishment, habit). However, in our replication, we tested Moody et al.'s full UMISPC model (Figure 1) along with the TIB and EPMT models, which also exhibit strong results in Moody et al.'s study.

[1] Google Scholar advanced search of articles containing the phrase "security policy compliance" in the title on 8/21/2019. Patents and citations excluded.

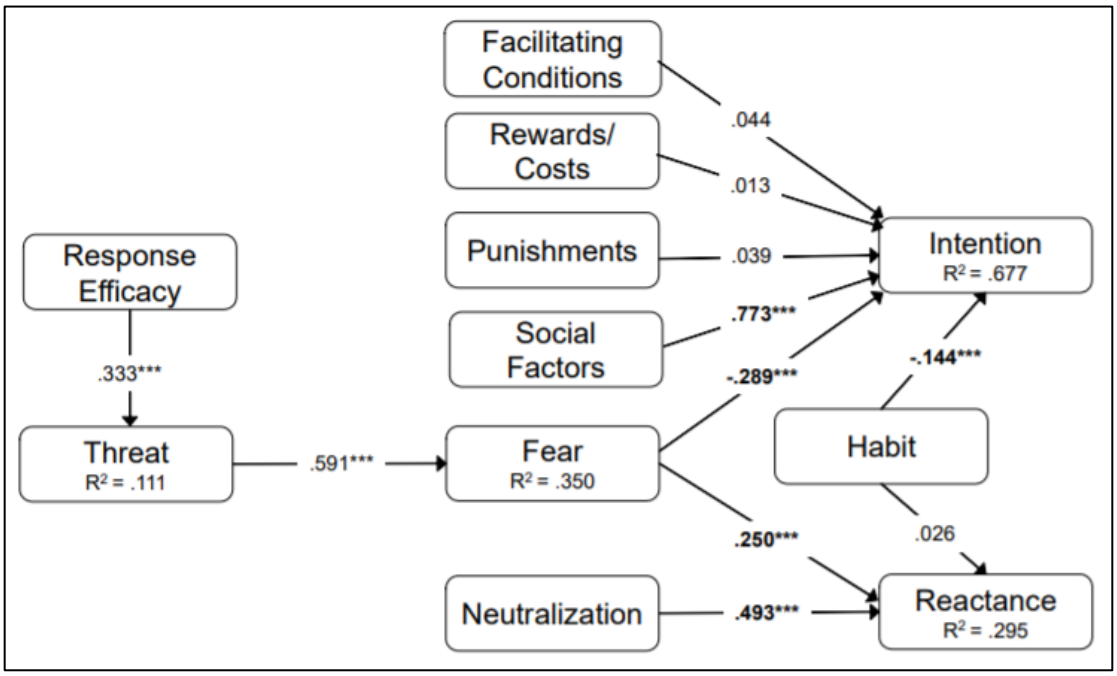

Figure 1: UMISPC Results (Moody et al. 2018)

2 Methods

The purpose of our study was to replicate Moody et al.'s (2018) UMISPC findings with a different target population and more parsimonious measures in order to assess the model's fit and explanatory power relative to the EPMT and TIB models. We focused our comparison on EPMT and TIB as they provided the first- and second-best explanations of security policy compliance intentions in the first phase of Moody et al.'s study. Additionally, TIB provided the foundational basis for UMISPC. Accordingly, we believe it is important to see if UMISPC provides better fit and explanatory value than EMPT and TIB in a different context. We chose not to compare the UMISPC model to the other nine models Moody et al. examined due to concerns regarding the length of the required survey instrument.

For the study we employed an electronic survey to collect the data and used the R package, PLSPM, to analyze the data. PLSPM has been widely used in IS research and has been noted as an appropriate tool for both confirmatory and explanatory research (Benitez et al., 2019; McIntosh et al., 2014). The following sections outline the steps involved in our research process.

2.1 Data Collection

We contracted with Qualtrics Sampling Services to collect a minimum of 210 responses from IT professionals. We chose that sample size as power analysis indicated that 134 responses were needed to detect a medium effect size in a regression equation containing six independent variables at the 0.05 error probability and 0.80 power levels.

Qualtrics aggregates online panel resources and distributes survey dashboards in which respondents can see all surveys that they qualified for. Once a respondent clicks on a survey they are interested in learning more about, Qualtrics begins tracking them. In total, 597 clicked on our survey. Of those 220 responses were complete and usable for analysis, which is a 37% completion rate.

When starting the survey, respondents were first asked to confirm that they were an IT professional. Those who responded affirmatively were shown a list of 18 IT occupations and asked to select the one that was most similar to their current position. The list of occupations was drawn from the United States Bureau of Labor Statistics Occupational Handbook (U.S. Bureau of Labor Statistics, 2015) and included options like

Business Intelligence Analyst, Database Administrator, Systems Administrator as well as an Other option, which required entry of the respondent's occupation in an associated textbox. At a later point in the survey, respondents were asked to also enter their current job title.

To validate that all respondents were indeed IT professionals, we compared each respondent's occupational selection to their entered job title. Two respondents were eliminated from the sample, as the titles they entered were not related to their chosen occupation, leaving 218 responses for analysis. The breakdown of the occupations represented in the sample is shown in Figure 2. As can be seen, slightly over 60% of the respondents identified as either an IT project management professional or a computer/IS manager. Seventeen respondents did not choose from the pre-defined list of occupations and selected the "other" option. We visually inspected the occupations entered by those individuals to ensure that they were actually IT related. All were judged to be valid and included occupations like IT consultant, IT auditor, CIO, and Business Owner.

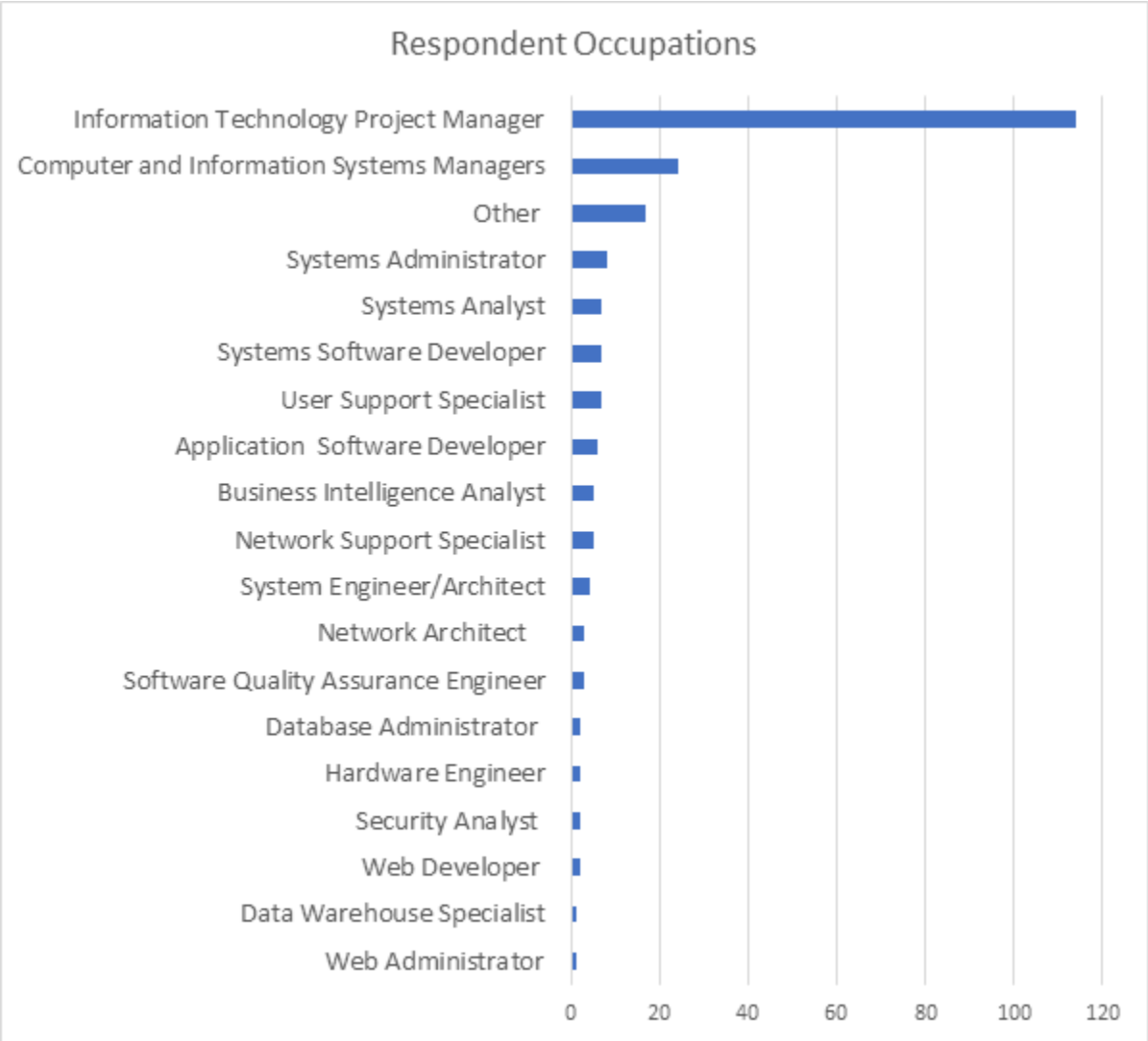

Figure 2: Count of Respondent Occupations

After the occupation validation step, each respondent was assigned to one of three scenarios, which were drawn from Moody et al. (2018) with updates made to change the scenario subject's name from Mattila to Chris. In addition, changes were made to instill consistency across the three scenarios regarding Chris's managerial level and length of employment. Finally, statements were added to emphasize Chris's

perceptions regarding the need to act promptly to meet an important deadline. Minor wording changes were also made to enhance readability of the three scenarios. The full text of each scenario can be found in Appendix A.

2.2 Measures

We modeled our instrument after Moody et al.'s (2018) instrument but reduced both the number of constructs assessed and the number of items used to measure each construct in an effort to create a shorter, more usable survey. Moody et al.'s full instrument contained 126 items with many constructs measured using five or more items. For example, habit was assessed using 12 items; response cost was assessed using 7 items; and fear was assessed using 11 items. At the outset of the study, we were highly concerned about the length of the Moody et al. instrument, the impact of survey fatigue on response rate, and IT professionals' tolerance toward completing such a long instrument. Accordingly, we designed our instrument to only include items to assess the constructs included in the TIB, EPMT, and UMISCP models. Additionally, we reduced the number of items for each construct by referring to Moody et al.'s (2018) factor analysis output and selecting the three items with highest loadings for each construct. In the case of Moody et al.'s threat construct, the three highest loading items were equivalent to the three items used to assess susceptibility in the EMPT model. In the case of reactance and intention, Moody et al. used two item measures that both exhibited strong reliability and validity, so we retained those two items. Our final instrument contained 55 items to assess the constructs included in the three models.

In the text of the items, all references to the scenario subject were changed from Mattila, a Finnish name, to Chris, a gender-neutral English name. Several items were modified to make the statements shorter and more colloquial in English as the original instrument was administered in Finnish. Across all items, the term "would" was updated to either "could" or "would likely". We felt this change was needed to ensure that the collected response was for the underlying construct rather than the probability that a threat would occur. For example, one of Moody et al.'s severity items stated, "If I were to do what Mattila did, there would be a serious information security problem for my organization." As "would" can be interpreted as certainty, it is possible that some individuals might respond to that question regarding the likelihood of a problem occurring rather than regarding the severity of a such problem. Accordingly, we believe the terms "could" and "would likely" lessened the degree of perceived certainty and will help subjects focus on the underlying construct to be measured.

Three new items were developed for the social factor constructs as none of the items used by Moody et al. (2018) loaded significantly on any of the identified factors. Additionally, items to assess the fear construct were updated to focus on "company computers" rather than "my computer". We felt this update was needed as information security policies are designed to protect all organizational computers not just the individual referenced in the scenario. The full list of items included on our electronic survey instrument can be found in Appendix B. The instrument was pilot tested using a sample of 180 Amazon Turk workers. Analysis of the pilot sample data indicated that the revised instrument exhibited adequate reliability and validity.

3 Results

The following sections outline the results of our analyses relating to the measurement and path models employed in the replication study.

3.1 Measurement Model

As our instrument contained items to assess three different theoretical models each containing different combinations of constructs, we began by constructing a composite model where all items were modeled as reflective indicators of the theorized construct. Several iterations of that model were tested with incremental removal of poorly loading indicators. During this process the following items were removed due to loading below 0.50 on the theorized construct: punishment1, social factors1, severity1, susceptibility1, response efficacy2, and fear1. Next, we assessed the reliability of the constructs. As can be seen in Table 1, most of the constructs exceeded the accepted 0.70 Cronbach's Alpha reliability threshold. Habit and severity were just under the threshold, whereas response efficacy, social factors, and susceptibility were each approximately 10 points below the threshold. However, the Dillon-Goldstein's composite reliability rho index for all of the constructs exceed 0.80.

Table 1: Construct Reliability

	Num of Items	Cronbach Alpha	DG Rho
Affect	3	0.948	0.967
Attitude	3	0.964	0.977
Fac_Conditions	2	0.912	0.958
Fear	2	0.721	0.878
Habit	3	0.683	0.826
Intention	2	0.964	0.982
Neutralization	3	0.950	0.968
Punishment	2	0.753	0.890
Reactance	3	0.891	0.932
Resp_Cost	3	0.821	0.893
Response_Efficacy	2	0.595	0.831
Rewards	3	0.879	0.925
Roles	3	0.958	0.973
Self_Concept	3	0.775	0.870
Severity	2	0.682	0.863
Social_Factors	2	0.603	0.834
Subj_Norms	3	0.964	0.976
Susceptibility	2	0.606	0.835

Vinzi (2010) notes that a block of items is considered homogeneous if the rho index is greater than 0.70. Further, Chin (1998) notes that Dillon-Goldstein's rho is a superior reliability measure as it is based on item loadings rather than the correlations between the manifest variables. As we collected the data with a highly parsimonious instrument, we felt the scales exhibited an adequate level of reliability to move forward with our analysis.

Next, we calculated correlations for each of the measured constructs. As PLSPM is based on standardized measures, the means and standard deviations are not shown in the Table 2.

Table 2: Correlations and Square Roots of AVE

	Rew	Pun	Att	Snor	Rol	Scon	Sfac	Affe	Seve	Susc	Reffi	Fear	Fcon	Rcos	Neu	Hab	Rea	Int
Rew	**0.90**																	
Pun	0.16	**0.86**																
Att	0.65	0.17	**0.97**															
Snor	0.63	0.19	0.80	**0.97**														
Rol	0.67	0.15	0.82	0.87	**0.96**													
Scon	0.04	0.32	-0.09	-0.07	-0.09	**0.83**												
Sfac	0.24	0.62	0.18	0.21	0.17	0.32	**0.85**											
Affe	0.63	0.13	0.93	0.76	0.77	-0.14	0.17	**0.95**										
Seve	0.08	0.43	0.10	0.16	0.11	0.29	0.28	0.08	**0.86**									
Susc	0.01	0.42	-0.12	-0.12	-0.13	0.55	0.38	-0.15	0.41	**0.84**								
Reffi	-0.05	0.35	-0.10	-0.16	-0.14	0.51	0.40	-0.10	0.29	0.63	**0.84**							
Fear	0.34	0.37	0.45	0.49	0.46	0.27	0.38	0.43	0.34	0.24	0.20	**0.88**						
Fcon	0.56	0.21	0.67	0.80	0.73	0.08	0.25	0.67	0.14	-0.06	-0.07	0.51	**0.96**					
Rcos	0.62	0.24	0.51	0.56	0.59	0.13	0.25	0.52	0.33	0.08	0.11	0.36	0.51	**0.86**				
Neu	0.63	0.15	0.79	0.83	0.84	0.07	0.19	0.75	0.16	-0.02	-0.04	0.57	0.72	0.59	**0.95**			
Hab	0.00	0.18	-0.14	-0.12	-0.11	0.21	0.13	-0.16	0.13	0.23	0.17	0.09	-0.09	-0.10	-0.13	**0.49**		
Rea	0.49	0.11	0.67	0.57	0.62	-0.01	0.16	0.66	0.02	-0.08	-0.05	0.38	0.48	0.40	0.64	-0.06	**0.91**	
Int	0.66	0.15	0.79	0.89	0.83	-0.05	0.19	0.73	0.15	-0.10	-0.10	0.50	0.76	0.57	0.82	-0.13	0.56	**0.98**

Diagonal elements represent the square root of AVE for each construct

Rew = Rewards, Pun = Punishment, Att = Attitude, Snor = Subjective Norms, Rol = Roles, Scon = Self Concept

Sfac = Social Factors, Aff = Affect, Seve = Severity, Susc = Susceptibility, Reffi = Response Efficacy, Fear = Fear,

Fcon = Facilitating Conditions, Rcos = Response Cost, Neu = Nuetralization, Hab = Habit, Rea = Reactance,

Int = Intention

An assessment of convergent validity was completed by examining the on-factor loadings for each indicator to ensure they were at or above 0.70 for the intended construct (Gefen et al., 2011). This was achieved for all constructs, except habit (Table 3). We tested all combinations of items in hopes of finding a measurement solution that included at least two indicators loading close to or above 0.70.

However, no combination of the three items results in that outcome. Accordingly, we chose to retain all three items in our model and offer caution when interpreted results involving that construct.

An additional difference we found in our data from Moody et al.'s (2018) results concerned the rewards/costs construct. When Moody et al. conducted principle factor analysis on all items included in the 11 models they tested, items from the TIB rewards and response cost constructs all loaded on a single factor that they named reward/costs. In our analysis, however, the three reward items loaded together on one factor and the response cost items loaded strongly together on another factor. Accordingly, we modeled reward and response cost as two separate constructs in our analysis.

Table 3: Factor Loadings

	Factors																	
Item	**Rew**	**Pun**	**Att**	**Snor**	**Rol**	**Scon**	**Sfac**	**Affe**	**Seve**	**Susc**	**Reffi**	**Fear**	**Fcon**	**Rcos**	**Neu**	**Hab**	**Rea**	**Int**
Rew1	0.92	0.06	0.57	0.58	0.60	0.01	0.18	0.56	0.03	-0.05	-0.08	0.31	0.51	0.57	0.56	-0.03	0.41	0.62
Rew2	0.91	0.22	0.56	0.57	0.61	-0.02	0.25	0.55	0.10	0.01	-0.08	0.30	0.49	0.57	0.58	0.03	0.42	0.58
Rew3	0.87	0.14	0.61	0.56	0.60	0.10	0.21	0.57	0.08	0.05	0.03	0.31	0.51	0.54	0.56	0.00	0.48	0.56
Pun2	0.08	0.71	0.04	0.05	0.03	0.35	0.51	0.03	0.41	0.44	0.38	0.31	0.10	0.17	0.06	0.18	0.05	0.04
Pun3	0.16	0.99	0.18	0.21	0.16	0.29	0.60	0.14	0.40	0.38	0.33	0.36	0.21	0.24	0.15	0.17	0.11	0.16
Att1	0.61	0.17	0.95	0.75	0.76	-0.05	0.20	0.88	0.12	-0.09	-0.05	0.43	0.62	0.48	0.74	-0.16	0.62	0.74
Att2	0.64	0.16	0.98	0.78	0.81	-0.10	0.16	0.90	0.06	-0.13	-0.10	0.44	0.65	0.49	0.79	-0.15	0.67	0.78
Att3	0.63	0.16	0.97	0.79	0.80	-0.11	0.17	0.91	0.10	-0.14	-0.12	0.44	0.68	0.51	0.77	-0.11	0.64	0.77
Snor1	0.60	0.20	0.76	0.96	0.82	-0.10	0.20	0.71	0.14	-0.12	-0.17	0.45	0.76	0.54	0.79	-0.08	0.53	0.85
Snor2	0.62	0.18	0.76	0.97	0.85	-0.06	0.23	0.73	0.15	-0.10	-0.17	0.49	0.79	0.55	0.80	-0.14	0.54	0.87
Snor3	0.62	0.17	0.80	0.96	0.86	-0.04	0.19	0.75	0.17	-0.12	-0.15	0.48	0.78	0.54	0.80	-0.12	0.58	0.87
Rol1	0.66	0.20	0.77	0.83	0.96	-0.06	0.19	0.72	0.11	-0.10	-0.12	0.43	0.71	0.54	0.78	-0.04	0.55	0.78
Rol2	0.64	0.11	0.79	0.83	0.97	-0.11	0.14	0.76	0.11	-0.13	-0.13	0.45	0.69	0.60	0.81	-0.13	0.60	0.80
Rol3	0.62	0.13	0.80	0.85	0.95	-0.10	0.15	0.76	0.10	-0.14	-0.17	0.44	0.70	0.55	0.82	-0.15	0.63	0.81
Scon1	0.08	0.35	0.02	0.06	0.03	0.72	0.27	-0.02	0.27	0.33	0.35	0.34	0.21	0.22	0.14	0.18	0.05	0.07
Scon2	0.08	0.25	-0.07	-0.05	-0.04	0.85	0.26	-0.10	0.21	0.53	0.42	0.25	0.09	0.05	0.08	0.24	0.03	-0.03
Scon3	-0.03	0.24	-0.13	-0.12	-0.15	0.90	0.28	-0.18	0.25	0.48	0.47	0.16	-0.01	0.10	0.01	0.12	-0.06	-0.11
Sfac2	0.19	0.53	0.14	0.17	0.10	0.33	0.86	0.11	0.20	0.30	0.31	0.36	0.22	0.15	0.16	0.14	0.15	0.18
Sfac3	0.22	0.51	0.18	0.19	0.19	0.21	0.83	0.18	0.27	0.34	0.36	0.28	0.20	0.29	0.17	0.08	0.12	0.13
Affe1	0.64	0.15	0.93	0.78	0.79	-0.14	0.17	0.95	0.06	-0.15	-0.12	0.45	0.68	0.50	0.76	-0.13	0.67	0.75
Affe2	0.58	0.09	0.84	0.67	0.69	-0.12	0.16	0.94	0.09	-0.13	-0.06	0.39	0.60	0.48	0.67	-0.15	0.60	0.64
Aff3	0.57	0.13	0.87	0.70	0.72	-0.13	0.15	0.96	0.09	-0.14	-0.09	0.40	0.62	0.49	0.69	-0.17	0.62	0.67
Seve2	0.07	0.36	0.11	0.16	0.14	0.22	0.20	0.10	0.96	0.32	0.21	0.31	0.14	0.33	0.16	0.07	0.03	0.15
Seve3	0.05	0.43	0.04	0.09	0.02	0.35	0.36	0.02	0.74	0.47	0.37	0.29	0.10	0.21	0.10	0.24	0.01	0.09
Susc2	0.02	0.35	-0.10	-0.11	-0.12	0.44	0.31	-0.13	0.40	0.91	0.49	0.19	-0.06	0.08	-0.02	0.15	-0.10	-0.07
Susc3	-0.02	0.37	-0.11	-0.10	-0.10	0.51	0.34	-0.13	0.27	0.78	0.61	0.24	-0.04	0.04	-0.01	0.26	-0.02	-0.10
Reffi1	-0.06	0.34	-0.07	-0.12	-0.10	0.30	0.33	-0.04	0.29	0.48	0.75	0.16	-0.09	0.05	-0.07	0.27	-0.06	-0.06
Reffi3	-0.03	0.28	-0.09	-0.15	-0.14	0.51	0.35	-0.11	0.22	0.58	0.92	0.18	-0.05	0.12	-0.01	0.07	-0.03	-0.10
Fear2	0.29	0.28	0.31	0.30	0.29	0.29	0.36	0.32	0.30	0.34	0.25	0.82	0.34	0.30	0.44	0.02	0.30	0.32
Fear3	0.31	0.36	0.46	0.52	0.48	0.21	0.32	0.43	0.31	0.14	0.14	0.93	0.53	0.33	0.55	0.12	0.36	0.52
Fcon2	0.55	0.23	0.66	0.78	0.72	0.07	0.28	0.67	0.14	-0.07	-0.05	0.51	0.96	0.52	0.72	-0.11	0.49	0.73
Fcon3	0.52	0.17	0.63	0.76	0.68	0.09	0.19	0.61	0.14	-0.05	-0.10	0.48	0.96	0.45	0.67	-0.07	0.43	0.73
Rcos1	0.58	0.19	0.46	0.53	0.56	0.10	0.22	0.48	0.27	0.04	0.07	0.40	0.48	0.90	0.57	-0.14	0.39	0.58
Rcos2	0.56	0.26	0.46	0.45	0.47	0.10	0.26	0.47	0.26	0.10	0.13	0.24	0.38	0.82	0.44	-0.05	0.30	0.45
Rcos3	0.47	0.17	0.38	0.45	0.47	0.16	0.17	0.37	0.32	0.08	0.10	0.26	0.43	0.85	0.49	-0.05	0.34	0.43
Neu1	0.54	0.12	0.71	0.72	0.73	0.11	0.17	0.66	0.11	-0.02	-0.01	0.50	0.61	0.49	0.93	-0.13	0.59	0.72
Neu2	0.63	0.13	0.77	0.82	0.83	0.02	0.18	0.73	0.17	-0.02	-0.05	0.55	0.72	0.60	0.96	-0.14	0.61	0.82
Neu3	0.63	0.17	0.78	0.82	0.82	0.09	0.20	0.75	0.17	-0.02	-0.06	0.58	0.73	0.58	0.97	-0.10	0.62	0.81
Hab1	0.06	0.33	-0.11	-0.09	-0.10	0.35	0.33	-0.12	0.27	0.44	0.40	0.15	-0.06	0.03	-0.12	0.84	-0.10	-0.09
Hab2	0.10	0.28	0.11	-0.03	-0.04	0.12	0.33	0.08	0.24	0.29	0.34	0.04	-0.05	0.14	0.05	0.04	0.00	0.00
Hab3	0.12	0.32	0.04	0.02	-0.01	0.31	0.40	0.03	0.28	0.43	0.47	0.13	0.04	0.21	-0.01	-0.08	-0.08	0.05
Rea1	0.46	0.11	0.60	0.49	0.54	0.01	0.16	0.62	0.05	-0.11	-0.03	0.32	0.44	0.34	0.55	0.00	0.90	0.48
Rea2	0.42	0.09	0.56	0.48	0.51	0.02	0.13	0.55	0.03	-0.06	-0.03	0.34	0.40	0.37	0.56	-0.09	0.92	0.48
Rea3	0.45	0.10	0.64	0.57	0.62	-0.05	0.14	0.63	-0.01	-0.05	-0.07	0.38	0.46	0.38	0.62	-0.09	0.90	0.56
Int1	0.65	0.16	0.80	0.88	0.81	-0.02	0.20	0.73	0.15	-0.08	-0.09	0.50	0.76	0.56	0.81	-0.14	0.56	0.98
Int2	0.64	0.13	0.76	0.88	0.82	-0.08	0.16	0.70	0.14	-0.12	-0.11	0.48	0.73	0.57	0.80	-0.12	0.55	0.98

To assess the discriminant validity of our measures, we reviewed the cross loadings for each item. While we did find high cross loadings for some constructs, such as those for affect and attitudes, these must be evaluated with the theorized relationships between those constructs in mind. Affect has been widely discussed as a determinant of attitude (Clore & Schnall, 2005). Accordingly, we did not consider high cross loadings between those constructs to be problematic. To further substantiate the discriminant validity of the scales, the square root of the average variance extracted (AVE) was calculated for each construct to ensure that the value was greater than the construct's correlations with all other constructs. As the diagonal elements in Table 2 show, each construct's square root of AVE exceeds its correlations with all other constructs.

Finally, we employed Harman's (1976) single latent factor technique to ensure that common method bias did not unduly impact our measurement model. Each of the three models included in our study fit the data better than a model with a single factor. Accordingly, we did not find evidence that common method variance biased the sample. We do note that Harman's single factor technique has recently been questioned and reported as insensitive and incomplete (Tehseen et al., 2017).

3.2 Path Models

We used PLSPM with 500 bootstrap resamples to test path models for each theory – TIB, EPMT, and UMISPC. Figure 3 shows the results of the TIB model.

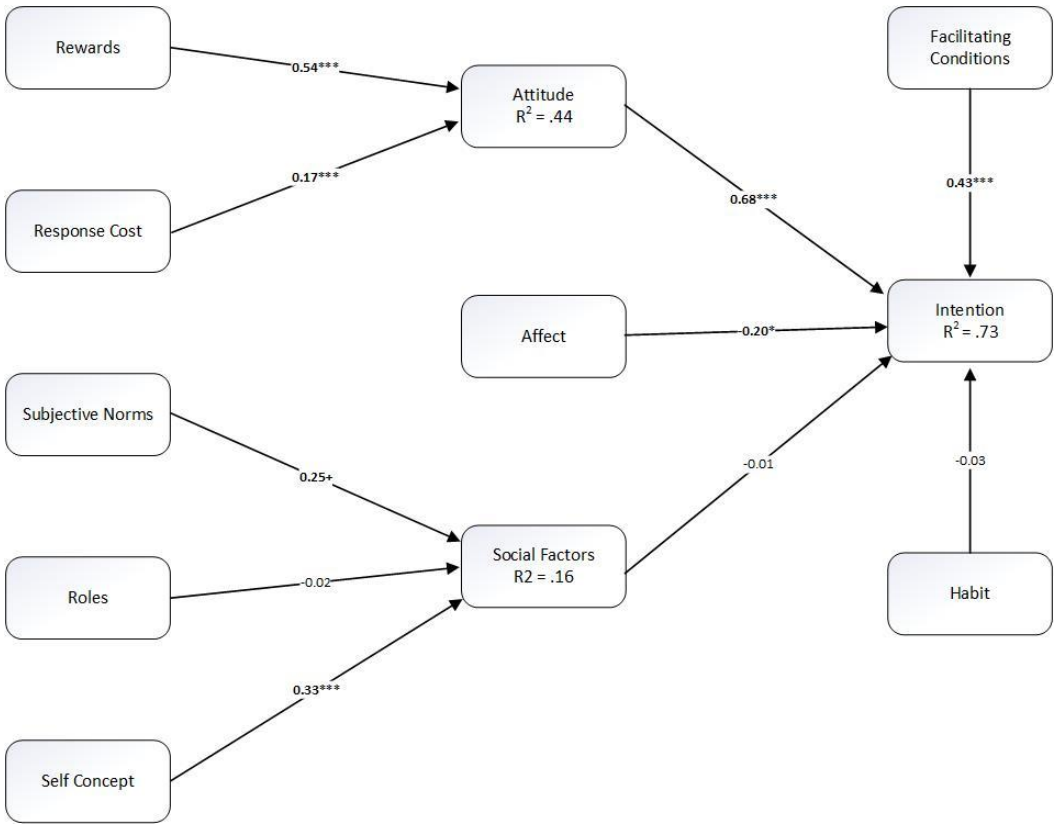

Figure 3: Theory of Interpersonal Behavior (TIB) Results

In the TIB model, rewards (β = 0.54, p < .001) and response cost (β = 0.17, p < .001) significantly influenced attitude explaining 44% of the attitude variance. Subjective norm (β = 0.25, p < .10) and roles (β = -0.02, p > .10) were not significantly associated with social factors, but self-concept (β = 0.33, p < .001) was significant, generating an R^2 of .16 for social factors. Attitude (β = 0.68, p < .001) significantly affected intention as did affect (β = 0.20, p < .05). Social factors (β = -0.01, p > .10) were not influential on intention. Overall, the R^2 value for intention was very good at .73 with facilitating conditions (β = 0.43, p < .001) significantly associated but not habit (β = -0.03, p > .10).

Next, we used PLSPM with 500 bootstrap resamples to test path models for EPMT (Figure 4). Of all the antecedents to intention in the EPMT model, response cost (β = 0.46, p < .001), rewards (β = 0.26, p < .001) and susceptibility (β = -0.15, p < .05) were significant. Severity (β = 0.06, p > .10), response efficacy (β = -0.06, p > .10) and self-efficacy (β = 0.10, p > .10) were not significant. Path values for costs and rewards were much larger than the other four variables. Severity, susceptibility, response efficacy and self-efficacy had relatively small path values and the R^2 value for the EPMT model was less than the TIB model at .50. Figure 3 details the results for the EPMT model.

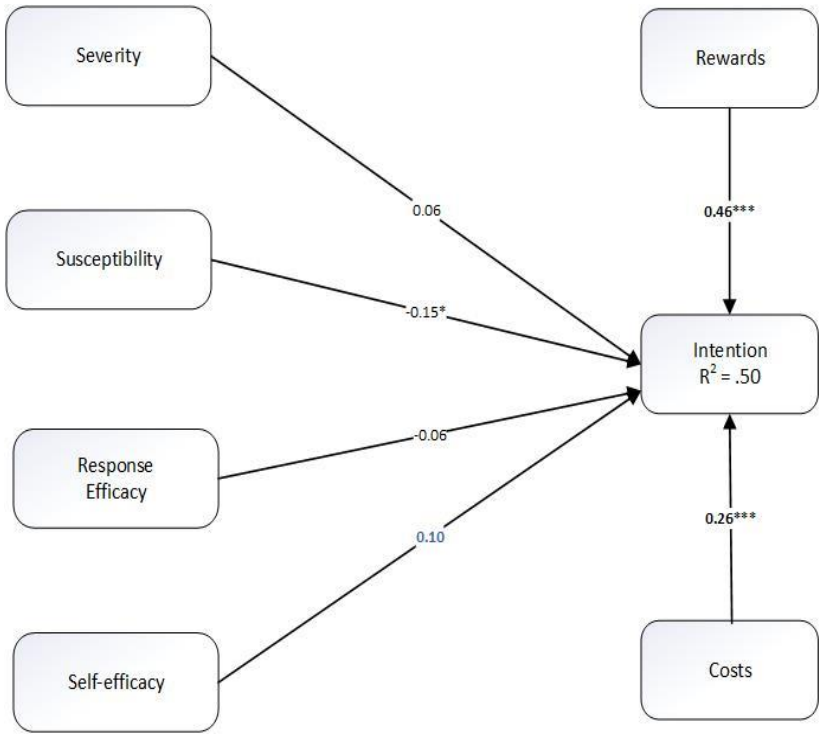

Figure 4: Extended Protection Motivation Theory (EPMT) Results

The UMISPC was the final model evaluated. Variables included facilitating conditions, response costs, rewards, punishments, social factors, fear, response efficacy, threat, neutralization, habit, reactance and intention. Figure 5 shows the results of the PLSPM analysis of UMISPC. Response efficacy ($\beta = 0.65$, $p < .001$) significantly affected threat ($\beta = 0.36$, $p < .001$), which in turn impacted fear significantly. Significant antecedents to intention included facilitating conditions ($\beta = 0.48$, $p < .001$), response costs ($\beta = 0.13$, $p < .01$), rewards ($\beta = 0.28$, $p < .001$) and fear ($\beta = 0.14$, $p < .01$).

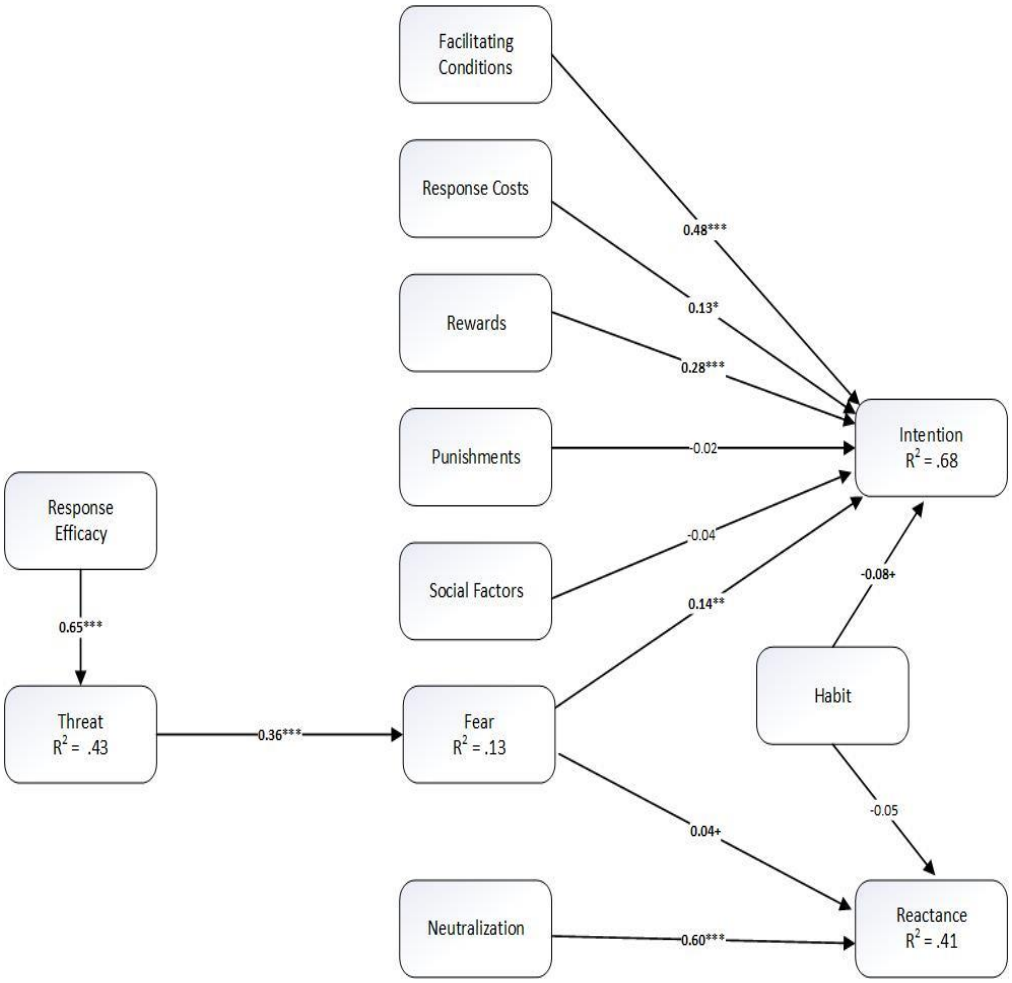

Figure 5: Unified Model of Information Security Policy Compliance (UMISPC) Results

Habit (β = -0.08, $p < .10$) was only marginally significant in its relationship with intention and insignificant with reactance. Neutralization (β = 0.60, $p < .001$) significantly influenced reactance.

Table 4: Summary of Fit and Explanatory Value of Tested Theories

Model	Relation	Moody et al. Result	Replication Result
EPMT	Severity → Intention	-0.07	0.06
	Susceptibility → Intention	**-0.12***	**-0.15***
	Response Efficacy → Intention	-0.04	-0.06
	Self-efficacy → Intention	**-0.72*****	0.10
	Reward → Intention	**0.24****	**0.46*****
	Costs → Intention	-0.05	**0.26*****
	Intention R^2	60%	50%
	Model Fit	CFI = 0.81, TLI = 0.79	GoF = 0.62
TIB	Rewards → Attitude	**0.30*****	**0.54*****
	Penalties → Attitude	**-0.29*****	**0.17*****
	Subjective Norms → Social Factors	**0.29*****	**0.25+**
	Roles → Social Factors	**0.19****	0.02
	Self-Concept → Social Factors	**-0.20*****	**0.33*****
	Attitude → Intention	**0.26*****	**0.68*****
	Affect → Intention	**0.36*****	**0.20***
	Social Factors → Intention	**0.62*****	-0.01
	Facilitating Conditions → Intention	**0.11****	**0.43*****
	Habit → Intention	-0.04	-0.03
	Intention R^2	59%	73%
	Model Fit	CFI = 0.72, TLI = 0.80	GoF = 0.59
UMISPC	Response Efficacy → Threat	**0.33*****	**0.65*****
	Threat→ Fear	**0.59*****	**0.36*****
	Facilitating Conditions → Intention	0.04	**0.48*****
	Rewards/Costs → Intention	0.13	
	Response Costs → Intention		**0.13***
	Rewards → Intention		**0.28*****
	Punishment → Intention	0.39	0.02
	Social Factors → Intention	**0.77*****	-0.04
	Fear → Intention	**-0.29*****	**0.14****
	Habit → Intention	**-0.14*****	**-0.08+**
	Habit → Reactance	0.03	-0.05
	Fear → Reactance	**0.25*****	**0.04+**
	Neutralization → Reactance	**0.49*****	**0.60*****
	Intention R^2	68%	68%
	Model Fit	CFI = 0.98, TLI = 0.96	GoF = 0.56

Table 4 provides a comparison of Moody et al.'s (2018) results and this study's results for each of the tested models. Unless otherwise noted, values in the result columns represent path beta coefficients and statistical significance. For our replication results, + represents significance levels of < 0.10, * represents significance levels of <= 0.05, ** represents significance levels of <= 0.01, and *** represents significance levels of <= 0.001. As Moody et al. (2018) did not specify the meaning behind the asterisk notation they used, care should be taken when comparing statistical significances between the two studies.

In terms of UMISPC, the explanatory value exhibited in both the original study and the replication was 68%, more than two-thirds of the variance detected in both datasets. However, several key differences existed in the original study and the replication study findings. First, facilitating conditions (β = 0.04) were not found to influence the compliance intentions of the graduate student sampled in the original study. However, facilitating conditions were found to strongly influence the compliance intentions of the IT professionals (β = 0.48***) sampled in the replication.

In the Moody et al. study, the reward and costs items loaded onto a single construct and support was not found for a relationship (β = 0.13) between that combined construct and compliance intentions. However, in the replication study, the reward and costs items loaded onto two distinct constructs both of which were found to be significantly related to the compliance intentions of IT professionals (costs β = 0.13*, reward β = 0.28***). Social factors were found to be highly associated with compliance intentions in the graduate student sample (β = 0.77**) but not in the IT professional sample (β = -0.04). Finally, habit and fear were found to be strongly associated with the compliance intentions of graduate students. However, both habit and fear were only approaching significance in the replication test involving IT professionals.

In terms of EPMT, the replication model exhibited a slightly lower level of explanatory value (50%) when compared to Moody et al. 's (2018) study (60%). In addition, the replication results concerning the influence of self-efficacy and costs on compliance intentions differed from Moody et al.'s results. In the original study, self-efficacy exhibited a significant negative influence on intention but support for that relationship was not found in the replication study. This may be due in part to the reduced scale that was used in the replication study. Moody et al. reported a 0.896 Cronbach alpha reliability level for their four-item measure of self-efficacy, while we only achieved a 0.595 Cronbach alpha reliability for our three-item measure. Finally, in the Moody et al. study, costs were not found to be significantly associated with compliance intentions. However, in our EPMT replication, a strongly significant association was found between costs and compliance intentions. Interestingly, the costs construct exhibited relatively similar levels of reliability across the two studies.

In terms of TIB, differences between Moody et al. and our replication results were mostly connected to the social factors construct. In Moody et al.'s original study, role was significantly associated with social factors, and in-turn social factors were significantly associated with intentions. In our replication, support for those associations was not found. These differences may be related to our reduced measurement scale for social factors. When validating the replication scales, one of the social factors items was dropped due to a very low loading level. The remaining two items only exhibited a Cronbach alpha reliability level of 0.603. Accordingly, the reduced measure may not be able to detect significant associations. Despite these differences, TIB exhibited the best explanatory value (73%), nearly 14 percentage points higher than what was detected for the TIB model in the original study.

In terms of the three models tested in the replication study, the TIB model demonstrated the greatest explanatory power with an R^2 of 0.73 and the second-best fit with a GoF fit index of 0.59. The EPMT model provided the lowest R^2 at 0.50 but had the strongest GoF fit index at .62. Finally, the UMISPC model provided an R^2 of 0.68 and the lowest fit index at .56.

4 Discussion

The replication results yielded several interesting insights when compared to Moody et al.'s (2018) results as well as when viewed in terms of differences between the models tested within the replication study. For clarity, we begin our discussion in terms of between study results (Moody et al. vs. replication) and end with discussion concerning within study results (replication TIB vs. EPMT vs. UMISPC).

4.1 Between Study Results

Our research largely validates the findings from the original Moody et al. (2018) study with a few notable differences. For example, we note that TIB had a dramatically higher R^2 for policy compliance intention in our study (0.73) as compared to the Moody et al. study (0.59). However, the R^2 values for UMISPC policy compliance intention were nearly identical at 0.68 in both the original and the replication studies. Given that the original study used Finnish students and our study used U.S. IT professionals, these results provide support for the notion that UMISPC may be more robust and consistent across dissimilar populations. This offers support for generalizing UMISPC since the cultural and work contexts between the studies were quite different. We also note that this consistency in results was achieved even after our deliberate efforts to create a more parsimonious instrument. After reducing the Moody et al. (2018) instrument to approximately half of its original length, it still explained a similar portion of the variance in policy compliance intention.

Results between the two studies also yield interesting differences when comparing fit statistics and significant pathways. The CLI and TLI fit statistics for UMISPC were greater in the original study than all other models while in the replication EPMT exhibited the best GoF fit statistic. Moody et al. (2018) expressed concern about fit statistics when only the Theory of Reasoned Action yielded optimal fit statistics and that for most theories "…the fully saturated models had a better fit than the theoretical models, implying that omitted relationships between the theoretical constructs were reducing the fit of the data to the model." These results indicate that further research is probably needed to identify and update UMISPC to account for missing or under-represented constructs.

In terms of path coefficients, we found several interesting differences in the influence that the UMISPC predictors have on the compliance intentions of graduate students and IT professionals. Specifically, in the original study involving graduate students, social factors, habit, and fear were all found to be strongly related to compliance intentions. However, no association was found between social factors and the compliance intentions of IT professionals while both habit and fear were only weakly (between 0.10 and 0.05) associated with the policy compliance intentions of IT professionals. Additionally, facilitating conditions, costs, and rewards were not found to be significantly associated with the compliance intentions of the graduate students but were found to be strongly associated with the compliance intentions of the IT professionals. These findings support the notion that IT professionals evaluate information security compliance decisions differently than graduate students and also provide support the use of UMISPC as a robust tool to assess compliance intentions across audiences. Further, these finding provide support for use of the full UMISPC model rather than Moody et al. suggested reduced model in which facilitating conditions, costs, and rewards were removed due to non-significant associations with intentions.

Our replication also provides support for the impact of fear and neutralization on reactance. We achieved a somewhat higher predictability for reactance with an R^2 of .41 as compared to the R^2 of .295 in the original Moody et al. (2018) study. This result is not comparable to TIB or EPMT due to differences in the models, but UMISPC's ability to predict a smaller percentage of reactance as compared to policy compliance intention in both studies points toward consistency across varied populations.

While our replication provides support for the general premise of UMISPC's combined policy compliance predictive model, much work remains to be done regarding refinement of the individual scales used to measure the model's constructs. We particularly note our issues with the shortened habit scale, where the retained items failed to load on a single factor during factor analysis. We believe this was partially caused by a restricted response range where most respondents answered "strongly agree" for each of the three items on the scale. We also suspect that wording of the habit items could be problematic in that phrases like "normally", "without thinking" and "automatically" may have different meanings for different respondents. Thus, we advocate for additional work to identify and validate new scale items for measuring the habit construct. We strongly believe that the twelve-item habit scale from (Verplanken & Orbell, 2003) that was adopted by Moody et al. (2018) is unnecessarily lengthy and can be revised to accurately assess the effects of habit in a more parsimonious form.

4.2 Within Study Results

When comparing the results of the three models included in our replication study, the strength of the TIB model cannot be understated. While both UMISPC and TIB explained over two thirds of the variance in the behavioral intentions of IT professionals to comply with security policies, TIB exhibited greater explanatory value than UMISPC in the replication (0.73 vs. 0.68). TIB achieved that level of explanatory value even though reconciliation of the constructs between the models yielded only 10 constructs for TIB compared to

13 constructs for UMISPC. Nine of the 10 pathways were significant for TIB when compared to 7 of 13 for the UMISPC. We also note that in the replication TIB had a higher R^2 for policy compliance intention when as compared to the EPMT model (0.50). These findings indicate that further work is needed to understand the TIB factors that better represented IT professionals' compliance intention decisions in order to incorporate and/or better represent those factors in a generalizable UMISPC model.

5 Limitations

The first limitation noted is the use of IT professionals as subjects. We chose that population as we believed that the compliance intentions of IT professionals might be different than those of general employees. IT professionals often have more knowledge regarding systems and security threats, which may lead them to feel better equipped to make security policy compliance choices. Accordingly, their perceptions of threats may be different from that of general employees, which could in-turn affect their compliance intentions. Thus, we viewed our sample selection as a potential limitation.

Second, while Moody et al (2018) called for additional constructs and moderators in different contexts, we chose to attempt a reduction of the instrument given its length and did not attempt to make use of additional constructs or relationships. Our item selection may have influenced the results and thus, we viewed this as a limitation.

A final limitation deals with our selection of Harman's single factor test for common method variance. Recently it has been suggested that this test is insensitive and incomplete, possibly contributing another potential limitation to our study.

6 Conclusion

This study furthers the aims of the original Moody et al. (2018) study in several important ways. First, it tests the notions of the model in a different context and with a more parsimonious instrument and it shows that the predictive power of the model is similar even under varied context. Second, our study helps to define the boundaries of UMISPC's applicability and situations where the model has weaknesses. Our findings related to the habit scale are one example of an area where additional work is necessary to develop a robust, parsimonious scale to measure the habit construct. Third, our research demonstrates the importance of retaining the constructs that were not significant predictors of policy compliance intention in the original Moody et al. (2018) study as these became important predictors when the model was applied to a different population. Overall, our replication indicates that UMISPC is robust model for assessing policy compliance intention in its current state but offers substantial opportunities for refinement.

7 References

Benitez, J., Henseler, J., Castillo, A., & Schuberth, F. (2019). How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research. *Information & Management*, 57(2), 103168.

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

Clore, G. L., & Schnall, S. (2005). The influence of affect on attitude. In D. Albarracín, B. T. Johnson, & M. P., Zanna (Eds.), Handbook of Attitudes (pp. 437-489). Mahwah: Erlbaum.

Gefen, D., Rigdon, E. E., & Straub, D. (2011). An update and extension to SEM guidelines for administrative and social sciences research. *MIS Quarterly*, *35*(2), iii–xiv.

Harman, D. (1976). A single factor test of common method variance. *Journal of Psychology*, *35*, 359–379.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125.

McIntosh, C. N., Edwards, J. R., & Antonakis, J. (2014). Reflections on partial least squares path modeling. *Organizational Research Methods*, *17*(2), 210–251.

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

Peters, E., Slovic, P., Hibbard, J. H., & Tusler, M. (2006). Why worry? Worry, risk perceptions, and willingness to act to reduce medical errors. *Health Psychology*, *25*(2), 144-152.

Ponemon. (2014). *Fourth Annual Benchmark Study on Patient Privacy & Data Security*. Ponemon Institute LLC. Retrieved from: http://www.ponemon.org/library/archives/2014/03.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, *51*(5), 551–567.

Schneier, B. (2011). *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons.

Siponen, M., & Baskerville, R. L. (2018). Intervention effect rates as a path to research relevance: Information systems security example. *Journal of the Association for Information Systems*, *19*(4), 247-265.

Tehseen, S., Ramayah, T., & Sajilan, S. (2017). Testing and controlling for common method variance: A review of available methods. *Journal of Management Sciences*, *4*(2), 142–168.

U.S. Bureau of Labor Statistics. (2015, December 17). *Computer and Information Technology Occupations*. Occupational Outlook Handbook. Retrieved from: http://www.bls.gov/ooh/computer-and-information-technology/home.htm.

Verplanken, B., & Orbell, S. (2003). Reflections on past behavior: A self-report index of habit strength. *Journal of Applied Social Psychology*, *33*(6), 1313–1330.

Vinzi, V. E., Trinchera, L., & Amato, S. (2010). PLS path modeling: From foundations to recent developments and open issues for model assessment and improvement. In *Handbook of partial least squares* (pp. 47–82). Springer.

8 Appendix A – Instrument Scenarios

8.1.1

8.1.2 Scenario 1 - USB Drive

Chris is a mid-level manager in a medium-sized company where he has worked for several years. Chris is working on an important report that requires analysis of the company's customer database, which contains sensitive financial and purchase history information. Chris is leaving on a business trip and is scheduled to return the day the report is due. Because of the sensitive nature of corporate data, the company has a strict policy that prohibits copying data to USB drives. Chris feels that copying the data to a USB and analyzing it while on the road will save time, money, and ensure the report is submitted on time. Accordingly, Chris copies the data to a USB.

8.1.3 Scenario 2 – Workstation Logout

Chris is a mid-level manager at a medium-sized company where he has worked in the inventory procurement department for several years. The company uses software that allows authorized employees to make inventory purchases. The company has a strict policy that employees must log off or lock workstations when not in use. However, Chris's department is very short staffed and the log on process for the procurement software is long, tedious, and slow. Chris feels that keeping his workstation logged-on and unlocked throughout the day saves time and allows him to work more efficiently. Accordingly, Chris leaves his workstation logged on and unlocked throughout the workday.

8.1.4 Scenario3 – Password Sharing

Chris is a mid-level manager at a medium company where he has worked for several years. The company has a strong policy that workstations must be password protected and that passwords must not be shared. However, Chris is on a business trip and a co-worker needs a file that is stored on Chris's workstation in order to complete an important report that is due today. Chris feels that sharing his password in instances like this one saves time and effort. Accordingly, he gives the coworker the password.

9 Appendix B - Instrument Measures

Unless otherwise noted, all items were measured on a standard seven-point Likert scale, anchored at one with strongly disagree and at seven with strongly agree.

Construct	Moody et al. Item ID	Moody et al. Item Text	Our Item Text	Our Item Num
Intention	Intent1	What is the chance you would do what Mattila did in the described scenario?	I would likely do what Chris did in the described scenario.	Intention1
	Intent2	I would act in the same way as Mattila did if I were in the same situation.	In a similar situation, I would respond like Chris.	Intention2
Severity	Sever1	An information security breach in my organization would be a serious problem for me.	An information security event resulting from my behavior could cause serious problems.	Severity3
	Sever2	An information security breach in my organization would be a serious problem for my organization.	An information security incident could have a critical effect on my company.	Severity2
	Sever3	If I were to do what Mattila did, there would be a serious information security problem for my organization.	Causing an information security incident could have severe consequences.	Severity1
Susceptibility	Vulner1	I would be subjected to an information security threat if I were to do what Mattila did.	The probability of security incidents occurring is heightened when people don't follow security policies.	Susceptibility2
	Vulner2	My organization would be subjected to an information security threat if I were to do what Mattila did.	Not following information security policies is likely to result in a security event.	Susceptibility3
	Vulner3	An information security problem would occur if I were to do what Mattila did.	A security incident would likely occur if I were to do what Chris did.	Susceptibility1
Response Efficacy	RespEff2	If I were to comply with information security procedures, IS security breaches would be scarce.	Complying with information security policies really helps the company avoid security incidents.	Resp_Efficacy1
	RespEff3	If I were to do the opposite to what Mattila did, it would keep IS security breaches down.	Not behaving like Chris keeps security breaches to a minimum.	Resp_Efficacy3

Construct	Moody et al. Item ID	Moody et al. Item Text	Our Item Text	Our Item Num
	RespEff4	If I were to do the opposite to what Mattila did, IS security breaches would be minimal.	Doing the opposite of Chris helps keep security events from happening.	Resp_Efficacy2
Self-Efficacy	SelfEffi2	I can use information security measures if someone tells me what to do as I go along.	I can abide by my company's security policies if instructions are provided for dealing with situations like the one described.	Self_Efficacy1
	SelfEffi3	Doing the opposite of what Mattila did would be difficult for me to do.	In a similar situation, it would be easy for me find a solution to the situation that fits within the boundaries of the security policy.	Self_Efficacy2
	SelfEffi4	Doing the opposite of what Mattila did would be easy for me to do.	In a similar situation, I would be able to figure out a way to abide by the policy.	Self_Efficacy3
Response Cost	Responceco st1	Complying with information security procedures would be time consuming.	In Chris's situation, complying with the policy would be time consuming.	Resp_Cost1
	Responceco st2	Complying with information security procedures would take work time.	Following the security policy in the given scenario would take additional work time.	Resp_Cost2
	Responceco st4	Complying with information security procedures makes my work more difficult.	Following security policies sometimes makes work more difficult.	Resp_Cost3
Rewards	Rewards/ Costs1	If I were to do what Mattila did, I would save time.	If I were to do what Chris did, it would save time.	Rewards1
	Rewards/ Costs2	If I were to do what Mattila did, I would save work time.	Responding like Chris would save work time.	Rewards2
	Rewards/ Costs3	Not complying with information security procedures saves work time.	In the given situation, not complying with the policy saved time.	Rewards3
Habit	Habit1	Complying with information security procedures is something I do frequently	I normally comply with information security policies.	Habit1
	Habit10	Complying with information security procedures is something I have no need to think about doing.	Complying with security policies is something I do without thinking.	Habit2

Construct	Moody et al. Item ID	Moody et al. Item Text	Our Item Text	Our Item Num
	Habit11	Complying with information security procedures is something that's typically "me."	Complying with security policies is something I do automatically.	Habit3
Attitude (semantic differential scale)	Atti2	If I were to do what Mattila did it would be a very: foolish idea – wise idea	In a similar situation, doing what Chris did would be a very wise/foolish idea	Attitude1
	Atti3	If I were to do what Mattila did it would be a very: unpleasant idea – pleasant idea	In a similar situation, doing what Chris did would be a very good/bad idea	Attitude2
	Atti4	If I were to do what Mattila did it would be a very: negative idea – positive idea	In a similar situation, doing what Chris did would be a very: negative idea – positive idea	Attitutde3
Subjective Norms	Subnorm1	I believe that top management in my organization thinks I should do what Mattila did.	I believe top management in my company thinks that I should do what Chris did.	Subject_Norm1
	Subnorm2	I believe that my immediate supervisor in my organization thinks I should do what Mattila did.	My immediate supervisor thinks I should respond like Chris.	Subject_Norm2
	Subnorm3	I believe that coworkers in my organization think I should do what Mattila did.	My coworkers think that I should respond like Chris.	Subject_Norm3
Facilitating Conditions	FacCon2	I have enough knowledge to follow information security procedures.	I have enough knowledge to follow information security procedures.	Fac_Cond1
	FacCon3	I need more guidance from my superiors with work-related information security policies.	I need more guidance from my superiors regarding information security policies at my company.	Fac_Cond2
	FacCon4	I need more guidance from the IT/information security personnel regarding information security issues related to my work	I need more guidance from IT regarding security policy issues related to my work.	Fac_Cond3
Affect	Affect1	What Mattila did is smart.	What Chris did is smart/dumb	Affect1

Construct	Moody et al. Item ID	Moody et al. Item Text	Our Item Text	Our Item Num
	Affect3	What Mattila did is enjoyable.	What Chris did makes sense/is senseless	Affect2
	Affect4	What Mattila did is pleasant.	What Chris did is reasonable/ is unreasonable	Affect3
Roles	Roles1	What Mattila did is compatible with his/her work.	What Chris did is compatible with his/her work.	Roles1
	Roles2	What Mattila did fits with his/her work style.	What Chris did is fits his/her job.	Roles2
	Roles3	What Mattila did can be justified due to the nature of Mattila's work.	Chris's choice can be justified due to the nature of his/her job.	Roles3
Self-Concept	SelfCon1	I would feel guilty if I did what Mattila did.	I would feel guilty if I did what Chris did.	Self_Con1
	SelfCon2	What Mattila did is consistent with my principles.	What Chris did is not consistent with my principles.	Self_Con2
	SelfCon3	It is acceptable to do what Mattila did.	It is not acceptable to do what Chris did.	Self_Con3
Social Factors	SocialFact1	With respect to complying with information security procedures, I have to do as the top management of my organization thinks	In my company, information security policy compliance is important.	Social_Fact1
	SocialFact2	With respect to complying with information security procedures, I have to do as my colleagues think.	My coworkers frown on those who do not follow the company's information security policies.	Social_Fact2
	SocialFact3	With respect to complying with information security procedures, I have to do as my superiors think.	People in my company are diligent about complying with information security policies.	Social_Fact3
Punishment	Formalcert2	I would receive corporate sanctions if I violated company information security procedures.	If management learned I had violated an information security policy, I would be punished.	Punishment1
	Formalsev2	I would receive severe corporate sanctions if I	The sanctions would be severe if it were known that	Punishment2

Construct	Moody et al. Item ID	Moody et al. Item Text	Our Item Text	Our Item Num
		violated company information security procedures.	I violated an information security policy.	
	Formalcert3	What is the chance that you would be warned if management learned you had violated company information security procedures?	I would be in trouble if management learned I had violated an information security policy.	Punishment3
Fear	Fear7	My computer might be compromised if I did what Mattila did.	Computers might be compromised if I did what Chris did.	Fear1
	Fear10	My computer might become unusable if I did what Mattila did.	Company systems might become unusable if I did what Chris did.	Fear2
	Fear11	My computer might become slower if I did what Mattila did.	Company computers might become slower if I did what Chris did.	Fear3
Neutralization	Neutcond3	It is not as wrong to violate company information security procedures that are too restrictive.	It is not wrong to violate security policies that are too restrictive.	Neutralizaiton1
	Neutloyal1	It is alright to violate company information security procedures to get a job done.	It is alright to ignore a security policy to get a job done.	Neutralization2
	Neutinjury3	It is OK to violate company information security procedures if no one gets hurt.	It is OK to violate a security policy as long as no one gets hurt.	Neutralization3
Reactance	React4	To what degree do you feel that problems resulting from acting like Mattila did are overly exaggerated?	To what degree do you feel that problems resulting from doing things like Chris did are exaggerated/downplayed?	Reactance1
	React3	To what degree do you think that problems resulting from acting like Mattila did are overstated?	To what degree do you feel that problems resulting from doing things like Chris did are overstated/understated?	Reactance2
			To what degree do you feel that problems resulting from doing things like Chris did are a fake problem/a real problem?	Reactance3

About the Authors

Diana K. Young is an Assistant Professor at Trinity University in San Antonio, TX. Her research interests include behavioral cyber security, software development processes, data analytics, health information systems, and IT related work-force issues. Her research has been published in the Journal of Computer Information Systems, the Association for Information Systems Transactions on Replication Research, Journal of Information Systems Education, the Journal of Medical Internet Research, and the Communications of the Association for Information Systems. Beyond her academic pursuits, she possesses over 20 years of practical IT experience.

Alexander McLeod is an Associate Professor and Chair of the Health Information Management Department at Texas State University. His research interests include cyber security, cyber analytics, healthcare information systems and ethics. He has publications in Decision Support Systems, Information Systems Frontiers, Communications of the Association of Information Systems, Transactions in Replication Research, Business Process Management, Decision Science Journal of Innovative Education and Information Technology and People.

Darrell Carpenter is the Director of the Center for Cyber Security and an Assistant Professor of Information Systems and Cyber Security at Longwood University in Virginia. His primary research interests include behavioral and organizational aspects of systems security including acceptance /rejection of security technologies, motivations for engaging in risky on-line behavior, and on-line deception. He is also interested in information privacy, technology adoption/continuance behaviors, and inter-organizational benefits/effects of information systems. His research is published academic outlets including Information Systems Frontiers, Information & Management, the Journal of Computer Information Systems, Computers in Human Behavior, Communications of the Association of Information Systems, the Association for Information Systems Transactions on Replication Research, and the International Journal of Information Management.