Malware Avoidance Motivations and Behaviors: A Technology Threat Avoidance Replication

Abstract

The current study presents a conceptual replication of Liang and Xue's (2010) test of their proposed Technology Threat Avoidance Theory (TTAT). Whereas the original study investigated individuals' spyware related threat perceptions, avoidance motivations, and behaviors; we applied the original study's research questions, hypotheses, and model to the more general context of malware. Results from a sample of 486 computer users revealed that safeguard effectiveness, safeguard cost, and self-efficacy are relatively robust predictors of avoidance motivation across varied settings. Perceived severity is a strong predictor of perceived threat, however the impact of this overall threat perception (along with its perceived susceptibility antecedent) may be less stable in predicting avoidance motivation under changing contextual/environmental circumstances. The results suggest that TTAT is a valid foundational framework for examining user behavior related to malicious software. Future research should investigate additional predictors of avoidance motivation such as risk propensity, distrust, and impulse control to improve the power of the model. Additionally, the current TTAT instrument offers several opportunities for enhanced measurement accuracy through item modifications, scale anchor revisions, and improvements in parsimony.

Keywords: technology threat avoidance theory, information security, malware, susceptibility, severity, safeguard cost, safeguard effectiveness, replication

Introduction

Research focused on understanding the antecedents of cyber security behaviors continues to draw attention in the Information Systems literature (Anderson & Agarwal, 2010; Boss, Galletta, Benjamin Lowry, Moody, & Polak, 2015; Chatterjee, Sarker, & Valacich, 2015; Johnston, Warkentin, & Siponen, 2015). Such research is important as prior studies have shown that insecure behaviors often contribute to security events (Sasse, Brostoff, & Weirich, 2001; Stantona, Stama, Mastrangelo, & Joiton, 2005; Workman, Bommer, & Straub, 2008). Accordingly, understanding the factors that influence individuals' security related behaviors may lead to technologies, policies, and procedures that effectively encourage individuals to behave more securely.

Liang and Xue (2010) proposed the Technology Threat Avoidance Theory (TTAT) to explain individuals' cyber security behaviors in terms of motivation to avoid threats. The theory argues that individuals weigh their susceptibility to and the severity of cyber threats against the effort necessary to implement safeguards in order to avoid the threats. The result of this calculus is a level of motivation needed to enact avoidance behaviors. A subsequent test of the theory in the context of anti-spyware software usage provided support for most of the theory's key proposals (Liang & Xue, 2010).

In the current study, we followed the conceptual replication definition found in Dennis and Valacich (2014) and replicated Liang and Xue's (2010) study using the same research questions

and hypotheses, slightly modified wording of measures, with a larger, more diverse sample of respondents. Accordingly, this paper makes several contributions to theory and practice. In terms of theory, the original study focused on individuals' spyware related threat perceptions and use of anti-spyware software to mitigate those threats. We altered the context of our study to focus on malware threat perceptions and use of anti-malware software to avoid such threats. We feel this is an important contribution, as spyware is just one of many types of malware that users must take actions to avoid. Today many anti-malware products protect against numerous types of security threats including spyware. Accordingly, testing the theory in this broader context provides support for applying the theory to more general threat avoidance technologies and processes.

Our results also support use of the theory to explain cyber security motivations and behaviors for a broad range of individuals. We included students from three institutions in our sample frame: one large public, research-oriented university with well-regarded cyber security programs; one large, public, doctoral granting higher research university; and one small, private Liberal Arts university. By including students from institutions with varied academic profiles, we broadened the diversity of the respondents and reduced the possibility of institution-based biases influencing our results. Additionally, our sample contained 486 usable responses, which provided a dataset large enough to detect even relatively small effect sizes (Cohen, 1992).

Finally, in terms of practice, our findings indicate that attempts to encourage more secure behavior should focus on: 1) emphasizing the effectiveness of threat avoidance safeguards, 2) nurturing individuals' beliefs regarding their ability to implement and use threat safeguards and 3) reducing individuals' perceptions concerning the level of effort needed to implement threat safeguards. Cyber security technology vendors and policy writers can use these findings to develop products, processes, and messages that effectively encourage more secure behavior.

The remainder of this paper is structured as follows. We begin with a short review of Liang and Xue's (2010) TTAT research model and hypotheses. We then describe our research method, data collection, and analysis processes, followed by a comparison of our results to Liang and Xue's (2010) results. Finally, we close with a discussion of the implications resulting from our study and suggestions for future research.

Research Model and Hypotheses

Drawing on Cybernetic and Coping theories, Liang and Xue (2009) proposed Technology Threat Avoidance Theory to explain users' cyber security motivations in terms of threat perceptions and coping ability. The theory posits that in a given context, an individuals' threat perception is formed based on their views regarding the severity associated with a given cyber threat and their own susceptibility to that threat. Individuals then appraise their ability to cope with a given threat based on: 1) how effective they believe a given safeguard is at helping them avoid the threat, 2) the overall effort cost of implementing the avoidance safeguard, and 3) their ability to implement the safeguard. The output of this appraisal process is a specific level of avoidance motivation which, in turn, influences the individual's decision to engage in behavior specifically intended to help them avoid the threat.

Liang and Xue (2010) tested their proposed theory in the context of anti-spyware software used to detect the presence of covert monitoring applications on a computer. A survey instrument was developed by incorporating or adapting items from pre-existing instruments for some constructs

with new item development for others. The initial set of items was vetted by a focus group though face-to-face interviews. The survey was then administered to 152 business students at a major US university. SmartPLS 2.0 was used to validate the instrument and test the nine hypotheses (Table 1). Support was found for all hypotheses except an interactive effect of perceived severity and perceived susceptibility on threat perceptions (H1c). Liang and Xue's (2010) TTAT research model and results are presented in Figure 1.

Table 1: Liang and Xue's (2010) Hypotheses

Hypothesis	Text	Result
H1a	Perceived susceptibility of being attacked by malicious IT positively affects perceived threat.	Supported
H1b	Perceived severity of being attacked by malicious IT positively affects perceived threat.	Supported
H1c	Perceived susceptibility and perceived severity have a positive interaction effect on perceived threat.	Not Supported
H2	Perceived threat positively affects avoidance motivation.	Supported
H3	Safeguard effectiveness positively affects avoidance motivation.	Supported
H3a	Perceived threat and safeguard effectiveness have a negative interaction effect on avoidance motivation.	Supported
H4	Safeguard cost negatively affects avoidance motivation.	Supported
H5	Self-efficacy positively affects avoidance motivation.	Supported
H6	Avoidance motivation positively affects the avoidance behavior of using the safeguard.	Supported

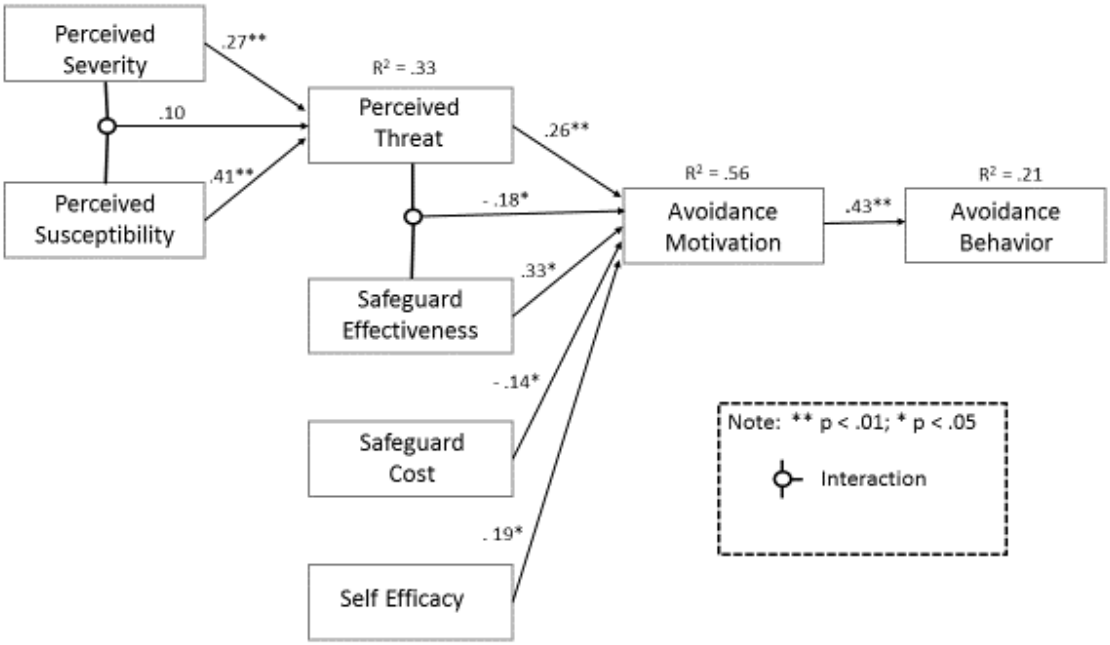

Figure 1: Technology Threat Avoidance Model reproduced from Liang and Xue (2010)

There have been several important considerations of Technology Threat Avoidance Theory since Liang and Xue first tested their theory. Arachchilage and Love (2013) incorporated TTAT in their examination of game based education as a safeguard against phishing attacks. Their results indicate support for TTAT and even found significant results for the interaction between Perceived Severity and Perceived Susceptibility where Liang and Xue (2010) found no significance. Subsequently, Arachchilage and Love (2014) modified TTAT to study the effects of Procedural Knowledge and Conceptual Knowledge as antecedents to Self-Efficacy excluding threat appraisal and other portions of the coping appraisal as conceived in TTAT. While results were significant, the R^2 value for Avoidance Motivation was .29 and Avoidance Behavior was .33. This reduction in explanatory power indicates further work is needed in determining antecedents to the Avoidance Behavior construct.

In a coping perspective study by Lai, Li and Hsieh (2012), a modified TTAT model was incorporated. This work looked at identity theft and the effects of Conventional Coping and Technological Coping on an individual's avoidance behaviors. While this work found significance for these constructs, factor loadings for Identity Theft Avoidance Behavior were low (.21 to .61) and the AVE for Conventional Coping and Technological Coping were also low (.54 and .66). It is important to note that Lai et al (2012) did also test Social Influence as an antecedent to coping and this construct demonstrated good reliability and validity.

Finally, Herath et al. (2014) consolidated Technology Acceptance, Technology Threat Avoidance and Protection Motivation Theories to explore how threat appraisal, internal coping mechanism appraisal, external coping mechanism appraisal influence coping motivation. Results indicate significant effects for email authentication service as a coping mechanism to deal with email threats.

Though the application of TTAT across these studies varied in context and conceptualization, all demonstrate the value of Technology Threat Avoidance Theory as a tool for exploring threat appraisal, coping mechanisms and threat avoidance behavior. Because of the inconsistent results when using modified models, we chose to test the original Liang and Xue's (2010) TTAT research model and hypotheses in our replication study. The following section outlines the details of our research method.

Methodology

We used an online survey instrument to collect data for the replication study. The instrument contained five blocks of indicators to assess the latent constructs included in the TTAT model. The first block of indicators measured beliefs regarding malware susceptibility as well as beliefs concerning the severity of the consequences resulting from a malware breach. The second block of indicators assessed beliefs concerning: 1) the level of threat associated with a malware breach, 2) the effectiveness of anti-malware software at protecting against such breaches, and 3) the effort cost associated with implementing and using an anti-malware application. The third block of indicators measured self-efficacy or the user's perception of their ability to effectively install and use anti-malware software. The fourth block of indicators assessed individuals' motivation to avoid malware breaches and their self-reported behavior toward that objective. The survey concluded with several demographic questions. Within blocks, all indicators were randomized to protect against ordering effects (Shadish, Cook, & Campbel, 2002).

Business students at three universities were invited to participate in the study. We used business students as surrogates for the more general population of technology users. Consistent with the recommendations of Compeau et al. (2012), we note that while most business students are avid technology users, it is important to acknowledge that they are typically younger and more technologically savvy than the population as a whole. Additionally, we note that this is a purposeful replication of a previous study that used students as its sample, so the use of consistent samples enhances the comparability of the findings between the studies.

At a large, public university, 60 students in an upper-division undergraduate Health Information Management course were asked to participate with no incentives offered for participation. Forty-five students completed the survey for a 75% response rate. At a small, private Liberal Arts university, students in 15 upper-division undergraduate business courses with a total enrollment of 393 students were asked to participate in exchange for nominal extra credit points. Some students were enrolled in two or more of the classes included in the sample frame. Those students were allowed to collect extra credit points in multiple classes but were instructed to only complete the survey a single time. One hundred ninety-six (196) of the invited students completed the survey. Internal Review Board anonymity requirements precluded tracking the identities of the responding students. Accordingly, we cannot calculate an exact response rate, but provide a highly conservative estimate of 49.8% (196 responses / 393 total students enrolled in the 15 classes) for this institution. We used 393 as the denominator in our response rate calculation as it assumes the largest potential subject pool with no duplicate enrollments and thus provides the lowest potential response rate. Finally, 471 students in two sections of a freshman-level undergraduate business course at a large, public research-oriented university were invited to participate in exchange for nominal extra credit points. Two hundred seventy-one (271) of those student completed the survey for a response rate of 57.5%.

Table 2 provides a demographic comparison of the Liang and Xue's (2010) sample and the samples we collected from the three universities. Respondents in our samples included students majoring in business, health information management, and undeclared majors. The original sample used by the Liang and Xue (2010) sample included only business majors. The Sample A respondents were similar in age and gender to the Liang and Xue respondents. In contrast, the Sample B respondents were younger, while the Sample C respondents were considerable older. A key difference between the three samples we collected was life state of the respondents. The Sample B respondents were mostly unmarried, childless, and did not work full-time. In contrast, 10% of the Sample A respondents were married and had children and 25% worked full-time. Finally, nearly half of the Sample C respondents worked full time, while a significant number were married and had children.

Table 2: Sample Demographics

Characteristic	Liang & Xue (2010) Sample	Sample A	Sample B	Sample C
Size	152	271	196	45
Institution Profile	Major U.S. University	Large public University	Small, private Liberal Arts University	Large public University
Academic Majors	Business	Business and Undeclared Majors	Business Majors	Health Information Management Majors
Student Level	Unknown	Freshman	Upper-division undergraduate	Upper-division undergraduate
Mean Age	23	22	20	31
Race	Unknown	47% Hispanic 35% White 10% Asian	50% White 27% Hispanic 16% Asian	42% White 28% Hispanic 20% Black
Gender Split	66% male	57% Male	59% Male	15% Male
Married	Unknown	9%	3.50%	40%
Have Children	Unknown	10%	3%	36%
Work Full Time	Unknown	25%	3.50%	44%

During the analysis phase of the project, the three samples were combined and 26 invalid or incomplete responses were identified. Accordingly, these responses were eliminated from the merged sample, leaving 486 complete and usable responses for analysis. Of the remaining responses in the merged sample, the average respondent age was 22.3 (SD = 5.33) and 54.4% were male. In terms of race, 8% of respondents identified as Black or African American, 13% as Asian, 37% as Hispanic, 2% as Native American, and 41% as White. Slightly less than 10% of respondents identified as married, 10% had children, and 18.3% indicated that they worked full-time.

Measurement of Constructs

Measures for the study were drawn from Liang and Xue (2010). All indicators were modified to fit the malware context. Wording of some indicators was revised slightly to improve clarity. Additionally, two of the original perceived susceptibility indicators were merged into a single indicator as their wording was nearly identical except that one focused on present perceptions of threat susceptibility and one focused on perceptions of future threat susceptibility. We felt that it was inappropriate to include perceptions of future susceptibility in an assessment of current avoidance motivation and behavior because no time frame was specified between this future susceptibility and the associated avoidance motivation or behavior actions. For example, a subject perceiving that her threat susceptibility might be great five years from now will likely not be motivated to take any action to avoid that threat now. Appendix A provides a comparison of the indicators used in the current study and the original Liang and Xue indicators.

Scale anchors for the perceived severity indicators were modified from the seven-point sematic differential descriptors used by Liang and Xue to seven-point Likert scale descriptors consistent with other scales on the instrument. Additionally, indicators to measure self-efficacy were rescaled from a ten-point Likert scale to a seven-point Likert scale. We made these changes so that all indicators were consistently measured using a seven-point Likert scale that was anchored in ascending order with the phrases strongly disagree, disagree, somewhat disagree, neutral, somewhat agree, agree, strongly agree. The final instrument contained four indicators to assess perceived susceptibility, ten indicators to assess perceived severity, five indicators to assess perceived threat, six indicators to assess perceived safeguard effectiveness, three indicators to assess safeguard cost, ten indicators to assess self-efficacy, two indicators to assess avoidance motivation, and two indicators to assess avoidance behavior.

Data Analysis and Results

The collected data were analyzed using the R language statistics package plspm, a partial least squares (PLS) approach for studying the linear relationships that exist between blocks of latent variables. PLS is a powerful method for analyzing complex models that contain related latent constructs. Additionally, the method has been shown to work well with both interval and ratio scales while making minimal demands on sample size and residual distributions (Chin, 1998).

Measurement Validation

We began the analysis process by first standardizing all data values. Next, we modeled all items as reflective indicators of the hypothesized latent constructs (Sanchez, 2013) and assessed the convergent and discriminate validity of the TTAT model using two procedures. First, for each indicator, the exploratory factor analysis loadings were inspected to ensure that they were higher

for the hypothesized construct than all other latent constructs. Next, for each indicator, the square root of the average variance extract (AVE) was checked to ensure that it was higher than the construct's correlations with any other construct (Fornell & Larcker, 1981). Initial results indicated that a small number of individual items loaded poorly on their hypothesized constructs. These included a single perceived severity indicator SEV7, as well as self-efficacy indicators SLF1, SLF2, SLF3, and SLF8. Both the perceived severity scale and the self-efficacy scale had large item pools and thus provided high internal consistency and high scale reliability without the poorly loading items. Accordingly, those indicators were removed from the model and the analysis was re-run.

Subsequent results provided support for the convergent and discriminate validity of the measurement model. As can be seen in Appendix B, all indicators loaded higher on their hypothesized constructs than on all other constructs. Additionally, each construct's square root of AVE was higher than its correlation with all other constructs as can be seen in Table 3. Next, to ensure the measures were reliable as well as valid, we calculated the composite reliability of each latent construct. All reliability coefficients exceeded the recommended .70 threshold suggested by Nunnally (1978) indicating an acceptable level of reliability also existed in the measurement model.

Table 3: Correlation matrix and AVEs for constructs

Constructs	R	AVE	1	2	3	4	5	6	7	8
Perceived Susceptibility	.936	.702	.838							
Perceived Severity	.860	.662	.389	.814						
Perceived Threat	.836	.603	.285	.618	.777					
Safeguard Effectiveness	.915	.701	.191	.585	.661	.837				
Safeguard Cost	.881	.807	.105	-.198	-.071	-.207	.898			
Self-efficacy	.875	.609	.136	.324	.268	.336	-.059	.780		
Avoidance Motivation	.908	.854	.127	.376	.368	.494	-.378	.256	.924	
Avoidance Behavior	.854	.872	.023	.272	.244	.370	-.308	.195	.753	.934

Note: The diagonal elements represent square roots of AVE

We followed the Liang and Xue (2010) methods for testing for the presence of common method variance. Since the publication of the original test of TTAT, the first method, Harman's (1976) single factor test has been criticized as not being a sufficiently robust procedure for detecting common method bias (Chin, Thatcher, & Wright, 2012; Podsakoff, MacKenzie, & Podsakoff, 2012; Sharma, Yetton, & Crawford, 2009); however, we felt that to be true to Liang and Xue's

work we should perform the test in the same manner. Therefore, we used two techniques to test for the presence of common method variance in our collected data. First, we conducted Harman's (1976) single factor test, which calls for factor analyzing all indicators and constraining the results to a single factor, un-rotated solution. If the resulting factor accounts for more than 50% of the variance in the data, large common method variance could be present in the data. The test revealed that a single-factor solution only accounted for 29% of the variance in the data. Further, inspection of both eigenvalues and the scree plot resulting from an unconstrained factor solution indicated that eight distinct factors existed and accounted for 68% of the variance in the data. Accordingly, the Harman test did not indicate that common method variance was of concern for the replication data.

Next, we applied Podsakoff et al.'s (2003) unmeasured latent method factor technique, which calls for comparing the results of the hypothesized factor model to the results of a revised model that includes a common method latent construct. In the revised model, all indicators are modeled to load on both their theorized construct and the common method construct. Accordingly, the revised model partitions each indicator's variance into three components representing the hypothesized construct, the method construct, and error.

To conduct this test, we used AMOS to estimate a confirmatory factor analysis model that included only the hypothesized latent constructs and their reflective indicators. The results of that model were compared to the estimate of an updated model that included a common method latent construct. Standardized regression weights and Chi squared values for the two models were compared. No significant differences were found suggesting that common method variance was unlikely to be of concern for our data.

TTAT Model Testing

Figure 2 shows that for the replication study, the TTAT model accounted for 39% of the variance in perceived threat, 34% of the variance in avoidance motivation, and 57% of the variance in avoidance behavior. Compared to the original study, the replication data provided a six percent increase in explanatory value for perceived threat (R^2 = .39 compared to R^2 = .33), a 22% decrease in explanatory value for avoidance motivation (R^2 = .34 compared to R^2 = .56), and a 36% increase in explanatory value for avoidance behavior (R^2 = .57 compared to R^2 = .21).

In the replication study, the influence of perceived severity on perceived threat was significant (β = .59, p < .001) providing strong support for H1b. However, neither perceived susceptibility nor the interactive effect of perceived severity and perceived susceptibility were found to be significantly related to perceived threat in the replication study. Accordingly, neither H1a nor H1c were supported.

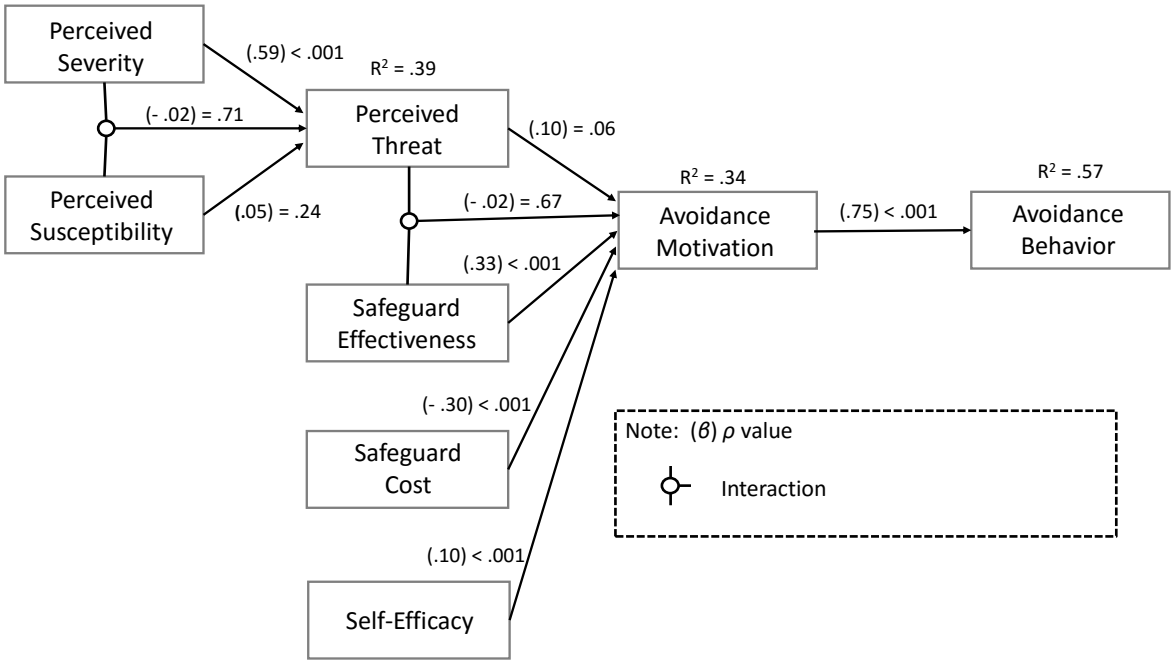

Figure 2: TTAT Model Replication Results

While Liang and Xue (2010) report similar findings in regards to the interaction term, they did find a significant association between perceived susceptibility and perceived threat (β = .41 p < .01). In fact, for the original study respondents, the influence of perceived susceptibility on perceived threat was greater than the influence of perceived severity (β = .41 compared to β = .27) on perceived threat. In the replication study, the influence of perceived susceptibility was both weak and non-significant (β = .05, p = .24) while the influence of perceived severity was strong and highly significant (β = .59, p < .001). Accordingly, the Liang and Xue (2010) respondents associated their susceptibility to spyware as more threatening than the replication study respondents associated their susceptibility to malware. In addition, the TTAT respondents' threat perceptions were more heavily influenced by their susceptibility to spyware than by the severity of the consequences resulting from a spyware inflection. In comparison, the replication study respondents did not associate a high level of threat with their susceptibility to a malware breach but did consider the severity of the consequences resulting from a malware breach to be highly threatening.

In regard to the antecedents of avoidance motivation, in the replication study, the influence of perceived threat on avoidance motivation was relatively small and marginally significant (β = .10, p = .058) providing weak support for H2. This finding is quite different from the moderately sized, significant influence found for perceived threat on avoidance motivation in the original study (β = .26, p < .01). In addition, the interactive effect of perceived threat and safeguard effectiveness on avoidance motivation was not significant in the replication study. Accordingly, support was not found for H3a. This deviates from the results of the original study in which the interaction term was found to be both significantly and negatively associated with avoidance motivation (β = -.18, p < .05). One potential explanation for this contrary finding may have been the relatively high threat perceptions (mean = 5.5, variance = 1.09, standard deviation = 1.04)

and safeguard effectiveness perceptions (mean = 5.6, variance = 1.02, standard deviation = 1.01) reported by our respondents on the 7 point Likert scale instrument. Mean and dispersion characteristics were not reported in the original study so we cannot compare them directly. However, we posit that the high means and relatively low dispersion for both variables in our study may make it difficult to detect the hypothesized interaction effect. We also note that the original Liang and Xue (2010) study only found a small to medium size effect of the interaction term which could further exacerbate any issues associated with low dispersion characteristics in our sample.

Replication results concerning safeguard effectiveness, safeguard cost, and self-efficacy were very similar to those found in the original study, providing strong support for H3, H4, and H5. In the replication study, safeguard effectiveness was found to significantly and positively influence avoidance motivation ($\beta = .33$, $p < .001$), which is very close to the results reported ($\beta = .33$, $p < .01$) in the original study. Safeguard cost was found to significantly and negatively influence avoidance motivation ($\beta = -.30$, $p < .001$), a stronger and more significant result than was found in the original study ($\beta = -.14$, $p < .05$). Finally, self-efficacy was found to significantly and positively influence avoidance motivation ($\beta = .10$, $p < .001$). This is similar to Liang and Xue's results ($\beta = .19$, $p < .05$), however, we caution against comparing the two study's beta coefficients for this variable as the measurement scale was changed for the replication study from a 10 point sematic differential to a 7 point Likert scale.

As neither of the interaction terms hypothesized in TTAT were significant when tested with the replication data, we removed them from the model to see if the change improved the significance of the perceived threat on avoidance motivation association.

Figure 3 shows the results of the test. With the interaction terms removed, perceived threat had a modest significant effect on avoidance motivation ($\beta = .10$, $p = .05$), while the relationship was nominally weaker ($\beta = .10$, $p = .06$) with the interaction term included. Thus we conclude that neither of the interaction terms substantially changed the relationship between perceived threat and avoidance motivation.

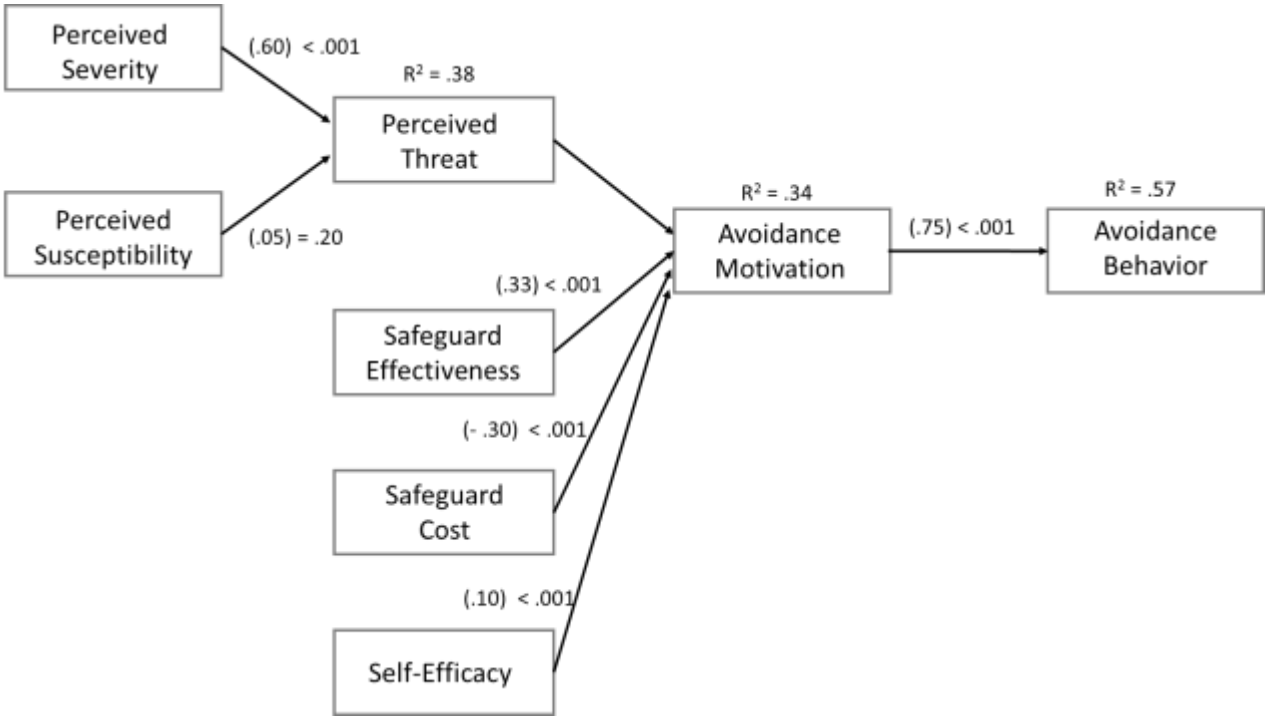

Figure 3: TTAT Model Replication Results - Interaction Terms Removed

Our replication results provide strong support for a significant association between avoidance motivation and avoidance behavior (β =.75, p < .001), which is similar to the results reported by Liang and Xue (2010) (β = .43, p < .05). Accordingly, support was found for H6. Table 4 summarizes our hypotheses results and compares our findings to those reported in TTAT.

Table 4: Hypotheses Results and Comparison

Hypothesis	Text	Replication Results	Liang & Xue (2010) Results
H1a	Perceived susceptibility of being attacked by malicious IT positively affects perceived threat.	Not Supported	Supported
H1b	Perceived severity of being attacked by malicious IT positively affects perceived threat.	Supported	Supported
H1c	Perceived susceptibility and perceived severity have a positive interaction effect on perceived threat.	Not Supported	Not Supported
H2	Perceived threat positively affects avoidance motivation.	Supported	Supported
H3	Safeguard effectiveness positively affects avoidance motivation	Supported	Supported
H3a	Perceived threat and safeguard effectiveness have a negative interaction effect on avoidance motivation.	Not Supported	Supported
H4	Safeguard cost negatively affects avoidance motivation.	Supported	Supported

H5	Self-efficacy positively affects avoidance motivation.	Supported	Supported
H6	Avoidance motivation positively affects the avoidance behavior of using the safeguard.	Supported	Supported

Discussion

While our findings largely mirrored those reported by Liang and Xue (2010), there were a few notable differences. First, perceived susceptibility was not a significant predictor of perceived threat. This contrary finding may be due to the increasing proliferation of malicious code that has occurred in the years since the original study. As noted in the original Liang and Xue (2010) article, the concept of spyware was relatively new and poorly understood at the time of their study. Malware of all types has grown substantially more pervasive and users have gained a much greater sense of their overall vulnerability to malevolent attacks. Thus it is likely that perceptions of general susceptibility to malware and/or spyware have increased over time, to the point where susceptibility is almost a given. This may lead respondents to place more emphasis on perceived severity when evaluating their overall perception of the threat in the current operating environment. We note that perceived severity was a stronger predictor of perceived threat in our study as compared to the original findings. Despite the divergent nature of these findings, the combined power of perceived severity and perceived susceptibility to predict perceived threat was relatively equal in both studies. A second notable difference in our findings was that perceived threat was, at best, a modestly significant predictor of avoidance motivation in our study, while this relationship was highly significant in the Liang and Xue (2010) study. Conversely, safeguard effectiveness, safeguard cost, and self-efficacy were all stronger predictors of avoidance motivation in our study, but the total percentage of avoidance motivation predicted was somewhat lower. Even though our ability to predict avoidance motivation was somewhat lower than the original study, we ultimately accounted for a substantially larger percentage of the variance in avoidance behavior. This phenomenon is more fully discussed under the directions for future research below.

Another interesting point of discussion was our consistent finding regarding the lack of a significant interaction effect between perceived severity and perceived susceptibility. While Liang and Xue (2009) provide a well-reasoned theoretical basis for expecting this interaction effect, it was not significant in the original study nor in our replication. One potential explanation for these findings may be underlying differences in threat perceptions between the technology threat domain and the referent domains which serve as the theoretical basis for this hypothesized interaction. In the organizational risk analysis domain, susceptibility to a threat is based on actuarial or quasi-actuarial projections, while the cost of damage is often based on previous event data. Similarly, in the healthcare domain, susceptibility is estimated based on known correlated factors such as lifestyle choices, proximity to risk vectors, and presence of related disease while perceived severity is based on previous patient data. In the technology threat domain, both perceived susceptibility estimates and perceived severity estimates are less likely to be based on historical data and much more likely to be influenced by emotion and socially derived perceptions. Quite simply, the types of highly structured and robust analytical processes that inform the organizational risk analysis and healthcare risk domains are less likely to be present when individual IT users are making a technology threat assessment. As carefully noted in Liang and Xue's (2009) original conceptual development, different individuals perceive the same threat

differently in terms of both severity and susceptibility due to subjective personal frames of reference. Thus, we contend that any observed significant interaction between perceived susceptibility and perceived severity in the personal technology threat domain is potentially a spurious finding in the absence of consistent data that drives those user perceptions.

Limitations and Directions for Future Research

An important limitation of our research is the use of university students as subjects in a manner similar to the original Liang and Xue (2010) study. Although a strong case can be made that university students are an appropriate subject pool for examining the phenomena of interest, care should be exercised in generalizing the results to other groups of computer users. We have carefully considered a variety of recommendations regarding generalizations using student samples (Compeau et al., 2012) and feel that the findings presented here can be reasonably construed to apply to a more general population of technology users. The university students used in our sample are, in fact, a key component of the broader technology user population. Although they tend to be younger, more frequent technology users, and more technology savvy than the population as a whole, they appear particularly well positioned to provide insights on technology threat avoidance behavior. They are similar to the general population in terms of using technology for a myriad of purposes, having to assess potential threats to their technology usage, and having to make assumptions about the cost and efficacy of protective measures. Thus, they are well-positioned to provide opinions representative of the broader population.

Another potential limitation of our study is that, in the course of our replication, we noted some potentially problematic items and scale anchors in the Liang and Xue (2010) instrument. We modified the scale anchors in our study but resisted substantially modifying the item wording as we felt it would have a negative impact on the replication quality. This brings us to our first suggestion for future research.

The Liang and Xue (2010) instrument presents several opportunities for improvement through item revisions and improved scale anchors. Liang and Xue (2010) incorporated several pre-existing scales from other domains. Some of these scales were originally semantic differential scales that were converted to Likert scales but the semantic differential anchors were retained. Consider the following example item: "Spyware would invade my privacy" where subjects were asked to rate perceived severity on a scale with anchors of 1=innocuous and 7=extremely devastating. It is apparent that revised anchors such as 1=strongly disagree and 7=strongly agree would present a clearer logical choice to the respondent. Additionally, several individual items on the original Liang and Xue (2010) instrument incorporate multiple disparate constructs, thus making the meaning of the respondent's answer unclear. Consider the following item: "I don't have anti-spyware on my PC because I don't know how to get an anti-spyware software". A respondent may interpret this item several ways such as "Strongly Disagree – I don't have it because it costs too much (rather than I don't know how to get it)" or "Strongly Disagree – I do have anti-spyware on my system". We believe a more robust and potentially more parsimonious instrument can be derived through careful item examination and additional instrument validation measures. In terms of parsimony, we believe most scales in the instrument can be reduced to approximately four item scales without substantial loss of reliability and such an improvement would significantly enhance the utility of the instrument. Therefore we believe any future research considering Technology Threat Avoidance Theory should incorporate efforts to improve these scale weaknesses.

A second direction for future research arises from our finding that the model's ability to predict avoidance behavior was better than its ability to predict avoidance motivation in the replication effort. Since motivation is often characterized as a direct antecedent of behavior, this finding suggests that some significant predictors of motivation are missing from the model. We urge future research that evaluates the impact of additional constructs supported as predictors of motivation in other cyber security contexts such as risk propensity (Chen, Wang, Herath, & Rao, 2011; Chung & Galletta, 2013) distrust, (Ho & Chau, 2013; Westin, 2003) and impulse control (Hu, West, & Smarandescu, 2015; Li, Sarathy, Zhang, & Luo, 2014).

Another potential research opportunity related to TTAT is the influence of risk tolerance and social factors. Works in this area would support Liang and Xue's (2009) conceptualization of risk tolerance impacting an individual's threat appraisal which remains untested. Liang and Xue (2009) also suggested a general relationship between social factors and the TTAT model. One research opportunity would be to determine whether social influences relate to an individual's threat appraisal, coping appraisal or coping. In addition, future researchers should consider which social influences are important – information influences or normative influences. Liang and Xue (2009) believe that informational influence is medicated by threat and coping appraisals and that normative social influence may have a direct effect. Both theoretical influences remain untested with one notable exception. Lai et al. (2012) looked at social influence as an antecedent to technological coping. Future research should begin to examine which social influences might impact technology threat avoidance.

Conclusions

Our study largely validates the usefulness and efficacy of the Technology Threat Avoidance Theory model through a conceptual replication examining predictors of avoidance motivation and avoidance behavior. The slight contextual change in the extant study, coupled with changes in the technology threat environment over time, highlight opportunities for continued refinements to the theoretical underpinnings of the model. While our research shows that safeguard effectiveness, safeguard cost, and self-efficacy are relatively robust predictors of avoidance motivation across varied settings, the impact of perceived threat (including its perceived susceptibility antecedent) may be less stable under changing contextual/environmental circumstances.

References

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613–A15.

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, *29*(3), 706–714.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. http://doi.org/10.1016/j.chb.2014.05.046

Boss, S. R., Galletta, D. F., Benjamin Lowry, P., Moody, G. D., & 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.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use. *Journal of Management Information Systems*, *31*(4), 49–87.

Chen, R., Wang, J., Herath, T., & Rao, H. R. (2011). An investigation of email processing from a risky decision making perspective. *Decision Support Systems*, *52*(1), 73–81.

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

Chin, W. W., Thatcher, J. B., & Wright, R. T. (2012). Assessing Common Method Bias: Problems with the Ulmc Technique. *MIS Quarterly*, *36*(3), 1003–A11.

Chung, R., & Galletta, D. F. (2013). Genetic Basis of Behavioral Security. In *Proceedings of the Twelfth Annual Workshop on HCI Research in MIS, Milan, Italy, December* (Vol. 15).

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155.

Compeau, D., Marcolin, B., Kelley, H., & Higgins, C. (2012). Research commentary-generalizability of information systems research using student subjects-a reflection on our practices and recommendations for future research. *Information Systems Research*, *23*(4), 1093–1109.

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

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research (JMR)*, *18*(1), 39–50.

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

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information Systems Journal*, *24*(1), 61–84. http://doi.org/10.1111/j.1365-2575.2012.00420.x

Ho, S. Y., & Chau, P. Y. K. (2013). The Effects of Location Personalization on Integrity Trust and Integrity Distrust in Mobile Merchants. *International Journal of Electronic Commerce*, *17*(4), 39–72. http://doi.org/10.2753/JEC1086-4415170402

Hu, Q., West, R., & Smarandescu, L. (2015). The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective. *Journal of Management Information Systems*, *31*(4), 6–48.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113–A7.

Lai, F., Li, D., & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52*(2), 353–363. http://doi.org/10.1016/j.dss.2011.09.002

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly*, *33*(1), 71–90.

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413.

Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, *24*(6), 479–502.

Nunnally, J. (1978). *Psychometric Theory* (2nds ed.). New York: McGraw-Hill.

Podsakoff, P. M., MacKenzie, S. B., Jeong-Yeon Lee, & Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology*, *88*(5), 879.

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of Method Bias in Social Science Research and Recommendations on How to Control It. *Annual Review of Psychology*, *63*(1), 539–569. http://doi.org/10.1146/annurev-psych-120710-100452

Sanchez, G. (2013). *PLS Path Modeling with R*. Gaston Sanchez.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "Weakest Link": a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, *19*(3), 122–131.

Shadish, W. R., Cook, T. D., & Campbel, D. T. (2002). *Experimental and Quasi-Experimental Designs for Generalized Casual Inference*. Boston: Houghton Mifflin Company.

Sharma, R., Yetton, P., & Crawford, J. (2009). Estimating the Effect of Common Method Variance: The Method--Method Pair Technique with an Illustration from Tam Research. *MIS Quarterly*, *33*(3), 473–A13.

Stantona, J. M., Stama, K. R., Mastrangelo, P., & Joiton, J. (2005). Analysis of end user security be haviors. *Computers & Security*, *24*(2), 124–133.

Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, *59*(2), 431–453. http://doi.org/10.1111/1540-4560.00072

Workman, M., Bommer, W., & Straub, D. (2008). Secuirty Lapses and the Omission of Information Security Measures: An Empirical Test of the Threat Control Model. *Journal of Computers in Human Behavior*, *24*(6), 2799–2816.

Appendix A

Construct	Indicator	Indicator Text	Liang and Xue (2009) Text
Perceived Susceptibility	SUS1	It is extremely likely that my computer will contain malware in the future.	It is extremely likely that my computer will **be infected by spyware** in the future.
	SUS2	The chances of getting malware on my system are great.	**My** chances of getting **spyware** are great.
	SUS3	There is a good possibility that my computer will contain malware at some point.	There is a good possibility that my computer will **have spyware**.
	SUS4	There is a good chance that there will be malware on my computer at some point in the future.	It is extremely likely that spyware will infect my computer
			I feel spyware will infect my computer in the future
Perceived Severity	SEV1	Malware could steal personal information from my computer without my knowledge.	**Spyware would** steal personal information from my computer without my knowledge
	SEV2	Malware could invade my privacy.	**Spyware would** invade my privacy
	SEV3	My personal information collected by malware could be misused by cyber criminals.	My personal information collected by spyware **would** be misused by cyber criminals.
	SEV4	Malware could record my Internet activities and send it to unknown parties.	**Spyware** could record my Internet activities and send it to unknown parties.
	SEV5	My personal information collected by malware could be subjected to unauthorized secondary use.	My personal information collected by **spyware** could be subjected to unauthorized secondary use.
	SEV6	My personal information collected by malware could be used to commit crimes against me.	My personal information collected by **spyware** could be used to commit crimes against me.

	SEV7 [1]	Malware could slow down my Internet connection.	**Spyware would** slow down my Internet connection.
	SEV8	Malware could make my computer run more slowly.	**Spyware would** make my computer run more slowly.
	SEV9	Malware could cause my systems to crash from time to time.	**Spyware would** cause my systems to crash from time to time.
	SEV10	Malware could affect some of my computer programs and make them difficult to use.	**Spyware would** affect some of my computer programs and make them difficult to use.
Perceived Threat	THR1	Malware poses a threat to me.	**Spyware** poses a threat to me.
	THR2	The consequences of getting malware on my computer threaten me.	The trouble cause by spyware threatens me.
	THR3	Malware is a danger to my computer.	**Spyware** is a danger to my computer.
	THR4	It would be dreadful if my computer was infected by malware.	It **is** dreadful if my computer **is** infected by spyware.
	THR5	It would be risky to use my computer if it had malware.	It **is** risky to use my computer if it **has** spyware.
Perceived Effectiveness	EFF1	Computer security software would be useful for detecting and removing malware.	**Anti-spyware** software would be useful for detecting and removing spyware.
	EFF2	Computer security software would increase my ability to protect my computer from malware.	**Anti-spyware** software would increase my performance in protecting my computer from spyware.
	EFF3	Computer security software would enable me to search and remove malware on my computer faster.	**Anti-spyware** software would enable me to search and remove malware on my computer faster.

[1] Indicator not included in data analysis due to poor loading on focal construct

	EFF4	Computer security software would enhance my effectiveness in finding and removing malware on my computer.	**Anti-spyware** software would enhance my effectiveness in finding and removing malware on my computer.
	EFF5	Computer security software would make it easier to search for and removed malware on my computer.	**Anti-spyware** software would make it easier to search for and removed malware on my computer.
	EFF6	Computer security software would increase my productivity in searching and removing malware on my computer.	**Anti-spyware** software would increase my productivity in searching and removing malware on my computer.
Safeguard Cost	CST1	I don't have security software on my computer because I don't know how to get it.	I don't have anti-spyware software on my computer because I don't know how to get **an anti-spyware software.**
	CST2	I don't have security software on my computer because it may cause problems with other programs on my computer	I don't have anti-spyware software on my computer because **anti-spyware software** may cause problems to other programs on my computer
	CST3	I don't have security software on my computer because installing it is too much trouble.	I don't have anti-spyware software on my computer because installing **anti-spyware software** is too much trouble.
Self-Efficacy	SLF1 [1]	I could successfully install and use computer security software if....There was no one around to tell me what to do.	I could successfully install and use **anti-spyware** software if....There was no one around to tell me what to do.
	SLF2 [1]	I could successfully install and use computer security software if....I had never used a package like it before.	I could successfully install and use **anti-spyware** software if....I had never used a package like it before.
	SLF3 [1]	I could successfully install and use computer security software if....I only had the software manuals for reference.	I could successfully install and use **anti-spyware** software if....I only had the software manuals for reference.

	SLF4	I could successfully install and use computer security software if....I had seen someone else do it before trying myself.	I could successfully install and use **anti-spyware** software if....I had seen someone else do it before trying myself.
	SLF5	I could successfully install and use computer security software if....I could call someone for help if I got stuck.	I could successfully install and use **anti-spyware** software if....I could call someone for help if I got stuck.
	SLF6	I could successfully install and use computer security software if....Someone helped me get started.	I could successfully install and use **anti-spyware** software if....Someone **else** helped me get started.
	SLF7	I could successfully install and use computer security software if....I had a lot of time to complete the task.	I could successfully install and use **anti-spyware** software if....I had a lot of time to complete the **job**.
	SLF8 [1]	I could successfully install and use computer security software if....I only had the built-in help facility for assistance.	I could successfully install and use **anti-spyware** software if....I had **just** the built-in help facility for assistance.
	SLF9	I could successfully install and use computer security software if....Someone showed me how to do it first.	I could successfully install and use **anti-spyware** software if....Someone showed me how to do it first.
	SLF10	I could successfully install and use computer security software if....I had used a similar package before.	I could successfully install and use anti-spyware software if....I had used similar packages like this one before to do the job.
Avoidance Motivation	MOT1	I intend to use computer security software to avoid malware breaches.	I intend to use **anti-spyware** software to avoid **spyware**.
	MOT2	I use computer security software to avoid malware breaches.	I **plan** to use **anti-spyware** software to avoid **spyware**.
	MOT3	I plan to use computer security software to avoid malware.	I predict I would use anti-spyware software to avoid spyware.

Avoidance Behavior	BEH1	I run computer security software regularly to remove malware from my computer.	I run **anti-spyware** software regularly to remove spyware from my computer.
	BEH2	I update my computer security software regularly.	I update my **anti-spyware** software regularly.

Appendix B. Cross Loadings of Construct Indicators

Indicators	Mean	S.D.	SEV	SUS	THR	EFF	COS	SLF	MOT	BEH
SEV1	5.73	1.348	0.85	0.33	0.52	0.47	-0.15	0.29	0.30	0.21
SEV2	5.88	1.272	0.88	0.31	0.58	0.55	-0.15	0.31	0.34	0.22
SEV3	5.74	1.275	0.84	0.30	0.53	0.50	-0.16	0.30	0.34	0.26
SEV4	5.69	1.345	0.80	0.32	0.49	0.49	-0.17	0.24	0.30	0.26
SEV5	5.71	1.327	0.87	0.33	0.50	0.50	-0.21	0.32	0.31	0.23
SEV6	5.40	1.466	0.71	0.31	0.46	0.39	-0.09	0.21	0.25	0.20
SEV8	5.87	1.255	0.81	0.31	0.46	0.48	-0.16	0.20	0.27	0.16
SEV9	5.61	1.304	0.78	0.35	0.49	0.45	-0.14	0.20	0.28	0.20
SEV10	5.71	1.297	0.78	0.29	0.48	0.46	-0.23	0.27	0.35	0.23
SUS1	4.59	1.561	0.24	0.84	0.18	0.10	0.13	0.09	0.06	0.00
SUS2	4.37	1.609	0.25	0.77	0.21	0.14	0.13	0.10	0.10	0.01
SUS3	5.07	1.502	0.39	0.86	0.24	0.20	0.03	0.13	0.11	0.02
SUS4	4.99	1.473	0.39	0.88	0.30	0.18	0.08	0.13	0.13	0.04
THR1	5.26	1.395	0.47	0.35	0.81	0.52	-0.02	0.19	0.26	0.19
THR2	5.28	1.325	0.43	0.21	0.80	0.50	0.04	0.19	0.26	0.18
THR3	5.69	1.300	0.56	0.24	0.78	0.52	-0.11	0.28	0.36	0.18
THR4	5.70	1.380	0.43	0.17	0.72	0.54	-0.10	0.16	0.28	0.19
THR5	5.49	1.334	0.49	0.10	0.77	0.50	-0.08	0.20	0.27	0.22

EFF1	5.66	1.172	0.50	0.14	0.30	0.84	-0.22	0.24	0.39	0.28
EFF2	5.74	1.222	0.48	0.13	0.29	0.81	-0.19	0.27	0.41	0.25
EFF3	5.52	1.226	0.49	0.17	0.32	0.83	-0.16	0.29	0.38	0.33
EFF4	5.61	1.201	0.50	0.19	0.34	0.85	-0.16	0.33	0.42	0.32
EFF5	5.60	1.203	0.48	0.15	0.29	0.84	-0.17	0.31	0.43	0.32
EFF6	5.54	1.221	0.49	0.18	0.33	0.85	-0.15	0.24	0.45	0.36
COS1	3.11	1.915	-0.17	0.11	0.01	-0.15	0.90	-0.04	-0.33	-0.28
COS2	3.06	1.806	-0.18	0.06	0.04	-0.22	0.87	-0.05	-0.31	-0.22
COS3	3.15	1.891	-0.19	0.10	0.00	-0.18	0.92	-0.06	-0.38	-0.33
SLF4	5.06	1.578	0.25	0.12	0.19	0.24	-0.05	0.84	0.22	0.19
SLF5	5.34	1.478	0.30	0.09	0.23	0.28	-0.08	0.80	0.27	0.17
SLF6	5.24	1.588	0.26	0.17	0.23	0.24	0.03	0.81	0.15	0.08
SLF7	5.14	1.507	0.21	0.06	0.20	0.21	0.04	0.70	0.11	0.10
SLF9	5.25	1.677	0.22	0.18	0.18	0.19	-0.01	0.77	0.11	0.06
SLF10	5.16	1.466	0.24	0.06	0.21	0.34	-0.11	0.75	0.22	0.21
MOT1	5.42	1.438	0.34	0.12	0.33	0.47	-0.36	0.26	0.93	0.66
MOT2	5.17	1.655	0.33	0.09	0.31	0.41	-0.39	0.19	0.89	0.77
MOT3	5.47	1.425	0.37	0.13	0.37	0.49	-0.30	0.25	0.93	0.64
BEH1	4.73	1.774	0.25	0.02	0.24	0.37	-0.29	0.15	0.73	0.94
BEH2	4.88	1.732	0.26	0.02	0.22	0.32	-0.29	0.21	0.67	0.93