Transactions on Replication Research

Methodological Replication DOI: 10.17705/1atrr.00053 ISSN 2473-3458

A Replication Study of User Motivation in Protecting Information Security using Protection Motivation Theory and Self-Determination Theory

Ning Yang
Department of Information Systems, Statistics and Management Science
Culverhouse College of Business
The University of Alabama
nyang@crimson.ua.edu

Tripti Singh
Department of Information Systems, Statistics and Management Science
Culverhouse College of Business
The University of Alabama
tsingh3@crimson.ua.edu

Allen C. Johnston
Department of Information Systems, Statistics and Management Science
Culverhouse College of Business
The University of Alabama
ajohnston@cba.ua.edu

Abstract:

Securing one's data and protecting important information from various security threats are essential tasks for all end users, whether they be home users or organizational users. The motivation for doing so, however, may be entirely different for these two user populations. In 2017, Menard et al. conducted a study of home end users' behavioral intentions regarding the installation of password management software using Self-Determination Theory (SDT), Protection Motivation Theory (PMT), and an integrated SDT-PMT model. This methodological replication study replicated those model comparisons to test organizational users' behavioral intentions. We surveyed more than 300 organizational users who did not have password management software installed on their devices. We found support to suggest that, while both home and organizational users are significantly motivated by PMT- and SDT-enabled appeals, organizational users are significantly more motivated than their home user counterparts to install password management software when exposed to SDT-embedded appeals. We believe this outcome is the result of the multi-faceted sense of accountability (to themselves, their coworkers, and their organization) that organizational users experience but home users do not. This methodological replication of Menard et al. (2017) provided an opportunity to expose this multi-faceted view of accountability among organizational users and offers a foundation for future research to delve more closely into the nature of accountability in this context.

Keywords: Information Security, Protection Motivation Theory, Security model comparison, Self-Determination Theory, User security behaviors, Organizational users

The manuscript was received 06/19/2019 and was with the authors 8 months for 3 revisions.

1 Introduction

End users, regardless of whether they are organizational users or home users, must protect their information from various forms of security threats. In the past, Protection Motivation Theory (PMT) has been adapted to the information security (InfoSec) context to better understand what drives end users to engage in such protective behaviors. Fear-appeal manipulations, as the core of PMT, were used to produce fear and to inspire users' motivations to protect information security (Boss et al. 2015; Johnston et al. 2015). However, there is no motivation-related construct in the PMT-related studies in InfoSec. This suggests that prior studies have failed to account for all the intrinsic and extrinsic motivations that trigger protective response behaviors (Menard et al. 2015). In response to this limitation of PMT, Menard et al. (2017) integrated Self-Determination Theory (SDT) with PMT to examine how motivation and its three antecedents of autonomy, competence, and relatedness explain and predict the protective security behaviors of home end users (henceforth referred to as home users). The results of their study indicate that, compared to a fear appeal (i.e., a PMT-embedded appeal), a self-determined appeal (i.e., a SDT-embedded appeal) tends to boost a more internalized motivation in home users to protect their information and digital assets. Their study was the first to directly compare the impact of SDT-embedded appeals and PMT-embedded fear appeals on home users' motivations and behavioral intentions to install password management software.

An important possible boundary condition of the integrated model developed by Menard et al. (2017) is its focus on home users. Organizational users are just as important to our understanding of protection motivation, perhaps even more so because of their role in helping organizations lose about $8.76 million annually (Ponemon Report 2018). Organizational users are employees of organizations who engage with both personal and organizational information technology and data in their daily work and have some responsibility for the protection of those assets. They are fundamentally required to participate in security practices, yet the exact nature of their participation is, for the most part, volitional (Johnston et al. 2019). To further complicate matters, many organizational users are allowed to use their personal devices at work and will often transmit and store organizational data on these devices. However, the extent to which they engage in recommended security protection behaviors such as advanced password schemas, data encryption, or password management tool usage to protect organizational assets accessed or stored in these personal devices is dependent upon their own discretion (Crossler et al. 2014; Menard et al. 2017).

Unlike home users, who are driven solely by personal reasons and manage their own implications for non-secure behavior, organizational users are accountable to others and to their employer. Yet this diversity of accountability should not be assumed to imply a sense of responsibility for the protection of organizational assets. Recent research has shown that organizational employees do not see organizational assets in the same light as they do personal assets when it comes to motivations to protect them (Johnston et al. 2015). Even when using their own devices at work, it is not clear that organizational users are motivated to protect the organizational data on them in the same way they are motivated to protect their personal data.

This variance in motivation is a critical distinction between organizational and home users, and, while Menard et al. (2017) claim their "self-determined appeal and integrated SDT-PMT model is applicable to organizational settings," (Menard et al. 2017, p. 1225), we believe that claim may not stand up well to scrutiny. Although both SDT and PMT are individual-level theories that can explain behavioral changes, home users and organizational users might react differently to the same security appeal. Home users, accountable solely to themselves, are likely to be highly motivated to protect their personal information, but it is still not clear that the sense of motivation applies similarly to organizational users asked to protect organizational assets. For these reasons, we believe a methodological replication of the study conducted by Menard et al. (2017) is warranted. In the current study, we adopted the same methods as the original study, but focused on organizational users. We examined organizational users' intentions to voluntarily install password management software using a PMT-only model, an SDT-only model, and an integrated SDT-PMT model.

2 Theoretical Background and Associated Hypotheses

The hypotheses tested in the current study are the same as those tested in the original study (see Figure 1), but the target population is the organizational user. Table 1 contains the hypotheses for the current replication study.

Table 1. Hypotheses for the Replication Study

Hypothesis 1	Perceived relatedness will positively influence perceptions of threat severity.
Hypothesis 2	Perceived relatedness will positively influence perceptions of threat susceptibility.
Hypothesis 3	Perceived competence will positively influence perceptions of self-efficacy.
Hypothesis 4	Perceived autonomy will positively influence perceptions of response efficacy.
Hypothesis 5	Perceived autonomy will negatively influence perceptions of response cost.
Hypothesis 6a	Perceived relatedness will positively influence motivation toward performing the recommended response.
Hypothesis 6b	Perceived competence will positively influence motivation toward performing the recommended response.
Hypothesis 6c	Perceived autonomy will positively influence motivation toward performing the recommended response.
Hypothesis 7a	Perceived threat severity will positively influence behavioral intention to perform secure behaviors.
Hypothesis 7b	Perceived threat susceptibility will positively influence behavioral intention to perform secure behaviors.
Hypothesis 7c	Perceived self-efficacy will positively influence behavioral intention to perform secure behaviors.
Hypothesis 7d	Perceived response efficacy will positively influence behavioral intention to perform secure behaviors.
Hypothesis 7e	Perceived response cost will negatively influence behavioral intention to perform secure behaviors.
Hypothesis 7f	Motivation toward performing the recommended response will positively influence behavioral intention to perform secure behaviors.
Hypothesis 7g	Perceived relatedness will positively influence behavioral intention to perform secure behaviors.
Hypothesis 7h	Perceived competence will positively influence behavioral intention to perform secure behaviors.
Hypothesis 7i	Perceived autonomy will positively influence behavioral intention to perform secure behaviors.

The hypothesized model is as follows:

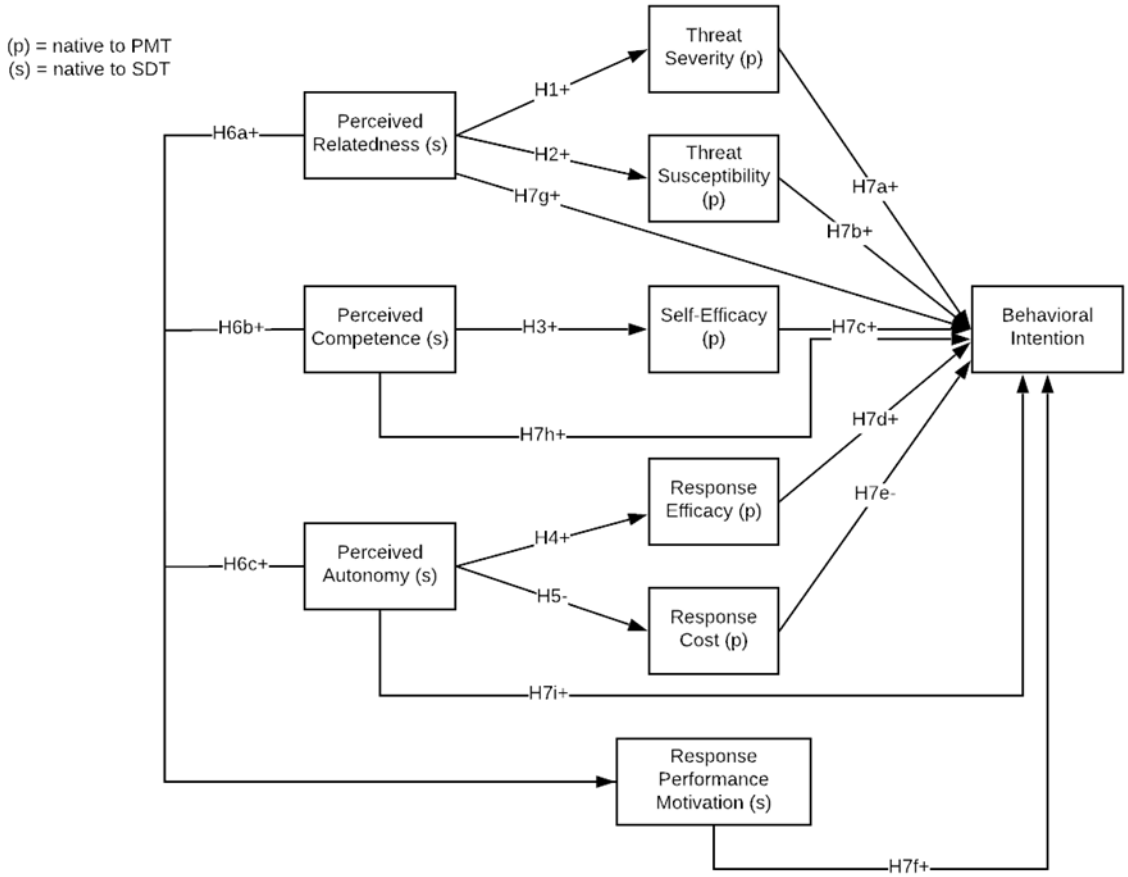

Figure 1. Integrated Model of SDT and PMT from the Original Study

3 Method

Being that we conducted a methodological replication, we used the same research design as Menard et al. (2017); however, we conducted the replication study with organizational users rather than home users. Consistent with Menard et al. (2017) and in order to detect and differentiate the effectiveness of SDT- and PMT-embedded appeals, we conducted a full factorial experimental design whereby each participant was presented with either an SDT-only or a PMT-only appeal. Each appeal was designed to trigger the participant's perceptions of the independent variables from the SDT or the PMT models. The integrated model contains variables from both the SDT models and the PMT model and articulates the relationships that autonomy, competence, and relatedness from the SDT model have with the PMT variables. We used the integrated model to examine whether variances in the PMT variables can be explained by the SDT variables.

3.1 Sampling Frame

Similar to Menard et al. (2017), we designed the survey using Qualtrics and recruited organizational user participants via Amazon Mechanical Turk (MTurk). Mechanical Turk has been previously validated as a way to recruit reliable participants in much academic research. As the original study has stated, U.S. participants on Mechanical Turk are more reliable than participants from other countries. Therefore, we also used only U.S. participants in the replication study and included attention check questions in the measurements to ensure the participants were answering the measurement items attentively. Further, because our desired sample was organizational users of electronic devices, we also restricted participation to MTurk workers who self-selected as people who used their devices for organizational purposes. Anonymity in the MTurk platform makes it difficult to verify an MTurk worker's employment status (Jia, Steelman, and Reich 2017),

but by following the MTurk data collection recommendations provided by Jia et al. (2017), (e.g. asking for a verifiable work email address, keeping the compensation for participation moderate ($1.5), and restricting participation to a single opportunity), we were able to increase the validity of the self-reported organizational user status of our sample. Table 2 contains the basic demographic information of the participants.

Table 2. Summary of Demographic Characteristics

		Percentage (%)
Gender		
	Male	56.23
	Female	43.13
	Unreported	0.01
Ethnicity		
	White, non-Hispanic	58
	Hispanic	21.4
	African American	11
	Asian	6.7
	Native American	0.6
	Pacific Islander	0.2
	Others	1.9
	Unreported	0.4
Age		
	25-34	40.5
	35-44	29.7
	45-54	13.2
	55-64	9.3
	Over 65	1.7
Employee Status		
	Full-time	80.7
	Part-time	11.7
	Unemployed	2.8
	Retired	2.2
	Disabled	1.5
	Student	0.6
Education Background		
	Two-year college or Higher Degree	67.1
	Some College Education	21.9
	High School or Lower	10
Occupation		
	Wholesale/retail	11.9
	Information Technology	11.7
	Education	10.2
	Healthcare Service	8.4
	Finance/insurance	8.2
	Business Service/Legal/Accounting	7.6

Participants had averaged 20.60 years of computing experience (SD = 7.75).

3.2 Procedures

The participants in our study were first presented with a filter question to determine if they used their own electronic devices for organizational purposes. A second filter question was then presented to determine if they had password management software already installed on their electronic device. Participants who used their devices for organizational purposes were deemed organizational users of their own devices and, if they did not have a password management software already installed on their respective electronic device, they were allowed to participate further in our study, starting with the presentation of either an SDT- or PMT-embedded appeal. This sample of organizational users are effectively bring your own device (BYOD) participants in their respective organizations – a more and more commonly occurring phenomenon in businesses (Doargajudhur and Dell 2019)).

Since we used a full factorial experiment design, one participant was presented with only one scenario. For example, if one participant was presented with SDT-embedded appeals, he or she would read one combination of statements within SDT-embedded appeals. He or she would not read scenarios with PMT-embedded appeals. After they read their designated appeal, the participants were then asked to report how likely they would be to install password management software on a 10-point scale ranging from “not likely at all” to “extremely likely”. Then the participants were assessed for perceptions of threat and coping appraisals and motivational variables. Participants directed to the SDT-embedded appeals were assessed on questions of SDT-related antecedents, while participants in the PMT group were asked to answer questions of PMT-related antecedents. As for the integrated SDT-PMT model, participants who were directed into this group were required to answer questions of both SDT- and PMT-related antecedents. For this assessment, the measures were assessed using a 5-point Likert scale ranging from “strongly disagree” to “strongly agree.” The SDT- and PMT-embedded appeals and measures were adapted from the Menard et al. (2017). Also, similar to Menard et al. (2017), participants were presented with demographic questions at the end of the study. The full instrument is presented in Appendix A.

3.3 Power Analysis and Data Collection

Based on the estimates provided by Menard et al. (2017), we conducted a F-test: Two-way ANOVA for fixed effect, special main effects, and interactions using G*Power. This test is used to calculate the power of the main effects in fixed-effects ANOVA with factorial designs. In accordance with the original study we have the constructs (factors) of SDT and PMT manipulated at two levels (presence and absence of variable), suggesting a factorial design with degrees of freedom equal to one (number of levels (2)-1 =1). Based on this calculation, we projected that for a sample of organizational users that were exposed to SDT-embedded appeals, we needed a minimum sample of 128 participants. For a sample of organizational users that were exposed to PMT-embedded appeals, we required a minimum of 129 participants. Based on some attrition in our full factorial experimental design, we collected responses from 897 participants, of which 431 participants were excluded because they already had password management software installed on their electronic devices (laptop/desktop/tablet/smartphone). Our final sample of the analysis for the integrated SDT-PMT model consisted of 153 participants. We had a final sample of 313 participants for the comparison between the SDT and PMT models. Of these 313 participants, 156 had seen an SDT-embedded appeal, and 157 had seen a PMT-embedded appeal.

4 Data Analysis and Results

In terms of analyzing the data obtained in our experimental design, we used the same data analysis techniques and software as in the original study, structural equation modeling using Smart PLS version 2.0.

4.1 Measurement Validity

All the measurements used in the replication study were from Menard et al. (2017). All scale items were modeled as reflective indicators of their associated hypothesized constructs. We tested item convergent validity and examined cross-loadings for validating the measurements of all models. The results of all measurement validity were included and shown in Appendix B.

4.2 Hypothesis Testing

The overall findings and path coefficients are show in Figure 2 and indicate that eight of the 17 hypotheses were supported. The supported hypotheses were in solid lines showed in Figure 2. The integrated SDT-PMT model explained 58.4% of the variance in organizational users' behavioral intentions to install password management software. Further, the SDT variables that affect the PMT model explain 31% of the variance in threat severity, 7.8% of the variance in threat susceptibility, 12.2% of the variance in self-efficacy, 44.9% of the variance in response efficacy, and 4.7% of the variance in response cost. All three SDT variables, relatedness, competence, and autonomy, combine to explain 67.6% of the variance in organizational users' motivation to install password management software. Table 3 contains a comparison of the Menard et al.'s (2017) original study and our methodological replication of their study based on the results of the integrated SDT-PMT model.

Table 3. Comparison of the Variances Explained in the Integrated Model from the Original Study and from the Replication Study

	Original Study	**Replication study**
Integrated model→ BI	54.8%	58.4%
Relatedness→ Threat Severity	41.3%	31%
Relatedness→ Threat Susceptibility	13.2%	7.8%
Competence→ Self-Efficacy	6.6%	12.2%
Autonomy → Response Efficacy	37.6%	44.9%
Autonomy → Response Cost	12.3%	4.7%
SDT→ BI	39.9%	67.6%

In Menard et al.'s (2017) original study, 12 hypotheses were supported, and their integrated SDT-PMT model was able to explain 54.8% of the variance in home users' behavioral intentions to install password management software. The integrated model explained 41.3%, 13.2%, 6.6%, 37.6%, and 12.3% of the variances in threat severity, threat susceptibility, self-efficacy, response efficacy, and response cost, respectively. Therefore, we can see that the integrated model worked slightly better for organizational users than home users. The SDT variables were able to explain much more variance in organizational users' motivation (67.6%) to perform the recommended response than in home users (39.9%).

There are some differences based on the findings of the original study and those of the replication study. In the original study, autonomy, relatedness, and competence all have significant impacts on home users' motivation, while only autonomy has a significant positive influence on organizational users' motivation. It seems that in the replication study that relatedness and competence have no significant impact on organizational users' motivation to install the password software.

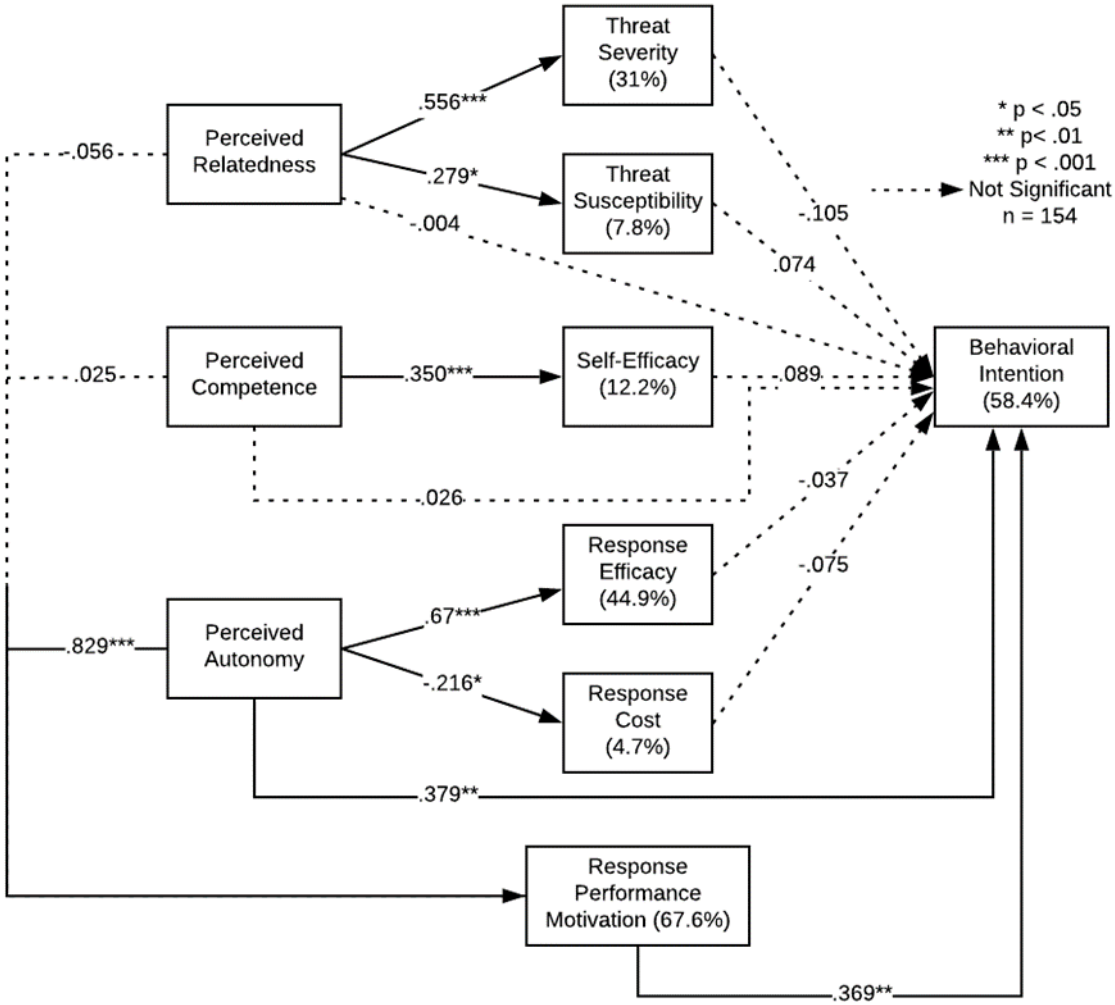

Figure 2. Integrated SDT-PMT Model with Path Significance and Explained Variance

When we examined the individual relationships in the integrated model, we followed Menard et al.'s (2017) inspection and began with the paths related to the integration of SDT and PMT. We analyzed the relationships between the motivational antecedents, relatedness, competence, and autonomy, and the variables from the traditional PMT model. Presented in Table 4, relatedness had a significant positive effect on threat severity (β = .556, p < .001) and threat susceptibility (β = .279, p < .05). Competence also revealed a significant positive effect on self-efficacy (β = .350, p < .001). Autonomy posed a significant positive influence on response efficacy (β = .67, p < .001) and a significant negative impact on response cost (β = -.216, p < .05). These were all consistent with the findings from the original study where it was clear that motivational antecedents from SDT further reinforced home users' perceptions of the PMT variables and successfully elicited their intrinsic desire to protect data. In our methodological replication, we are also able to confirm that the motivation antecedents reinforce organizational users' perceptions of all five PMT variables and trigger their intrinsic desire to protect data.

Next, we examined the effect of relatedness, competence, and autonomy on motivation, and the influence of motivation on behavioral intention. An organizational user's motivation to install password management software had a significant positive impact on his or her behavioral intention to perform the response (β = .369, p < .01). Unlike the original study suggested, however, our findings suggest that only autonomy revealed a significant positive influence on organizational users' motivation to perform the appeal's recommended response (β = .829, p < .001), with relatedness and competence having no significant impact on organizational users' motivation.

Finally, the direct paths between motivational antecedents and behavioral intention, along with the traditional PMT variables and behavioral intention, were analyzed. Among the eight direct paths, only one was

significant. Threat severity (β = -.105, $p > .05$), threat susceptibility (β = .074, $p > .05$), self-efficacy (β = .089, $p > .05$), response efficacy (β = -.037, $p > .05$), and response cost (β = -.075, $p > .05$) all failed to show a significant direct influence on organizational users' behavioral intention to install password management software. Although relatedness (β = -.004, $p > .05$) and competence (β = .026, $p > .05$) did not significantly affect behavioral intention, autonomy had a significant positive effect on organizational users' behavioral intention (β = .376, $p < .01$). In the original study, there were three significant direct paths stemming from the PMT model to home users' behavioral intention to install password management software: response-efficacy, competence, and autonomy. Therefore, competence and response-efficacy can be attributed to the behavioral intention of home users to install password management software, but not organizational users' intentions.

Table 4. Comparison of Path Estimates between Original Study and Replication Study-Integrated Model

Hypothesis (with direction)	Path coefficient (β)	*t*-statistics	*p-value*	Supported
H1: REL → TSEV (+)				
Original Study	0.642	21.298	< 0.001 ***	Yes
Replication Study	0.556	5.705	5.890E-08 ***	Yes
H2: REL → TSUS (+)				
Original Study	0.363	9.101	< 0.001 ***	Yes
Replication Study	0.279	2.421	0.017 *	Yes
H3: COMP → SEF (+)				
Original Study	0.256	5.397	< 0.001 ***	Yes
Replication Study	0.350	4.511	1.284E-05 ***	Yes
H4: AUTO → REF (+)				
Original Study	0.613	19.059	< 0.001 ***	Yes
Replication Study	0.67	12.771	7.724E-26 ***	Yes
H5: AUTO → COS (-)				
Original Study	-0.351	7.568	< 0.001 ***	Yes
Replication Study	-0.216	2.074	0.039 *	Yes
H6a: REL → MOT				
Original Study (+)	0.110	3.059	< 0.05 *	Yes
Replication Study (-)	-0.056	0.849	0.397	No
H6b: COMP → MOT (+)				
Original Study	0.083	1.934	< 0.05 *	Yes
Replication Study	0.025	0.278	0.782	No
H6c: AUTO → MOT (+)				
Original Study	0.565	16.821	< 0.001 ***	Yes
Replication Study	0.829	15.067	5.781E-32 ***	Yes
H7a: TSEV → BI				
Original Study (+)	0.048	1.436	> 0.05	No
Replication Study (-)	-0.105	1.187	0.237	No
H7b: TSUS → BI (+)				
Original Study	0.010	0.308	> 0.05	No
Replication Study	0.074	0.861	0.391	No
H7c: REF → BI				
Original Study (+)	0.011	0.305	> 0.05	No
Replication Study (-)	-0.037	0.377	0.707	No
H7d: SEF → BI (+)				
Original Study	0.088	2.185	< 0.05 *	Yes
Replication Study	0.089	1.081	0.281	No
H7e: COS → BI (-)				

Original Study	-0.024	0.572	> 0.05	No
Replication Study	-0.075	0.925	0.356	No
H7f: MOT → BI (+)				
Original Study	0.319	7.334	< 0.001 ***	Yes
Replication Study	0.369	3.040	0.003 **	Yes
H7g: REL → BI				
Original Study (+)	0.013	0.356	> 0.05	No
Replication Study (-)	-0.004	0.048	0.962	No
H7h: COMP → BI (+)				
Original Study	0.114	3.603	> 0.05	No
Replication Study	0.026	0.346	0.730	No
H7i: AUTO → BI (+)				
Original Study	0.344	7.242	< 0.001 ***	Yes
Replication Study	0.379	3.012	0.003 **	Yes
Notes: * P < 0.05; ** P < 0.01; *** P < 0.001				

4.3 Analysis of Differences between Self-Determination Theory and Protection Motivation Theory Models for Organizational Users

In order to assess the differences between the two competing models (SDT and PMT), we followed Menard et al.'s (2017) lead and used an adapted version of Motulsky and Ransnas (1987) to conduct a series of F-tests using the models' residual sum of squares and degrees of freedom. We also included the adjusted R^2 values to show the variances explained in the dependent variables by the independent variables presented in the models. Table 5 contains the results of the model and hypothesis comparisons within the replication study.

Table 5. Results of Model and Hypothesis Comparisons for Organizational Users

		Statistics from Model 1				Statistics from Model 2					
Model 1 and Hypothesis	**Model 2 and Hypothesis**	**SSR**	**n**	**IVs**	**R^2**	**SSR**	**n**	**IVs**	**R^2**	***F*-stat**	***p***
Traditional PMT: PMT→ BI	SDT: SDT→ BI	1125.042	156	5	.109	544.088	153	3	.518	159.096	<.001
Modified PMT: PMT→ Mot	SDT: SDT→ Mot	618.927	156	5	.423	407.664	153	3	.576	77.216	<.001
Traditional PMT: PMT→ BI	Modified PMT: PMT+Mot → BI	1125.042	156	5	.109	804.633	156	6	.359	59.332	<.001
Modified PMT: PMT+Mot→ BI	Modified SDT: SDT+Mot→ BI	804.633	156	6	.359	447.582	153	4	.588	118.064	<.001

The first model comparison involved the traditional PMT and SDT models. The traditional PMT model had five independent variables and accounted for 10.9% of the variance in behavioral intention, while the SDT model explained 51.8% of its variance. There was a significant difference between the two models (F =

159.096; p < .001), and the results indicate that the SDT model is able to explain more variance in organizational users' behavioral intention than the PMT model, with fewer independent variables.

The second model comparison also involved a comparison between PMT and SDT, but with organizational users' motivation to install password management software as the dependent variable instead of behavioral intention. The independent variables of PMT explained 42.3% of the variance in motivation, while those from SDT explained 57.6% of its variance. There was a significant difference between these two models (F = 77.216; p < .001), suggesting that the SDT model was better in explaining organizational users' motivation to install password management software.

The third model comparison was between the traditional PMT model and a modified PMT model that positions motivation as an additional variable for organizational users' behavioral intentions to install password management software. The findings of this comparison suggest that, by adding motivation, the modified PMT model was able to explain a significantly greater amount of variance in organizational users' behavioral intention to install password management software (F = 59.332; p < .001), with the explained variance improving from 10.9% to 35.9%.

The last model comparison was between the modified PMT model and a modified SDT model that also included motivation as an additional variable. Although the modified SDT model had fewer independent variables, it was able to explain a significantly greater amount of variance in organizational users' behavioral intentions (58.8% as opposed to 35.9%) to install password management software (F = 118.064; p < .001).

4.4 Analysis of Differences between Self-Determination Theory and Protection Motivation Theory Models across Organizational and Home Users

We also made a similar set of model comparisons, as described in the previous section, to compare the models between home users (Menard et al., 2017) and organizational users (methodological replication). We followed the same process outlined in the previous section, and the results are presented in Table 6.

Table 6. Model Comparisons for Home Users versus Organizational Users

	Model from Original Study-Home Users				Model from Replication Study-Organizational Users					
Comparison	**SSR**	**n**	**IVs**	**R^2**	**SSR**	**n**	**IVs**	**R^2**	**F-stat**	**p**
PMT→ BI	2090.565	449	5	.335	1125.042	156	5	.109	.439	>.05
SDT→ BI	1415.027	336	3	.422	544.088	153	3	.518	1.303	<.05
PMT+Mot→ BI	1705.293	449	6	.458	804.633	156	6	.359	0.567	>.05
SDT+Mot→ BI	1183.636	336	4	.515	447.582	153	4	.588	1.330	<.05

The first model comparison involved the traditional PMT model and its ability to explain the behavioral intentions of home users versus organizational users to install password management software. Based on the *F*-test results (33% for home users versus 10.9% for organizational users), the models did not differ significantly, suggesting that despite the possible influences of personal relevance or psychological ownership stated in the original study, organizational users reacted to a PMT-embedded fear appeal similar to home users.

The second model comparison involved the SDT model and its ability to explain the behavioral intentions of home users versus organizational users to install password management software. The findings of this comparison suggest that the SDT model is able to explain significantly more variances ($F = 1.303$; $p < .05$) in organizational users' behavioral intentions (51.8%) than home users' behavioral intentions (42.2%).

The third model comparison was between the traditional PMT model and a modified PMT model that positions motivation as a mediating variable for home users versus organizational users' behavioral intentions to install password management software. Although the modified PMT model is able to explain more variance in home users' behavioral intentions (45.8%) than those of their organizational users' counterparts (35.9%), the *F*-test indicated that the difference between the two populations was not significant.

Finally, comparisons of a modified SDT model on the behavioral intention of home users versus organizational users reveal that an SDT model that includes motivation as a mediating variable is able to

explain significantly more variance ($F = 1.330$; $p < .05$) in organizational users' behavioral intentions to install password management software (58.8%) than home users' behavioral intentions (51.5%).

5 Discussion and Implications

We conducted the methodological replication of Menard et al. (2017) with organizational users and interpreted our results in light of the original study, where the sample population was home users. As we interpreted our results and made comparisons with the original study, we found organizational users reacted similar to the home users to PMT-embedded fear appeals; however, organizational users are significantly more motivated than their home user counterparts (from the original study) to install password management software when exposed to SDT-embedded appeals. Although autonomy, competence, and relatedness all had significant positive impacts on home users' behavioral intention to install password management software, our findings showed that autonomy is the only antecedent that had a significant positive influence on organizational users' behavioral intention to install password management software. Therefore, an emphasis on autonomy in appeals to organizational users should produce the most favorable response from them.

One possible reason for the greater motivation among organizational users to install password management software could be their multi-faceted sense of accountability, accountability to themselves, their coworkers, and to their organization. Recent research on the topic of deterrence and organizational security has shown that organizational users are concerned with the potential embarrassment and loss of respect and goodwill among their colleagues if they are found responsible for a breach of security (Johnston et al. 2015). It is quite possible that the motivation to install password management software was greater among organizational users because of their desire to remain in good standing among their peers.

In terms of the isolated role of autonomy as the only significant driver of organizational users' motivation and intention to install password management software, a recent study on the collective nature of security efficacy suggests that organizational users do not formulate their security beliefs in isolation, but rather as part of a collective of peers of similar education, rank, and socio-economic standing in their firm (Johnston et al. 2019). In collective environments, the question of autonomy to execute their decisions may be the only true question that drives users' motives and intentions to act. It's not surprising that relatedness and competence were not significant drivers of motivation or intention to install password management software, as the data in question are not their own and likely difficult to relate to. Much of the users' competence with the software could be discounted due to the collective efficacy shared within their community of users (Johnston et al. 2019).

Interestingly, compared with the original study of home users by Menard et al. (2017), organizational users' perceptions of competence with password management software and the efficacy of it as a response to device and asset protection were not significant direct determinants of their intentions to install the software. There are several possible reasons for this outcome, but perhaps the simplest explanation is that organizational users have IT support structures and people in place to compel and support their compliance behavior when they don't feel capable (competence) of installing software or don't believe that the solution will work (response efficacy). In either case, organizational users are prone to succumbing to the pressures provided by organizational IT officers.

The findings of our study also suggest that PMT and SDT are both able to effectively model organizational users' intentions to install password management software, but there are some clear differences in how the two models were differentiated for organizational users compared to the home users studied in the original study by Menard et al. (2017). On its own, PMT clearly struggles to capture organizational user intentions. This is the possible result of having organizational IT support structures and personnel in place – a demotivator of fear-driven responses – or because of a weakly worded fear appeal lacking sufficient details for how the lack of password management software could harm their respective companies. With SDT focused on the motivation to enact protective technologies, such as password management software, there's less of a connection with or influence from local IT support structures and personnel.

Our findings also suggest that SDT works better than PMT in explaining users' intentions regardless of whether they are home or organizational. SDT provides a more parsimonious and more explanatory model of their intentions. It is possible that when users are presented with fear appeals, they might think they are expected to exhibit certain behaviors and might hesitate to follow a recommended course of action. They

may do this simply because performing those actions is not based on their intrinsic motivation to do so. Even if they ultimately perform the recommended response, they do so because they are extrinsically motivated, not intrinsically motivated. However, if a security appeal contains a component of autonomy, it will bolster organizational users' perceptions of intrinsic motivation and perhaps help them avoid thinking that they have been persuaded to act in a certain way.

All told, the findings of this methodological replication reinforce a boundary condition of an integrated model of SDT and PMT for security appeal perceptions that was left unclear in Menard et al. (2017). This replication study confirms the initial contention of Menard et al. (2017), that their integrated model of SDT and PMT is applicable to both home and organizational users, but also suggests that the results will vary significantly depending on the home or organizational user audience to which it is applied. When applied to organizational users, we should expect the model to produce dramatically different results, primarily in terms of the underlying drivers of motivation and intentions to engage in protective security behaviors. As explained in this study, the accountability for organizational users is to many, whereas for home users, they are accountable only to themselves. Future research should delve more closely into the nature of accountability in this context and how it might complement the integrated model of SDT and PMT as a moderating or mediating factor.

Practically speaking, this research suggests that a clear driver of organizational users' motivation for and intentions to engage in protective security behaviors is perceived autonomy. In the original study where autonomy is rarely a question for home users, but in our study of organizational users, there are often situations where the autonomy of decisions and actions may be in doubt. The findings of this research suggest that appeals for action to organizational users would benefit from a focus on making clear to the users their autonomy over their protective security actions.

6 Limitations

Although by having organizational users as the target population of our study, we have addressed one of the limitations of the original study by Menard et al. (2017), our methodological replication of their work is still limited. First, beyond asking participants to self-identify as users of devices for organizational purposes, we did not validate our participants as organizational users. As such, it is possible that some participants may not be organizational users, but that is a general concern among many studies that employ online panel data from sources such as Amazon Mechanical Turk.

Secondly, we did not include any scales to measure organizational users' psychological ownership. Menard et al. (2017) stated that the psychological ownership organizational users' perceive for their organizational assets could affect how they formulate their strategies for protecting them. If we had captured their perceptions of psychological ownership, we could have reported the effect it has on organizational users' intentions to protect their organizational assets.

Also, Menard et al. (2017) pointed out the complexity of organizational contexts, suggesting that there are other possible unknown influences from those contexts that could impact how organizational users response to security threats. We did not identify or include any organizational factors in our methodological replication beyond those presented by Menard et al. (2017), opting instead to remain true to the tenets of methodological replication described by Dennis and Valacich (2014). Future research, however, would benefit from a consideration of characteristics of organizational contexts and users, extending the ability of the integrated model to explain organizational user protective security motivations and intentions beyond what is currently modeled.

Finally, because the focus of this replication study is on organizational users' motivations and intentions to protect their personal devices used for organizational purposes, it's difficult to differentiate whether the protection motivations and intentions are for organizational or personal purposes. Future research should attempt to better isolate these motivations, beyond what is possible in a methodological replication.

References

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors. MIS Quarterly, 39(4), 837–864.

Churchill, G. A. (1979). A Paradigm for Developing Better Measures of Marketing Constructs. Journal of Marketing Research, 16(1), 64–73.

Doargajudhur, M., and Dell, P. (2019). Impact of BYOD on Organizational Commitment: An Empirical Investigation. Information Technology and People, 32(2), 246-268.

Gefen, D., and Straub, D. (2005). A Practical Guide To Factorial Validity Using PLS-Graph: Tutorial And Annotated Example. Communications of the Association for Information Systems, 16, 91–109.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.

Jia, R., Steelman, Z., and Reich, B. (2017). Using Mechanical Turk Data in I.S. Research: Risks, Rewards, and Recommendations. Communications of the Association for Information Systems, 41, 301-318.

Johnston, A. C., Gangi, P. M. D., Howard, J., and Worrell, J. (2019). It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups. Journal of the Association for Information Systems, 20(3), 186–212.

Johnston, A. C., Warkentin, M., and Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. MIS Quarterly, 39(1), 113–134.

Lowry, P. B., and Gaskin, J. (2014). Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It. IEEE Transactions on Professional Communication, 57(2), 123–146.

Menard, P., Bott, G. J., and Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. Journal of Management Information Systems, 34(4), 1203–1230.

Motulsky, H. J., and Ransnas, L. A. (1987). Fitting Curves to Data Using Nonlinear Regression: A Practical and Nonmathematical Review. *FASEB Journal : Official Publication of the Federation of American Societies for Experimental Biology,* 1(5), 365–74.

Ponemon Report. (2018, April 23). Cost of Insider Threat – Global Organizations. Retrieved from https://www.observeit.com/ponemon-report-cost-of-insider-threats/

Shaw, E., Ruby, K. G., and Post, J. M. (1998). The Insider Threat to Information Systems: The Psychology of the Dangerous Insider. *Security Awareness Bulletin*, 2(98), 1-10.

Appendix A: Instrument Items

Behavioral Intention to Install Password Manager Software

Now that you have read the message above, please indicate the likelihood that you will install the password manager software described above:

- Likelihood to install slider scale, 0–10 (0 = Extremely unlikely; 10 = Extremely likely)

Response Performance Motivation (I would choose to install password manager software…)

- …because I think that this activity is interesting.
- …because I think that this activity is pleasant.
- …because I think that this activity is fun.
- …because I feel good when doing this activity.
- …because I am doing it for my own good.
- …because I think that this activity is good for me.
- …because I decided that this activity is beneficial.
- …because I believe that this activity is important to me.
- …because I am supposed to do it.
- …because it is something that I have to do.
- …because I don't have any choice.
- …because I feel that I have to do it.
- …but I am not sure if it is worth it.
- …but I don't see what the activity brings me.
- …but I am not sure it is a good thing to pursue it.
- …but personally I don't see any good reasons to do this activity.

Threat Severity

- If my online passwords were discovered by hackers, it would be severe.
- If my online passwords were discovered by hackers, it would be serious.
- If my online passwords were discovered by hackers, it would be significant.

Threat Susceptibility

- My online passwords are at risk for becoming compromised.
- It is likely that my online passwords will be breached.
- It is possible that my online passwords will be compromised.

Response Efficacy

- Password manager software works for protection.
- Password manager software is effective for protection.
- When using password manager software, online accounts are more likely to be protected.

Self-Efficacy

- Password manager software is easy to use.
- Password manager software is convenient to use.

- I am able to use a password manager without much effort.

Response Cost

- Using password manager software is time consuming for me.
- Using password manager software is burdensome for me.
- Using password manager software is financially costly for me.
- Installing password manager software would require too much from me.
- Installing password manager software is not worth it.

Autonomy

- The software described is what I would choose to install on my computer.
- I feel that the software I'm told to install fits perfectly with what I prefer to use on my computer.
- I feel that the software described is an expression of my own software preferences.
- I feel that I have the opportunity to make choices with respect to what I am told to install in the message.

Competence

- I feel I have a better understanding of password manager software.
- I feel that I effectively learned about password manager software.
- I feel that I did a good job learning about password manager software.
- I feel that I can manage the requirements of learning more about password manager software.

Relatedness

- I feel a strong connection with my digital information.
- If the information contained in my online accounts is affected, then so am I.
- The thought of information contained in my online accounts being tampered with makes me anxious.
- Protecting the information contained in my online accounts is a way to protect myself.

Computing Experience

How many total years of general experience do you have working with a computer in any form (e.g., surfing the internet, spreadsheets, gaming, word processing)? (Text entry)

Appendix B: Instrument Validity

All the scales we used in this replication study were from the original study. We tested the convergent validity similar to the original study. As in Menard et al. (2017), we assessed convergent validity for all of the constructs' scales using three criteria (Churchill, 1979; Gefen and Straub, 2005; Lowry and Gaskin, 2014): (1) all indicator factor loadings should be significant and greater than 0.7, (2) construct composite reliability should be greater than 0.8, and (3) average variance extracted (AVE) of each construct should exceed 0.5. The results of the replication study indicate that construct reliability ranged from 0.821 to 0.947 and AVE ranged from 0.534 to 0.856 for all three models. Therefore, measurement validity was checked and established for the replication study. Table B1 depicts the construct validity values only for the integrated SDT-PMT model.

Table B1. Construct Validity for Integrated SDT-PMT Model	
Construct	**Reliability**
Autonomy	.943
Competence	.926
Relatedness	.821
Response Efficacy	.926
Self-Efficacy	.826
Threat Severity	.926
Threat Susceptibility	.855

We also checked and examined PLS reports for cross-loadings. Convergent validity was significantly established for all constructs except for autonomy and competence. Items for AUTO4 and COMP4 were removed from the analysis because they failed to load on to their respective constructs. All the remaining items in the models had loadings above 0.70 except for two. The first exception was REL1 in the integrated model. The item REL1 had a loading of 0.696 that was very close to 0.70, so we decided to keep it in the model. The other exception was REL4 in the SDT model. We had to drop REL2 from the SDT model because it had a very low loading. Then, the construct of relatedness had only three items: REL1, REL3, and REL4. Therefore, we kept REL4 (0.671) as the third item for relatedness.

Table B2. Cross-Loadings, Reliability, and AVE for Latent Variables-Integrated Model									
	AUTO	COMP	REL	REF	SEF	TSEV	TSUS	**Composite Reliability**	**AVE**
AUTO1	.933	.450	.351	.625	.460	.328	.283	.943	.846
AUTO2	.919	.400	.357	.614	.408	.343	.278		
AUTO3	.907	.395	.277	.610	.414	.284	.293		
COMP1	.471	.882	.366	.352	.336	.128	.093	.926	.807
COMP2	.378	.919	.161	.299	.294	.089	.008		
COMP3	.349	.895	.281	.292	.305	.177	-.037		
REL1	.293	.323	.696	.255	.253	.306	.273	.821	.534
REL2	.158	.148	.719	.253	.079	.465	.088		
REL3	.372	.254	.730	.259	.168	.446	.221		
REL4	.188	.168	.775	.202	.165	.400	.224		
REF1	.555	.305	.266	.880	.401	.292	.250	.926	.807
REF2	.587	.291	.247	.919	.373	.211	.183		
REF3	.658	.355	.376	.895	.340	.204	.350		
SEF1	.262	.234	.080	.220	.794	.176	.019	.862	.676
SEF2	.518	.354	.245	.476	.875	.307	.306		
SEF3	.289	.239	.204	.239	.794	.244	.137		
TSEV1	.359	.153	.494	.184	.267	.878	.313	.926	.807
TSEV2	.291	.124	.510	.260	.268	.911	.190		
TSEV3	.283	.116	.496	.257	.292	.906	.267		
TSUS1	.284	.027	.232	.257	.216	.337	.871	.855	.664
TSUS2	.315	.096	.177	.288	.184	.148	.754		
TSUS3	.149	-.047	.276	.168	.128	.176	.816		

An average variance extracted (AVE) of 0.50 or greater was achieved on all constructs. Factor loading scores for the analysis of the integrated model are shown in Table B2. The scores for PMT items are shown in Table B3, while the scores for SDT items are in Table B4. The reliability of the scales was examined using composite reliability scores. The original study used 0.70 or greater as an accepted level. All constructs in the replication study obtain scores of at least 0.70 for composite reliability.

Table B3. Cross-Loadings, Reliability, and AVE for Latent Variables-PMT Model

	REF	SEF	TSEV	TSUS	**Composite Reliability**	**AVE**
REF1	.897	.207	.212	.092	.917	.786
REF2	.887	.259	.128	.160		
REF3	.875	.163	.202	.019		
SEF1	.273	.865	.272	.117	.877	.707
SEF2	.155	.936	.217	.226		
SEF3	.298	.703	.375	.125		
TSEV1	.234	.353	.956	.307	.947	.856
TSEV2	.175	.213	.895	.283		
TSEV3	.135	.181	.924	.231		
TSUS1	.204	.210	.364	.840	.840	.637
TSUS2	.022	.174	.175	.845		
TSUS3	.004	.070	.176	.701		

Table B4. Cross-Loadings, Reliability, and AVE for Latent Variables-SDTModel

	AUTO	COMP	REL	**Composite Reliability**	**AVE**
AUTO1	.919	.393	.242	.929	.814
AUTO2	.911	.397	.219		
AUTO3	.875	.432	.159		
COMP1	.416	.909	.379	.941	.841
COMP2	.394	.917	.289		
COMP3	.425	.925	.401		
REL1	.251	.308	.790	.814	.595
REL3	.183	.291	.843		
REL4	.055	.333	.671		

Appendix C: Post Hoc Analysis

Mediation Analysis

In the original study, the integrated SDT-PMT model indicated several mediated relationships. Therefore, a series of medication tests were conducted. We adopted the same process to test mediation effects in the replication study, using the Sobel test to determine the significance of the indirect effects in the integrated model. Because all five components of the PMT model: threat severity, threat susceptibility, response efficacy, self-efficacy, and response cost, had no significant direct effect on behavioral intention, they could not mediate the relationships between any SDT antecedent and behavioral intentions.

Similarly, relatedness and competence could not mediate behavioral intention though motivation because both did not show significant direct effects on behavioral intention. The last antecedent of the SDT model, autonomy, demonstrated a significant direct effect on behavioral intention, as well as a significant indirect effect on behavioral intention through motivation ($p < .01$). That was the only mediation effect we found in the replication study. The results of the mediation analysis are shown in Table C1.

Table C1. Mediation Testing for Indirect Effects							
Relationship (IV→ MV →DV)	**ß (IV→MV)**	**S.E. (IV→MV)**	**ß (MV→ DV)**	**S.E. (MV→ DV)**	***t*-Value**	***p*-Value**	**Mediation**
REL→ TSEV→ BI	.556	.098	-.105	.088	-1.168	.243	None
REL→ TSUS→ BI	.279	.115	.074	.086	1.260	.208	None
COMP→ SEF→ BI	.350	.078	.089	.082	.925	.355	None
AUTO→ REF →BI	.670	.053	-.037	.097	-.381	.703	None
AUTO→ COS→ BI	-.216	.104	-.075	.081	.846	.398	None
REL→ MOT →BI	-.056	.066	.369	.121	-.817	.414	None
COMP→ MOT→ BI	.025	.089	.369	.121	.280	.780	None
AUTO→ MOT→ BI	.829	.055	.369	.121	2.99	.003	Partial

Partial Least Squares Analysis of Individual Relationships for Model Comparison

The original study analyzed the individual path estimates and evaluated them in each model. The first model we assessed in the replication study was the traditional PMT model. Shown in Table C2, it is clear that only response efficacy (ß = .341, $p < .001$) shows a significant direct effect on organizational users' behavioral intention to install password management software. The other components of the traditional PMT model had no significant influence on behavioral intention.

Table C2. Path Estimates-Traditional PMT Model				
IV→ DV (with direction)	**Path Coefficient (ß)**	**t-Value**	**p-Value**	**Supported?**
TSEV →BI (-)	-.062	.534	> .05	No
TSUS→ BI (+)	.084	.752	> .05	No
REF→ BI (+)	.341	3.291	< .01	Yes
SEF →BI (+)	.175	1.165	> .05	No
COS→ BI (-)	-.075	.577	> .05	No

The second model we evaluated was the modified PMT model. The modified PMT model included both traditional PMT components and response performance motivation. In this model, response efficacy (ß = .578, $p < .001$) and self-efficacy (ß = .228, $p < .05$) had significant impacts on motivation. Motivation also demonstrated a significant impact on intention (ß = .673, $p < .001$). Other direct effects were not found in the modified PMT model. The results for path estimates are shown in Table C3.

Table C3. Path Estimates-PMT Model with Motivation Included				
IV→ DV (with direction)	**Path Coefficient (ß)**	***t*-Stat**	***p*-Value**	**Supported?**
TSEV →MOT (-)	-.144	1.599	> .05	No
TSUS→ MOT (+)	.165	1.829	> .05	No
REF→ MOT (+)	.578	6.980	< .001	Yes
SEF →MOT (+)	.228	2.076	< .05	Yes
COS→ MOT (+)	.016	.144	> .05	No
TSEV →BI (+)	.035	.307	> .05	No
TSUS→ BI (-)	-.022	.239	> .05	No
REF→ BI (-)	-.048	.358	> .05	No
SEF →BI (-)	-.008	.070	> .05	No
COS→ BI (-)	-.097	.762	> .05	No
MOT→ BI (+)	.673	7.487	< .001	Yes

The third model examined was the traditional SDT model on behavioral intention. Organizational users' behavioral intentions to perform the appeal's recommended response increased as their perceptions of

autonomy (ß = .674, $p < .001$) increased. However, their behavioral intentions did not increase based on the changes in competence or relatedness. This finding indicated that autonomy was the only antecedent in the traditional SDT model that bolstered organizational users' behavioral intentions to perform a recommended response. However, in the original study, all three antecedents in the traditional SDT model had significant impacts on home users' behavioral intentions to perform the recommended response in the fear appeal. Table C4 shows the direct relationships between autonomy, competence, and relatedness toward behavioral intention in the replication study.

Table C4. Path Estimates-Assessing Direct Effects of Self-Determined Appeal on BI

IV→ DV (with direction)	Path Coefficient (ß)	*t*-Stat	*p*-Value	Supported?
AUTO →BI (+)	.674	10.341	< .001	Yes
COMP→ BI (+)	.102	1.311	> .05	No
REL→ BI (+)	.007	.072	> .05	No

Finally, we analyzed the modified SDT model with motivation included. Autonomy had significant positive influences on both motivation (ß = .832, $p < .001$) and behavioral intention (ß = .291, $p < .05$). Response performance motivation also demonstrated a significant impact on organizational users' behavioral intention (ß = .459, $p < .001$). The results of the path estimates for the modified SDT model is illustrated in Table C5. ACR stands for autonomy, competence, and relatedness.

Table C5. Path Estimates-Traditional SDT Model with Direct Effects of ACR on BI Included

IV→ DV (with direction)	Path Coefficient (ß)	*t*-Stat	*p*-Value	Supported?
AUTO →MOT (+)	.832	17.529	< .001	Yes
COMP→ MOT (+)	.044	.598	> .05	No
REL→ MOT (+)	.000	.007	> .05	No
AUTO →BI (+)	.291	2.283	< .05	Yes
COMP→ BI (+)	.122	1.637	> .05	No
REL→ BI (+)	.008	.089	> .05	No
MOT→BI (+)	.459	4.222	< .001	Yes

References

Crossler, R. E., Long, J. H., Loraas, T. M., and Trinkle, B. S. (2014). Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap. *Journal of Information Systems*, 28(1), 209-226.

Johnston, A. C., Di Gangi, P. M., Howard, J., and Worrell, J. (2019). It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups. *Journal of the Association for Information Systems*, 20(3), 186-212.

Johnston, A. C., Warkentin, M., and Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric. *MIS Quarterly*, 39(1), 113-134.

Menard, P., Bott, G. J., and Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems*, 34(4), 1203-1230.

About the Authors

Ning Yang. is a Ph.D. student of Management Information System (MIS) Program, under the Department of Information Systems, Statistics, and Management Science in the Culverhouse College of Business at the University of Alabama. She received her M.A. and M.S. degrees at the University of Alabama. Her research interests include how technology influences people's decisions and behaviors, Cybersecurity, and healthcare analytics.

Tripti Singh. is a Ph.D. student of Management Information System (MIS) Program, under the Department of Information Systems, Statistics, and Management Science in the Culverhouse College of Business at the University of Alabama. She received her M.B.A. and M.P.H. degrees at the University of Alabama at Birmingham. Her research interests include healthcare information systems, behavioral information security, and privacy.

Allen C. Johnston. is an Associate Professor of Management Information Systems (MIS) in the Culverhouse College of Business at the University of Alabama. The primary focus of his research is in the areas of behavioral information security, privacy, data loss prevention, collective security, and innovation. His research can be found in such outlets as MIS Quarterly, Journal of the AIS, European Journal of Information Systems, Information Systems Journal, Decision Sciences, Decision Support Systems, and Communications of the ACM, among others. He currently serves as Associate Editor for European Journal of Information Systems, Decision Sciences Journal, as well as serving on the Editorial Review Board for the Journal of the AIS. He is a founding member and current Chair of the IFIP Working Group on Information Systems Security Research (WG8.11/11.13). Dr. Johnston has also served as a consultant, visiting professor or invited speaker at several universities, workshops, panels, and companies in the U.S. and abroad, including as a Visiting Erskine Fellow at the University of Canterbury, Auburn University, Kennesaw State University, the University of Oulu, Mississippi State University, Nokia, Regions Financial Inc., the Birmingham, AL and Harrisburg, PA chapters of ISACA, and the Robert Wood Johnson Foundation New Careers in Nursing National Program Liaison's Summit (2011, 2013), among others. He is presently a Visiting Erskine Fellow at the University of Canterbury.