# Application of Protection Motivation Theory to Adoption of Protective Technologies

Tim Chenoweth
Boise State University
TimChenoweth@boisestate.edu

Robert Minch
Boise State University
RMinch@boisestate.edu

Tom Gattiker
Boise State University
TomGattiker@boisestate.edu

## Abstract

*While most technology adoption models have focused on beneficial technologies, Protection Motivation Theory (PMT) is a potentially valuable model for predicting adoption of protective technologies, which help users avoid harm from a growing number of negative technologies, such as malware. We present a PMT-based model of users' intentions to adopt anti-spyware software and test the model on undergraduate student computer users. Results show that perceived vulnerability, perceived severity, response efficacy, and response cost influence behavioral intention to use anti-spyware software as a protective technology. Maladaptive coping was affected to a much lesser degree by these variables, although it did have its own significant effect on behavioral intention. Results are compared to the small but growing number of promising PMT-based research models investigating technology adoption.*

## 1. Introduction

This paper tests a model designed to explain behavioral intention to adopt an important form of protective technology: anti-spyware software. Over 80% of home computer users have been found to lack core anti-malware protections, such as recently-updated anti-virus software, a properly configured firewall, and/or spyware protection [1]. In a business computing context, 65% of firms have experienced repeated external breaches in the last 12 months [2]. Security vulnerabilities cataloged by the CERT Coordination Center have risen from less than 1,100 in the year 2000 to over 7,000 in 2007 [3].

### 1.1. Spyware and anti-spyware software

Spyware is "a class of malware that collects information from a computing system without the data owner's consent." [4] Characteristics of six main classifications of spyware (adware, keyloggers, Trojans, scumware, dialers, and browser hijackers) can be found in [5]. Over 90% of PCs in large organizations have spyware, with some studies finding an average of 28 spyware programs running on each scanned PC [6]. Of 19 types of external breaches reported in a survey of global financial firms, spyware was the fifth most common cause, with 26% of organizations reporting repeated occurrences [2]. Spyware is a serious problem—as researchers recently reported, "The rampant invasion of spyware into home and business computers threatens the foundations of the networked economy with far-reaching legal and financial consequences." [7] The ability of spyware to hijack large numbers of computers, disable networks in times of crisis, and participate in denial-of-service attacks even raises the spyware problem to the level of a national security threat. [8]

Anti-spyware software is a useful tool for combating spy-ware; however, user adoption of the protective technology is currently a constraint on its effectiveness. Only some 10% of Internet users are using anti-spyware software [5]. Almost 75% of Internet users are aware of spyware, and 70% realize the importance of installing anti-spyware software but have no immediate plans to do so [9]. Even in a business context, individual user adoption is an important issue because to combat spyware, individual users often need to be involved in personally installing, configuring, and maintaining anti-spyware software. Thus understanding factors that facilitate and impede behavioral intentions to adopt anti-spyware software is a vital area for research.

### 1.2. Theoretical lenses on the problem

Anti-spyware software is a *protective technology.* Protective technologies differ from so-called *beneficial technologies*, such as word processing and electronic commerce applications, in that protective technologies combat or protect against negative

978-0-7695-3450-3/09 $25.00 © 2009 IEEE

technologies such as viruses and spyware [10]. The IS field's understanding of beneficial technologies has benefited from a rich and valuable collection of adoption frameworks including the Theory of Reasoned Action (TRA) [11], the Technology Acceptance Model (TAM) [12], and the Theory of Planned Behavior (TPB) [13]. However, with a few exceptions, these theories have not been applied to protective technologies. A few studies have applied TAM and TPB to spyware [5] [7]. Notably, however, the role of major constructs from these theories (such as perceived ease of use and self efficacy) has been found to be less important than in many studies of beneficial technologies awareness [10].

Mainstream IS technology acceptance theories will certainly play a key role in understanding intentions to use anti-spyware software; however, the IS field may benefit from applying theories from other disciplines as well. In particular, health researchers have spent many years applying and refining Protection Motivation Theory (PMT) [14] in domains such as seat belt usage and smoking cessation. Since adopting anti-spyware software can be conceptualized as a protective measure, it stands to reason that PMT might help IS researchers better understand intention to adopt anti-spyware software.

This paper develops a model that applies PMT to the spyware domain. The model is tested using survey data from 204 individuals. Implications and contributions are then discussed.

## 2.0. Literature review and research model

Protection Motivation Theory, proposed by Rogers in 1975 [14], theorizes that motivation to protect oneself from potential harm can be influenced by fear appeals. These fear appeals are said to contain three main components: (1) the magnitude of noxiousness of a depicted event; (2) the probability of that event's occurrence; and (3) the efficacy of a protective response. PMT is a special case of expectancy-value theory [15] in which a person's cognitive mediating processes evaluate the three fear appeal components, producing an appraised severity, expectancy of exposure, and belief in efficacy of a coping response, respectively. From this cognitive appraisal arises protection motivation, which is then postulated to produce an attitude change and intent to adopt a recommended (protective) response. The attitude change is not claimed to result from an emotional state of fear, but rather from protective motivation arising out of the cognitive appraisal process.

PMT has undergone a number of revisions and extensions since its inception. Its original developer proposed significant extensions eight years after its inception in several areas: (1) sources of information, providing input into the cognitive mediation process; (2) a refinement of cognitive mediating processes, including partitioning into adaptive responses versus maladaptive responses (the latter not directly managing the threat) forming a linear additive model leading to threat appraisal and coping appraisals; and (3) the addition of self-efficacy, or belief that one is or is not capable of performing a behavior [16]. Each of these model components is defined in the Section 3 description of our research model.

As researchers further investigated PMT, primarily in health-related domains, findings indicated that individuals appeared to make decisions that were largely predictable although not always with strict rationality (which the model notably does not require). For example, when perceived vulnerability was low and both self efficacy and response efficacy were high, subjects tended to adopt a precautionary or hyper-defensive strategy. The main effect of threat was also found to have an energizing effect on both adaptive and maladaptive coping. Such phenomenon are said to be indicative of various alternative methods utilized by individuals [17].

As more sophisticated path analyses began to be applied, more complex relationships became evident. While most maladaptive coping was found to be avoidant thinking, avoidance had a negative effect on fear (which was also affected by several other factors) while fear had a positive effect on avoidance [18]. Prescriptive recommendations for promoting protective behavior were difficult to clarify, with the most promising finding possibly being that both high self efficacy and high response efficacy increased desired adaptive coping without a corresponding increase in maladaptive coping.

Within 15 years of its inception, PMT had been applied to over 30 different domains, both inside and outside of health-related contexts, and was reviewed by its originator [19]. Among the stable assumptions noted were that PMT does not assume a rational decision maker, that many researchers have reported strong interaction effects between threat levels and coping responses, and that the appropriate measure of protection motivation is assumed to be behavioral intention. Fear appeals are treated as a form of verbal persuasion and part of environmental sources of information that initiate cognitive mediation processes [16] but do not have a direct effect on attitude change. Individual difference variables did not typically affect the outcomes in PMT research.

Subsequent meta-analyses of PMT in health contexts continued to support a greater predictive validity for coping appraisal components (self efficacy, response efficacy, and response costs) than threat appraisal components [20] [21]. A PMT model used by Milne et al. [20] is shown in Figure 1. Our research model (Figure 2) is an adaptation of Milne's model. Arrows in the model indicate directional associations and influences between variables, with +ve indicating positive associations and –ve indicating negative associations.

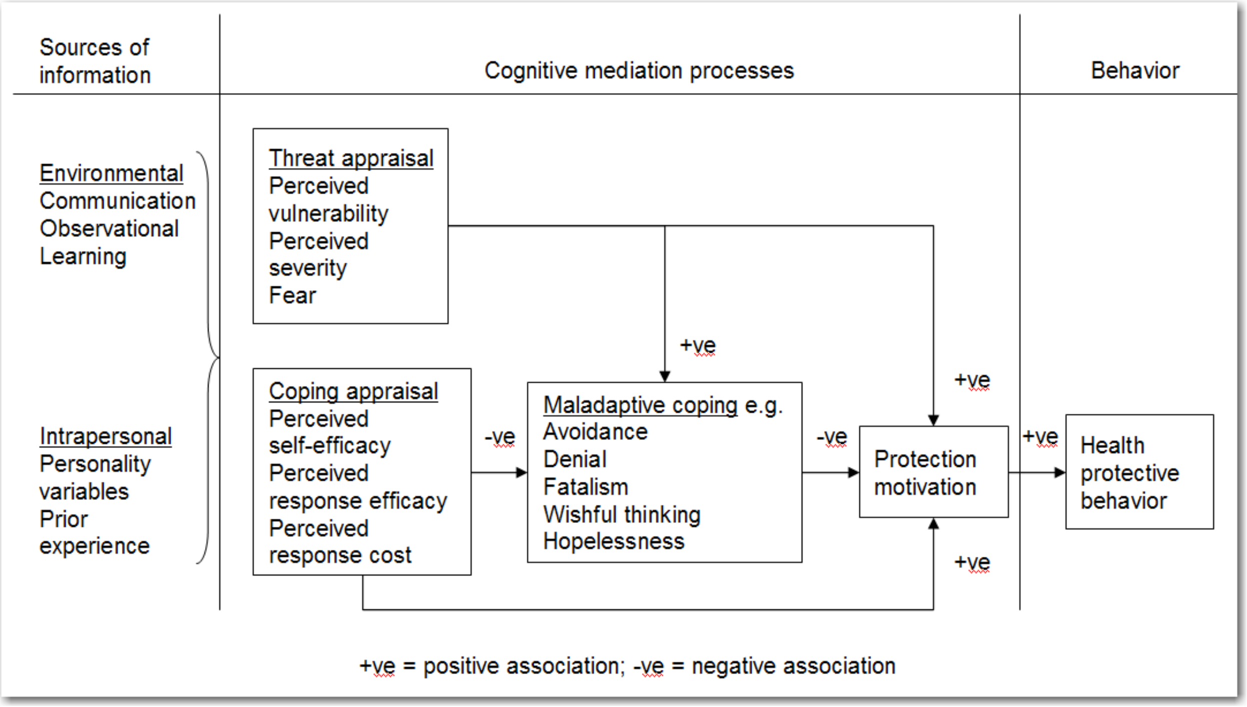

**Figure 1: Adapted PMT (Milne et al., 2000 [20])**

### 2.1. PMT in IT adoption research

Only a very few attempts at applying PMT to IT acceptance have been made. Employee's behavior towards IS security policy compliance [22] was studied using a theoretical model combining PMT along with General Deterrence Theory, TRA, Information Systems Success, Triandis' Behavioral Framework, and Rewards. Scale items from a 1997 version of PMT [19] for threat appraisal (five items) and coping appraisal (three items) were included in factor analyses followed by regression analysis for hypothesis testing. Three separate regression models were used, one of which contained PMT constructs. In this model as tested, the hypothesis "Threat appraisal affects employees' attitude toward complying with IS security policies" was supported (t-value +4.51, significant at p < .001) while the hypothesis "Coping appraisal affects employees' attitude toward complying with IS security policies" was not supported. Two important additional findings were that: (1) *attitude* towards complying with IS security policies has a significant impact on *intention* to comply and (2) employees' *intention* to comply with IS security policies has a significant impact on *actual* compliance. These findings strengthen confidence in the attitude-intention-behavior links important for models such as PMT to accurately predict behavior.

Components of PMT, along with concepts from the Elaboration Likelihood Model and Social Cognitive Theory, were included in research investigating the role of personal responsibility in Internet Safety [23]. Several interaction effects were found that involve PMT constructs. There was a "boomerang" interaction where moderate levels of threat susceptibility were the least related to protective behavior, compared with higher levels of the desired behavior at both low and high threat levels. A second interaction was evident when "those with low self-efficacy and low safety involvement had lower safety intentions when told safety was their personal responsibility than when told it was not . . ." [23] (page 75). Of the three most important factors influencing user safety behavior, two were PMT components (self-efficacy and response efficacy) while the third (personal responsibility) was not. Several other findings, such as differences in safety initiation versus maintenance activities, led to speculations concerning the various interaction effects and a call for more experimental studies to better understand safety behaviors and validate causes of safe and unsafe behavior.

Five components of PMT (threat appraisal items perceived vulnerability and perceived severity; and coping appraisal items self efficacy, response efficacy, and response cost) were employed in a study of home wireless security [24]. Rather than using a coping response such as intention to adopt a recommended behavior, a binary dependent variable of actual behavior was used—defined as whether a user has or has not enabled security features on their home wireless networks. All components except perceived vulnerability were found to significantly influence enabling of security features.

Research “broadly guided by concepts taken from Roger’s Protective Motivation Theory” considers perceived vulnerability, perceived severity, response efficacy, and self efficacy, in addition to non-PMT factors including personally accountability and punishment for non-compliance, to explore how users may be persuaded to employ desirable password security practices [25]. The authors found that conventional fear appeals were not always effective unless various other necessary conditions, both technical and social, are also in place.

A very recent study applies PMT to test a threat control model (TCM) designed to explain users’ omission of information security measures. [26] This is an interesting complement to the research we describe here, as instead of examining the intention to *use* a protective technology as we do, it examines the *lack* of intention to use (and furthermore the lack of actual use of) protective technologies and practices. Their TCM incorporates the PMT threat assessment factors perceived severity and perceived vulnerability, the coping assessments factors self-efficacy, response efficacy, and response cost, as well as locus of control from social cognitive theory and TPB. Dependent variables include both subjective user self-reported intended behaviors and objective direct observation of actual behavior via examination of computer logs. Notably, maladaptive coping was not considered as part of the model tested—all relationships considered were direct between independent variables and the two separately examined dependent variables.

Results reported in [26] indicate very strong relationships between perceived severity and self efficacy affecting both dependent variables, a weak effect for locus of control, and somewhat mixed but significant results for other relationships. The authors express a hope for many follow-up studies investigating interactions for coping versus actual and perceived behavioral outcomes, as well as other more complex relationships (some of which are considered in our present research).

## 3. Our research model

Our theoretical model, shown in Figure 2, is an adaptation of Milne et al.’s 2000 version of PMT [20].

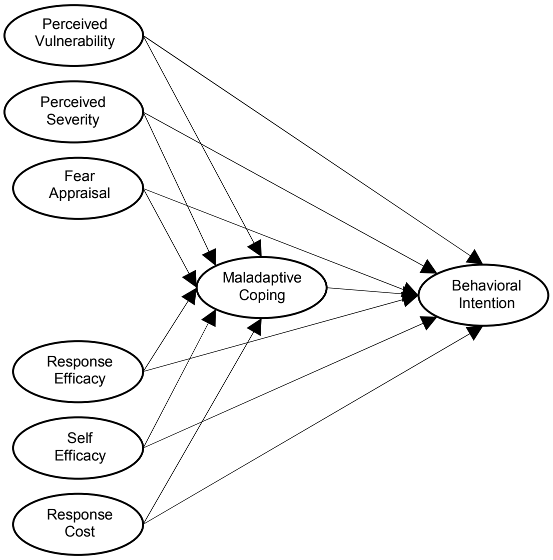

**Figure 2: Theoretical model for anti-spyware software adoption.**

The key constructs of our model are: perceived vulnerability, perceived severity, fear appraisal, response efficacy, self efficacy, response cost, maladaptive coping, and behavioral intention to adopt and use anti-spyware software. Consistent with the TRA [11], PMT postulates that behavioral intention indicates the degree to which someone is willing to try to perform a behavior such as installing and maintaining anti-spyware software. The more intense their behavioral intention, the higher the probability an individual will, in fact, adopt anti-spyware software. Maladaptive coping is defined as coping behaviors that do not directly manage the threat of becoming infected with spyware. PMT predicts that maladaptive coping will negatively impact behavioral intention. We therefore hypothesize that:

**H1. Maladaptive coping has a negative effect on behavioral intention to use anti-spyware software.**

Perceived vulnerability is defined as a user's assessment of his/her own probability of having their computer infected with spyware. PMT predicts that perceived vulnerability positively influences maladaptive coping and behavioral intention. We therefore hypothesize that:

**H2a. Perceived vulnerability has a positive effect on maladaptive coping.**

**H2b. Perceived vulnerability has a positive effect on behavioral intention to use anti-spyware software.**

We defined perceived severity as a measure of the perceived magnitude of what might happen if a respondent's computer is infected with spyware. Examples used were the loss of personal information and identity theft. PMT predicts that perceived severity will positively affect and maladaptive coping and behavioral intention. We therefore hypothesize that:

**H3a. Perceived severity has a positive effect on maladaptive coping.**

**H3b. Perceived severity has a positive effect on behavioral intention to use anti-spyware software.**

Fear appraisal is defined as the degree to which the possibility of becoming infected with spyware causes a user to feel afraid or apprehensive. Our adapted PMT model assumes fear appraisal has a role in threat appraisal similar to perceived vulnerability and perceived severity, directly and positively impacting both maladaptive coping and behavioral intention. We therefore hypothesize that:

**H4a. Fear appraisal has a positive effect on maladaptive coping.**

**H4b. Fear appraisal has a positive effect on behavioral intention to use anti-spyware software.**

Response efficacy is defined as the belief that the recommended response (i.e., using anti-spyware software) will be effective in reducing the risk of becoming infected with spyware. This is a measure of the respondents' confidence in the effectiveness of anti-spyware software in preventing spyware from being loaded onto their computer. PMT predicts that response efficacy will have a negative relationship with maladaptive coping and a positive relationship with behavioral intention. We therefore hypothesize that:

**H5a. Response efficacy has a negative effect on maladaptive coping.**

**H5b. Response efficacy has a positive effect on behavioral intention to use anti-spyware software**.

Self efficacy is defined as a respondent's level of confidence in their ability to perform the recommended coping behavior (e.g., installing and configuring anti-spyware software). PMT predicts that self efficacy will negatively impact maladaptive coping and positively impact behavioral intention. We therefore hypothesize that:

**H6a. Self efficacy has a negative effect on maladaptive coping.**

**H6b. Self efficacy has a positive effect on behavioral intention to use anti-spyware software**.

Response cost is defined as the perceived costs incurred by a user in performing a recommended coping behavior (i.e., installing and configuring anti-spyware software). This definition is in terms of the effort involved in using anti-spyware software, not the dollar cost of purchasing and updating the software. PMT predicts that response cost will positively impact maladaptive coping and negatively impact behavioral intention. We therefore hypothesize that:

**H7a. Response cost has a positive effect on maladaptive coping.**

**H7b. Response cost has a negative effect on behavioral intention to use anti-spyware software**.

## 4. Questionnaire development and data collection

Because very little work using Protection Motivation Theory had appeared in the IS literature at the time we constructed our survey instrument, we adapted questions from several studies in various areas including condom usage [27], exercise behavior [28], coping with stress [29], and HIV prevention [30]. These questions were combined with questions adapted from [24] and questions developed by the authors. Questions concerning intent to adopt were adapted from [10].

In order to refine the measures, we conducted two pilot studies, modifying the instrument after each. First, the survey questions and construct definitions were presented to eight MBA students specializing in IT, who were asked to sort the questions into groups according to which construct they felt the questions belonged to. Students were also invited to provide unstructured feedback on question wording. Second, the survey was administered to 232 undergraduate students and the resulting data analyzed using exploratory and confirmatory factor analysis. Based on these two pilots questions were added, removed and or modified.

Next, to further purify the measures and to enable testing of hypotheses 1 through 7, an additional 204 undergraduate students were surveyed, using the refined instrument. The descriptive statistics from the sample are presented in Table 1.

**Table 1: Descriptive statistics**

| *Measure* | *Items* | *Freq.* | *%* |
|---|---|---|---|
| Gender | Male | 125 | 61.3 |
| | Female | 74 | 36.3 |
| | Not Reported | 5 | 2.5 |
| | | | |
| Age | Under 25 | 115 | 56.4 |
| | 25 to 34 | 62 | 30.4 |
| | 35 to 44 | 15 | 7.4 |
| | 45 to 54 | 6 | 2.9 |
| | 55 to 64 | 0 | 0 |
| | 65 and over | 1 | 0.5 |
| | Not Reported | 5 | 2.5 |
| | | | |
| Computer Exp. (self Reported) | I consider myself a novice. | 9 | 4.4 |
| | I have some but limited experience. | 73 | 35.8 |
| | I have quite a lot of experience. | 85 | 41.7 |
| | I consider myself an expert. | 32 | 15.7 |
| | Not Reported | 5 | 2.5 |

Because the sample was collected at a university with many non-traditional students (i.e. working adults) the sample is somewhat representative of the overall population of general computer users. During fall 2009, the survey will be administered to a sample that is carefully constructed to be more representative of our target population. The data were analyzed using both exploratory and confirmatory factor analysis. Based on low factor loadings and high normalized residuals, some items were judged to not adequately represent their intended construct and were thus eliminated [31] [32]. During this analysis, items for perceived severity and fear appraisal loaded on the same factor, even after various items were eliminated and various subsets of items were tested, thus calling into question the discriminant validity of these constructs. Additionally, this was confirmed by a chi square difference test [33] (i.e. the chi square statistic for the one construct model was not significantly different from the two construct model). Because of this, we concluded that we had no discriminant validity between perceived severity and fear appraisal. Review of [19] makes it clear that perceived severity is one of the core constructs of PMT, with fear appraisal playing a less central role. Thus fear appraisal was removed making it impossible to test H4. Means, standard deviations, and Cronbach's alpha scores for the remaining constructs appear in Table 2. All Cronbach's alpha scores are greater than 0.7 indicating good reliability [33].

**Table 2: Construct means, variances, and cronbach's alpha scores**

| *Construct Items* | *Mean* | *Standard Deviations* | *Cronbach's Alpha* |
|---|---|---|---|
| Perceived Vulnerability: | 4.75 | 1.26 | 0.755 |
| Perceived Severity: | 4.57 | 1.37 | 0.848 |
| Response Efficacy: | 5.46 | 0.98 | 0.843 |
| Self Efficacy: | 5.37 | 1.40 | 0.898 |
| Response Cost: | 3.48 | 1.50 | 0.858 |
| Maladaptive Coping: | 3.53 | 1.33 | 0.844 |
| Behavioral Intention: | 5.85 | 1.17 | 0.893 |

The measurement purification process results in final scales of three or four items per construct. Confirmatory factor analysis of this final measurement model using AMOS 16.0 yielded excellent goodness of fit statistics. The relative chi squared value (1.59) is less than 2.0, as recommended in [34] as the acceptable limit. In addition, both the Tucker-Lewis coefficient (0.94) and the comparative fit index (0.95) are greater than 0.9 [35] [36] and the RMSEA (0.54) is less than 0.08 and reasonably close to 0.05 [37]. All indicator loadings exceed 0.68 and are significant ($p < 0.001$). These loadings are displayed in Table 3 along with the estimated error term variances.

**Table 3: Standardized factor loadings and estimated error variances**

| *Construct Items* | *Standardize Indicator Loadings* | *Estimated Error Variance* |
|---|---|---|
| **Perceived Vulnerability:** | | |
| PV1 | 0.68 | 1.07 |
| PV6 | 0.68 | 1.34 |
| PV9 | 0.77 | 1.03 |
| **Perceived Severity:** | | |
| PS1 | 0.78 | 0.94 |
| PS10 | 0.82 | 0.86 |

| | | |
|---|---|---|
| PS11 | 0.82 | 0.73 |
| **Response Efficacy:** | | |
| RE1 | 0.70 | 0.76 |
| RE5 | 0.74 | 0.58 |
| RE6 | 0.72 | 0.68 |
| RE7 | 0.86 | 0.38 |
| **Self Efficacy:** | | |
| SE1 | 0.88 | 0.56 |
| SE4 | 0.84 | 0.65 |
| SE7 | 0.87 | 0.56 |
| **Response Cost:** | | |
| RC5 | 0.95 | 0.28 |
| RC7 | 0.82 | 0.96 |
| RC8 | 0.69 | 1.48 |
| **Maladaptive Coping:** | | |
| A1 | 0.83 | 0.68 |
| A2 | 0.81 | 0.84 |
| A6 | 0.77 | 0.94 |
| **Behavioral Intention:** | | |
| BI1 | 0.72 | 0.37 |
| BI2 | 0.78 | 0.31 |
| BI3 | 0.92 | 0.77 |
| BI4 | 0.89 | 0.73 |

Correlations between the constructs were computed during confirmatory factor analysis and are provided in Table 4. The absolute values of all correlations are less then 0.5, providing additional evidence of discriminant validity [38].

**Table 4: Correlations between constructs**

| *Constructs* | *Correlation* |
|---|---|
| Perceived Vulnerability ⇔ Perceived Severity | 0.170 |
| Perceived Vulnerability ⇔ Response Efficacy | 0.032 |
| Perceived Vulnerability ⇔ Self Efficacy | 0.275 |
| Perceived Vulnerability ⇔ Response Cost | 0.039 |
| Perceived Vulnerability ⇔ Maladaptive Coping | -0.154 |
| Perceived Severity ⇔ Response Efficacy | 0.272 |
| Perceived Severity ⇔ Self Efficacy | -0.053 |
| Perceived Severity ⇔ Response Cost | 0.085 |
| Perceived Severity ⇔ Maladaptive Coping | -0.119 |
| Response Efficacy ⇔ Self Efficacy | 0.307 |
| Response Efficacy ⇔ Response Cost | -0.317 |
| Response Efficacy ⇔ Maladaptive Coping | -0.311 |
| Self Efficacy ⇔ Response Cost | -0.463 |
| Self Efficacy ⇔ Maladaptive Coping | -0.314 |
| Response Cost ⇔ Maladaptive Coping | 0.439 |

## 5. Results of hypothesis tests

We estimated our model using AMOS 16.0. Overall, the model provided a good fit. As with the confirmatory factor analysis, the relative chi squared value (1.57) is less than 2.0 while both the Tucker-Lewis coefficient (0.94) and the comparative fit index (0.95) are greater than 0.9 and the RMSEA (0.05) is less than 0.08. Taken together, these results indicate a close fit between the data and our model. The estimated model is presented in Figure 3. The model explains 43% of the variance of behavioral intention to use anti-spyware software and 26% of the variance of intention to use a maladaptive coping strategy (i.e. avoidance), providing evidence that PMT is an appropriate framework for studying protective technologies.

Hypotheses H1, H2b, and H5b are significant at the 0.05 level ($p < 0.05$ and $p > 0.01$). Hypotheses H3b, H7a, and H7b are significant at the 0.01 level ($p < 0.01$). Hypotheses H2a, H3a, H5a, H6a and H6b were not significant ($p > 0.05$).

Our finding that response cost has a highly significant effect on behavioral intention (H7a) is consistent with the results of Hu and Dinev [7] but contradicts the results of Lee and Kozar [5]. Both the Hu and Dinev study and the Lee and Kozar study focused on spyware usage and referred to our response cost construct as perceived ease of use. This was the only construct in common across all three studies.

A closer fit with our study is Woon's work, which uses PMT and focuses on the determinants affecting whether an individual enables the security features for their home wireless network [24]. Like Woon, we found that perceived severity, response efficacy, and response cost have significant relationships with our dependent variable. Our results differed from Woon's in that perceived vulnerability was significant in our study and self efficacy was not. It is important to note that Woon's dependent variable was whether a respondent had enabled the security features for their wireless network while ours was a respondent's intention to use spyware in the future.

Pahnila et al. also used PMT in their study of employees' behavior concerning IS security policy compliance [22]. They combined perceived vulnerability and perceived severity into a threat appraisal construct, and response efficacy, self efficacy, and response cost into a coping appraisal construct. They then included threat appraisal and coping appraisal in their regression with employees' attitude toward complying with IS security policies as the dependant variable. Pahnila et al. found that threat appraisal did have a significant relationship with attitude toward compliance, while coping appraisal did not. This is consistent with our finding, which found that perceived vulnerability and perceived severity did have a significant relationship with intention to use spyware (Pahnila et al.'s threat appraisal construct), while self efficacy did not (part of their coping appraisal construct). However, in our study response efficacy and response cost were significantly related to intention to use spyware. These relationships were not directly test by Pahnila et al.

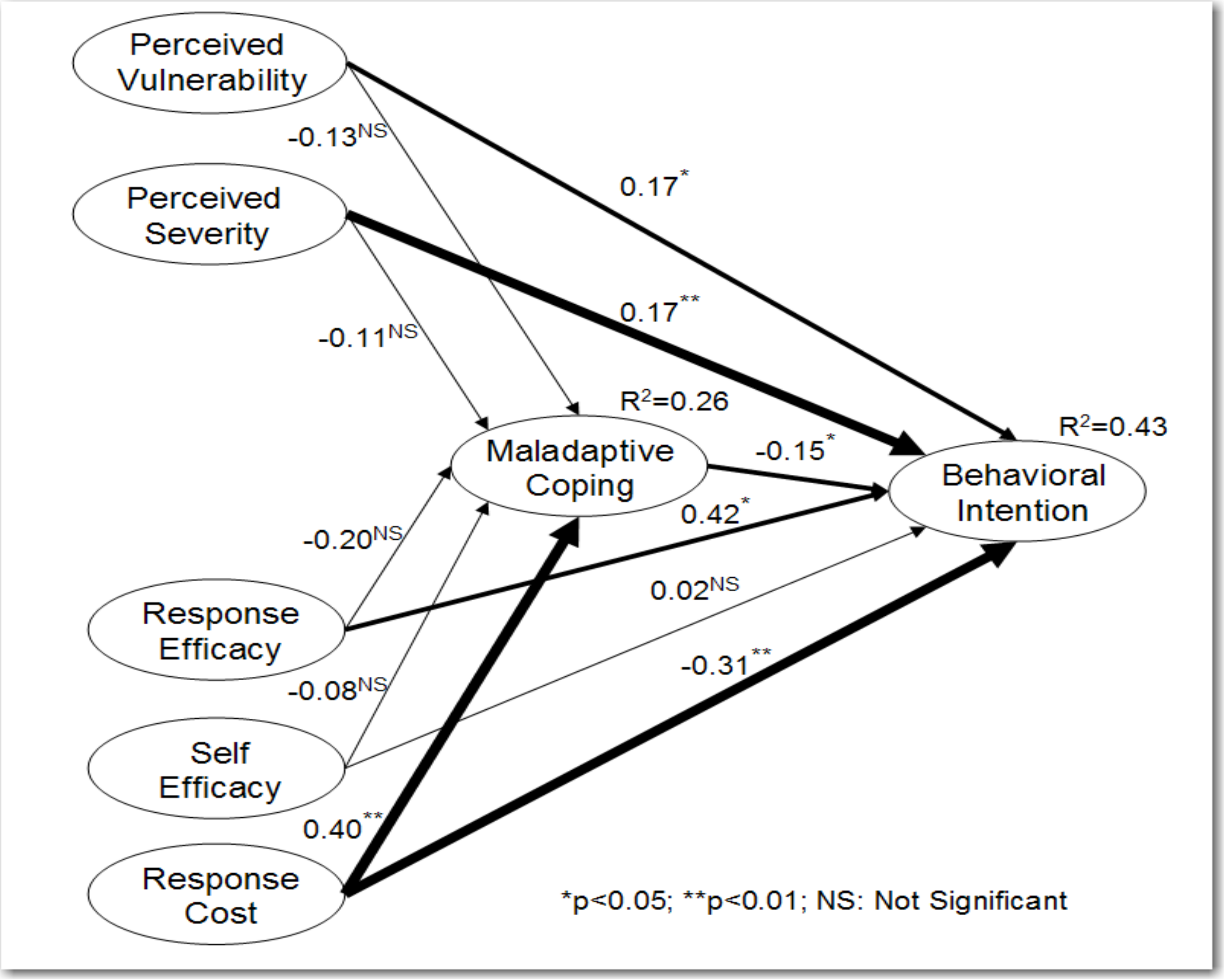

**Figure 3: The estimated model**

## 6. Discussion and conclusions

Perceived vulnerability, perceived severity, response efficacy and response cost were found to be significant influencers of users' intention to adopt anti-spyware protective technology. This is in keeping with PMT's expectancy-value heritage, which assumes a cognitive appraisal process primarily based on users' perceptions of costs and benefits weighted by estimated likelihoods. Subjects with perceptions that anti-spyware software is effective and reasonably easy to use are likely to have a high behavioral intention to use it.

We found that self efficacy did not significantly influence a user's behavioral intention to use anti-spyware software. This finding contrasts with the importance of self efficacy in much health-related PMT research. This may be a contextual artifact. In many health-related PMT studies, the prescribed protective behavior may be very difficult to perform and thus individuals may doubt their ability to do so. For example, many smokers doubt their ability to successfully complete a smoking cessation program. A smoker who doubts his or her ability to stop smoking may raise the importance of this factor to a near pre-emptive level and thus not even make an attempt to stop. By contrast, in the context of anti-spyware software, the issue seems to not be an individual's belief in their own *ability* to install and maintain the software (self efficacy) as much as their estimation of the level of *difficulty* associated with doing so (response cost).

Maladaptive coping was significantly influenced only by response cost in our model. Since our response cost component primarily relates to effort and time required rather than monetary cost, and our maladaptive coping component relates to avoidance behaviors, this may be explainable by positing that users who estimate a high commitment of time and effort may simply avoid further consideration of the protective behaviors, however desirable they may be in other regards. It should also be noted that maladaptive coping itself had only a weakly significant effect on behavioral intention.

For organizations, these results highlight the importance of educating their employees concerning both the dangers of spyware and that using and maintaining anti-spyware software on both their corporate machines and their personal machines is an effective way to prevent spyware infections. This educational process should focus on why employees are vulnerable to spyware infection, the potential consequences of becoming infected (loss of sensitive personal or corporate information, etc.), and why using and maintaining anti-spyware software is effective in preventing spyware infections.

Our results also demonstrate the importance of organizations providing anti-spyware support to their employees. Or work clearly shows that a users perception concerning how much difficulty they will have installing and using anti-spyware software (our response cost construct) plays a key role in their decision whether or not to use anti-spyware software. As an individual's perception concerning these response costs increase, their intention to use anti-spyware software decreases and their tendency to adopt some maladaptive coping strategy (such as avoiding the issue) increases. Organizations will need to provide both training on how to use anti-spyware software and support for helping their employees properly install the software.

For researchers, our study provides evidence that PMT may be a valuable tool for understanding and explaining why individuals do or do not adopt protective technologies such as anti-spyware software. In addition, PMT needs to be tested using other forms of protective technologies such as firewall or anti-virus adoption.

A significant limitation is that we tested the model using undergraduates. Even though many individuals in the sample were older, "non-traditional" students with significant work experience, the sample, may limit generalizability. Compared to the overall population, undergraduates may be less risk averse when it comes to spyware; and they may be more technologically sophisticated and more willing to try new applications. Our research agenda includes testing the model on a broader sample.

## 7. References

[1] National Cyber Security Alliance, "AOL/NCSA Online Safety Study," Dec. 2005; http://staysafeonline.org/pdf/safety_study_2005.pdf.

[2] Deloitte, "2007 Global Security Survey," 2007; http://www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf.

[3] CERT/CC, "Full Statistics," 2008; http://www.cert.org/stats/fullstats.html.

[4] A. Hackworth, "Spyware," 2005; http://www.us-cert.gov/reading_room/spyware.pdf.

[5] Y. Lee and K.A. Kozar, "Investigating factors affecting the adoption of anti-spyware systems," *Commun. ACM*, vol. 48, 2005, pp. 72-77.

[6] X. Zhang, "What do consumers really know about spyware?," *Commun. ACM*, vol. 48, 2005, pp. 44-48.

[7] Q. Hu and T. Dinev, "Is spyware an Internet nuisance or public menace?," *Commun. ACM*, vol. 48, 2005, pp. 61-66.

[8] R. Thompson and R. Thompson, "Why spyware poses multiple threats to security," *Commun. ACM*, vol. 48, 2005, pp. 41-43.

[9] R. Poston, T.F. Stafford, and A. Hennington, "Spyware: a view from the (online) street," *Commun. ACM*, vol. 48, 2005, pp. 96-99.

[10] T. Dinev and Qing Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies.," *Journal of the Association for Information Systems*, vol. 8, Jul. 2007, pp. 386-408.

[11] M. Fishbein and I. Ajzen, *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*, Reading, MA: Addison-Wesley, 1975.

[12] F.D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology.," *MIS Quarterly*, vol. 13, 1989, pp. 319-340.

[13] I. Ajzen, "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, Dec. 1991, pp. 179-211.

[14] R.W. Rogers, “A Protection Motivation Theory Of Fear Appeals and Attitude Change.,” *Journal of Psychology*, vol. 91, 1975, pp. 93-114.

[15] W.J.H. Edwards, “The Theory of Decision Making.,” *Psychological Bulletin*, vol. 51, 1954, pp. 380-417.

[16] R.W. Rogers, “Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation,” *Social Psychophysiology: A Sourcebook*, London: Guilford, 1983, pp. 153-176.

[17] S. Prentice-Dunn and R.W. Rogers, “Protection Motivation Theory and preventive health: beyond the Health Belief Model,” *Health Education Research*, vol. 1, 1986, pp. 153-161.

[18] P.A. Rippetoe and R.W. Rogers, “Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping With a Health Threat,” *Journal of Personality and Social Psychology*, vol. 52, 1987, pp. 596-604.

[19] R.W. Rogers and S. Prentice-Dunn, “Protection Motivation Theory,” *Handbook of Health Behavior Research I: Personal and Social Determinants*, New York: Plenum Press, 1997, pp. 113-132.

[20] S. Milne, P. Sheeran, and S. Orbell, “Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory,” *Journal of Applied Social Psychology*, vol. 30, 2000, pp. 106-143.

[21] D.L. Floyd, S. Prentice-Dunn, and R.W. Rogers, “A Meta-Analysis of Research on Protection Motivation Theory,” *Journal of Applied Social Psychology*, vol. 30, 2000, pp. 407-429.

[22] S. Pahnila, M. Siponen, and A. Mahmood, “Employees' Behavior towards IS Security Policy Compliance,” *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, IEEE Computer Society, 2007, p. 156b; http://portal.acm.org/citation.cfm?id=1255934.

[23] R. LaRose, N.J. Rifon, and R. Enbody, “Promoting personal responsibility for internet safety,” *Commun. ACM*, vol. 51, 2008, pp. 71-76.

[24] I. Woon, G. Tan, and R. Low, “A Protection Motivation Theory Approach to Home Wireless Security,” *Proceedings of the Twenty-Sixth International Conference on Information Systems*, 2005, pp. 367-380.

[25] D. Weirich and M.A. Sasse, “Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World,” *New Security Paradigms Workshop*, Cloudcroft, NM: ACM, 2002, pp. 137-143.

[26] M. Workman, W. Bommer, and D. Straub, “Security lapses and the omission of information security measures: A threat control model and empirical test,” *Computers in Human Behavior*, vol. (in press), 2008.

[27] R. Ho, “Predicting intention for protective health behaviour: A test of the protection versus the ordered protection motivation model,” *Australian Journal of Psychology*, vol. 52, 2000, pp. 110-118.

[28] S. Milne, S. Orbell, and P. Sheeran, “Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions,” *British Journal of Health Psychology*, vol. 7, 2002, pp. 163-184.

[29] C. Carver, M. Scheier, and J. Weintraub, “Assessing Coping Strategies: A Theoretically Based Approach,” *Journal of Personality and Social Psychology*, vol. 56, 1989, pp. 267-283.

[30] C. Abraham et al., “Exploring teenagers' adaptive and maladaptive thinking in relation to the threat of hiv infection,” *Psychology & Health*, vol. 9, 1994, pp. 253-272.

[31] J. Anderson and D.W. Gerbing, “Structural equation modeling in practice: A review and recommended two-step approach,” *Psychological Bulletin*, vol. 103, 1988, pp. 411-423.

[32] R. Bagozzi and Y. Yi, “On the Evaluation of Structural Equation Models,” *Academy of Marketing Science*, vol. 16, 1988, pp. 74-94.

[33] R. Bagozzi and L. Phillips, “Representing and Testing Organizational Theories: A Holistic Construal,” *Administrative Science Quarterly*, vol. 27, 1982, pp. 459-489.

[34] B. Byrne, *A Primer of LISREL: Basic applications and programming for confirmatory factor analytical models*, New York: Springer-Verlag, 1989.

[35] K. Bollen, “A new incremental fit index for general structural equation models,” *Sociological Methods and Research*, vol. 17, 1989, pp. 303-316.

[36] P. Bentler, “Comparative fit indexes in structural models,” *Psychological Bulletin*, vol. 107, 1990, pp. 238-246.

[37] M. Browne and R. Cudeck, “Alternative ways of assessing model fit,” *Testing Structural Equation Models*, Newbury Park, CA: Sage, 1993, pp. 136-162.

[38] J. Bailey and S. Pearson, “Development of a tool for measuring and analysing computer user satisfaction,” *Management Science*, vol. 29, 1983, pp. 530-545.