Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data

Robert E. Crossler
The University of Texas – Pan American
recrossler@utpa.edu

Abstract

This study uses Protection Motivation Theory (PMT) as a theoretical framework to empirically test why people back up data on their personal computers. The theory was tested using 112 surveys collected using both paper and online data sources. The findings show that computer self-efficacy and response efficacy both positively affect the backing up of data, while perceived security vulnerability and perceived security threat both negatively affect the backing up of data. The results and implications of these findings suggest further research is necessary to fully understand the relationship between security threats and protective behaviors.

1. Introduction

Businesses regularly fight cyber crime to protect information that it has and to ensure that company resources continue to operate as necessary. One aspect of cybercrime that businesses face is the battle against attacks that steal and destroy important documents such as viruses, worms, Trojan horses, laptop theft and hackers [1]. One method to ensure that files are available should they be lost is to back up the important files and folders regularly. If a computer malfunctions or is destroyed by a malicious hacker, not having backups of important files means that those files are lost forever (http://www.us-cert.gov/). However, research shows that people are not backing up their data as regularly as they ought to [2, 3]. This raises the following research question – What determines whether individuals backup the data on their personal computer? The remainder of this paper answers this question by presenting Protection Motivation Theory (PMT) as a potential theory to explain differences in security behavior, particularly backing up personal data. The following section discusses the background literature and proposes the PMT model to be tested. The analysis of the data and a discussion of the results follow. Finally, the conclusions of the findings are presented.

2. Background

One theory generally been relied upon to explain IS misuse within an organization is General Deterrence Theory (GDT), which was adapted from the criminal justice field and has been used within IS research to show that security countermeasures can act as a deterrent by increasing the perceptions of the severity and certainty of punishment for misusing information systems [4]. GDT uses three variables to explain IS misuse within an organization; severity of punishment, certainty of punishment, and rival explanations, which has been operationalized in many different ways including IS specific codes of ethics [5], preventative measures [6], and ethics training [7]. One limitation to GDT is that it only applies within a corporate setting. When expanding the explanation of preventing IS misuse through punishment to a home environment, the theory no longer holds, as there is no one to punish individual users.

A recent panel on IS security at the 2007 Americas Conference on Information Systems (AMCIS) suggested that, in order to deal with the increased challenges of IS security, new theories from reference disciplines needed to be examined [8]. One theory from the field of social psychology called Protection Motivation Theory (PMT), has recently been used in IS security literature [9]. PMT can explain security behaviors outside of a corporate setting, providing a theoretical explanation as to why people perform certain countermeasures to detect and prevent computer threats, which ultimately result in deterring continued attacks on computer systems.

The premise of PMT is that information is first received (sources of information), which leads to an evaluation of it by the person receiving that information (cognitive mediating process), and finally to the person taking some action based on the

IEEE computer society

978-0-7695-3869-3/10 $26.00

information received (coping mode). Sources of information are the input variables to the model and include environmental and intrapersonal sources. Environmental sources of information include verbal persuasion and observational learning. Intrapersonal sources include personality aspects and feedback from prior experience including experiences associated with performing the behavior of interest [10]. There are two types of cognitive mediating processes: the threat appraisal process, and the coping appraisal process. The threat appraisal is comprised of the threat perception (severity and vulnerability) of continuing with the maladaptive response. In the case of this study, threat appraisal is called security threat appraisal and is defined as *an individual's assessment about the level of danger posed by a security event*. The coping appraisal process consists of the individual's confidence that a coping response will reduce or mitigate a security threat (response efficacy) and that he believes he can perform the given response (self-efficacy), but that the cost of performing such an action is not too high (prevention cost). In this study, coping appraisal is called security coping appraisal and is defined as *an individual's assessment of his ability to perform a given behavior and his confidence that a given behavior will be successful in mitigating or averting the potential loss or damage resulting from a threatening security event, at a perceived cost that is not too high*.

The outcome of the cognitive mediating processes is a decision to apply the applicable adaptive response or the behavior of interest. The two types of adaptive behaviors are adaptive coping (to protect the self or others) and maladaptive coping (not to protect the self or others) [10]. Figure 1 models this process.

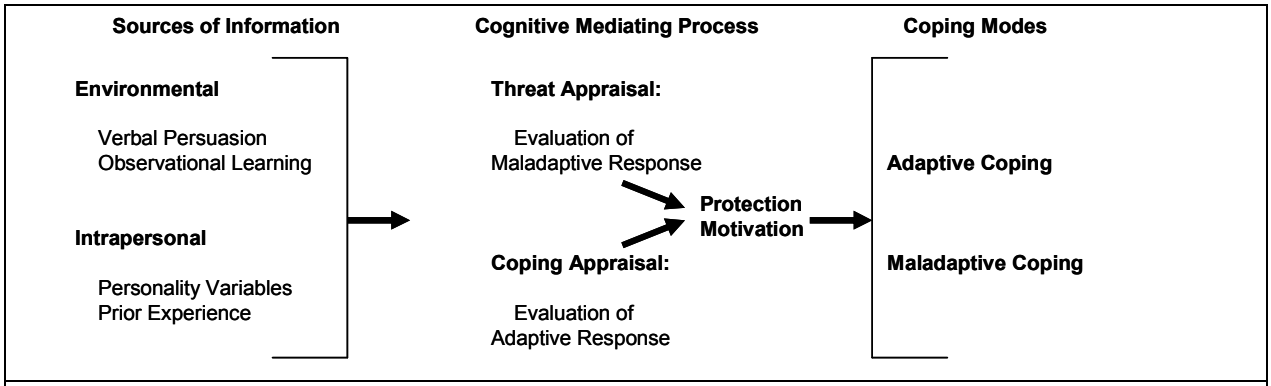

Figure 1. Protection Motivation Theory [10]

Currently, one study has been published that empirically tests PMT in an IS context. It was found that perceived vulnerability, response efficacy, and response cost led to a person enabling home wireless security measures [9]. These results suggest that adapting PMT to an information security context will produce positive results. The paper by Woon et al. only studied wireless security usage and did not use a context specific measure of self-efficacy as proposed by Marakas et al. [11]. Recently, other studies that propose the use of PMT are appearing at IS conferences [12, 13].

2.1. Security Threat Appraisal

Security threat appraisal is similar to perceived risk, which is conceptualized as uncertainty and consequences [14-16]. These conceptualizations are similar in that both capture uncertainty and consequences, but security threat appraisals refers to uncertainty as vulnerability and captures how vulnerable a person thinks he is to a given threat. This study conceptualizes security threat appraisal as being comprised of perceived security vulnerability and perceived security threat. Perceived security vulnerability is *an individual's assessment of the probability of a threatening security event occurring*. Perceived security threat is *an individual's assessment of the severity of the consequences resulting from a threatening security event*.

PMT posits that threat appraisal is one determinant that impacts whether a person adopts a given behavioral response [10]. A number of studies suggest that as a person's perception of risk increases he is less likely to participate in risky activities or is more likely to take steps to protect himself from risks [14, 15, 17-19]. When investigating people's willingness to share private information on a government website, the perceived risk of anti-terrorism measures by the government led to a lower likelihood to share information. However, perceived risk in the Internet environment did not show the

same effects [17]. Another study looking just at perceived risk found that as perceived risk increases a person's intention to enter into electronic transactions decreases [15]. Further confirming this research is another study which found that increases in perceived risk led to a lower likelihood of people using inter-organizational data exchanges [14]. In a study investigating the online privacy behaviors of teenagers on the Internet, risk appraisal (susceptibility and severity of perceived risk) led to a lower willingness to provide information to websites. People that were less likely to provide information to websites were also more likely to practice other coping behaviors to protect their personal information, such as provide false information or provide incomplete information [18]. The difference between the study of privacy behavior and the use of electronic transactions and data exchanges is that practicing privacy behaviors is a task that limits risk, whereas the other two examples are entering into a transaction that puts an individual more at risk. In addition, results from research utilizing General Deterrence Theory (GDT) have shown that deterrent certainty and severity impact IS misuse [4] which is a behavior that limits or reduces risk (that of being punished). In this study, the performance of behaviors that are done to protect an individual from security risks are being investigated; therefore, I hypothesize that increases in security threat appraisal will lead to increases in the frequency of running data backups.

H1: Greater perceived security vulnerabilities will lead to running data backups more frequently.

H2: Greater perceived security threats will lead to running data backups more frequently.

2.2. Security Coping Appraisal

This study conceptualizes the security coping appraisal as being comprised of security self-efficacy, response efficacy, and prevention cost. Security self-efficacy is *an individual's confidence in his/her own ability to perform the recommended behavior to prevent or mitigate the threatening security event*. Response efficacy is *an individual's confidence that a recommended behavior will prevent or mitigate the threatening security event*. Prevention cost is *the opportunity costs – time, cognitive effort, financial – of adopting the recommend behavior to prevent or mitigate the threatening security event*.

2.2.1. Security Self-Efficacy. PMT posits that coping appraisal is one determinant that impacts whether a person adopts a given behavioral response [10]. An experimental study showed that as a person's coping appraisal increased his willingness to perform the coping behavior also increased [20]. PMT research has found similar results. As noted above, one of the components of coping appraisal is self-efficacy. Self-efficacy was initially conceptualized by Bandura [21] and defined as "*the conviction that one can successfully execute the behavior required to produce outcomes"* [21]. Since its initial conceptualization, a number of studies have applied the concept of self-efficacy to explain individual's performance at using computers [22-29]. Rather than simply use self-efficacy to test usage of computer systems, one study validated and tested an instrument called computer self-efficacy, which found that computer self-efficacy influenced the expectations of individuals on the outcome of using computers [30]. However, there exists conflicting results with those of Compeau and Higgins. In one study that combined the technology adoption literature, computer self-efficacy was shown to not be a significant determinant in the proposed model [31]. That study used the original measures for computer self-efficacy that were proposed by Compeau and Higgins [30], and did not adapt it to the study's context. Noting the discrepancy in findings with computer self-efficacy in the Venkatesh et al. study and others [32, 33], Marakas et al. [11] conducted an analysis of the research done with this construct. They found that when computer self-efficacy is adapted to the setting being studied it shows to be a good predictor of performance. However, in the studies when computer self-efficacy is not adapted to the setting, then it is not a significant predictor of performance. Marakas et al. justified these findings by going back to the work of Bandura [34], the person that originally conceptualized self-efficacy, to show that computer self-efficacy needs to be context specific.

As this study is about security, it is necessary and appropriate to adapt the instrument to security and rename the construct security self-efficacy. Similar to prior research, it is expected that increases in security self-efficacy will lead to increases in security behavior.

H3: Greater security self-efficacy will lead to running data backups more frequently.

2.2.2. Response Efficacy. By definition, response efficacy is measuring the same thing as outcome expectations. Response efficacy is *the confidence a person has that a given response will mitigate or reduce a threat;* outcome expectations is defined as

"*a person's estimate that a given behavior will lead to certain outcomes" [21]*. IS research has shown that outcome expectations influence individual performance or acceptance of technology [22, 30, 31, 35, 36]. One study of end users found that along with computer self-efficacy, outcome expectations led to usage of technology [22]. Additionally, in a study that combined the variables from a number of different acceptance models it was shown that outcome expectations led to intention to use a technology [31]. As response efficacy is by definition the same thing as outcome expectations and IS research has shown that outcome expectations lead to a higher likelihood to use a technology, it is expected that as response efficacy increases the frequency of backing up data will also increase.

H4: Greater response efficacy will lead to running data backups more frequently.

2.2.3. Prevention Cost. PMT posits that as the response cost goes up the likelihood of performing the adaptive coping response goes down. Such a suggestion is in line with other security research that says a security countermeasure will not occur when the cost of responding to a security threat is greater than the damage of the resulting threat [37]. This follows from security recommendations that suggest a weighted analysis be performed that considers the likelihood of the threat occurring, along with the expected consequences of the threat versus the expected cost of taking preventative measures [3]. This is similar to technology adoption literature, which shows that as the cost for using a technology increase, an individual becomes less likely to use the technology [38-40]. One study shows that cost is one of the greatest inhibitors of behavioral intention to use mobile commerce [39]. Also, medical clinics that have the smallest number of physicians sharing the cost of purchasing an electronic medical record (EMR) system are the least likely to implement such a technology [38]. Similarly, bank managers are concerned with economic considerations when deciding whether or not to implement a technologically complicated system [40]. Such findings from previous research suggest that as the perceived cost of invoking a coping response increases then the likelihood of implementing the response goes down. Following this, it is expected that increases in prevention cost will lead to less frequent data backups.

H5: Greater prevention costs will lead to running data backups less frequently.

Figure 2 presents a graphical representation of the hypotheses in this study, while Table 1 provides a comparison of original PMT items with PMT items in a security context. The next section discusses the methodology used to test the hypotheses.

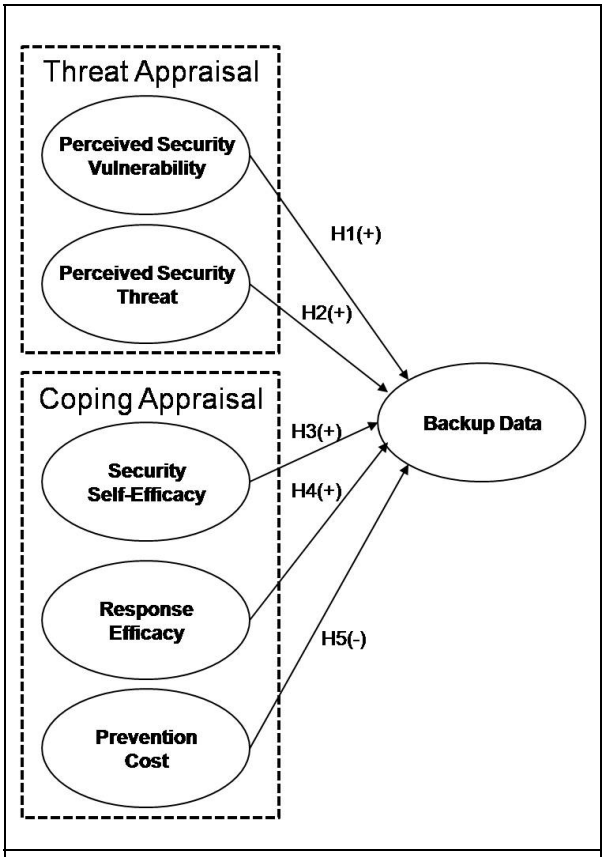

Figure 2. Behavioral security research model

3. Methodology

When hypothesizing theoretical models, not only is it important to test the hypotheses in the model, but it is also important to define and test the nature of the constructs in the model. Models can be composed of any combination of reflective, formative, and multi-dimensional constructs [41]. Petter et al. define the above constructs accordingly: Reflective constructs are *observed measures that are affected by underlying latent construct.* Formative constructs are *a composite of multiple measures where changes in the formative measures cause changes in the underlying construct.* Multi-dimensional constructs are *constructs with more than one dimension, with each dimension representing some portion of the overall latent construct and with each dimension, itself being either reflective or latent.*

Table 1. PMT in a security context

Original PMT Construct	PMT Construct in Security Context	Definition
Threat Appraisal	Security Threat Appraisal	An individual's assessment about the level of danger posed by a security event.
Coping Appraisal	Security Coping Appraisal	An individual's assessment of his ability to perform a given behavior and his confidence that a given behavior will be successful in mitigating or averting the potential loss or damage resulting from a threatening security event, at a perceived cost that is not too high.
Vulnerability	Perceived Security Vulnerability	An individual's assessment of the probability of a threatening security event occurring.
Severity	Perceived Security Threat	An individual's assessment of the severity of the consequences resulting from a threatening security event.
Self-Efficacy	Security Self-Efficacy	An individual's confidence in his/her ability to perform the recommended behavior to prevent or mitigate the threatening security event.
Response Efficacy	Response Efficacy	An individual's confidence that a recommended behavior will prevent or mitigate the threatening security event.
Response Cost	Prevention Cost	The opportunity costs – time, cognitive effort, financial – of adopting the recommend behavior to prevent or mitigate the threatening security event.

Table 2. Item framework.

Dimension	Item	Source
Perceived Security Vulnerabilities	I am at risk for losing information or files on my computer.	[42]
	It is likely that I will lose information or files on my computer.	
	It is possible that I will lose information or files on my computer.	
Perceived Security Threats	I believe that losing information or files on my computer would be a severe problem.	[42]
	I believe that losing information or files on my computer would be a serious problem.	
	I believe that losing information or files on my computer would be a significant problem.	
Security Self-Efficacy	I believe I have the ability to perform [*recommended response*].	[11, 30, 42]
Response Efficacy	Backing up my data works to prevent the loss of information or files on my computer.	[42]
	Backing up my data is effective at preventing the loss of information or files on my computer.	
	If I back up my data, I am less likely to lose information or files on my computer.	
Prevention Cost	Backing up data on my computer requires significant financial cost.	[20, 43]
	Backing up data on my computer requires a significant amount of time.	
	Backing up data on my computer requires significant cognitive effort (brain power).	

Previously validated measures exist for the independent variables in this study. Four of the independent variables are measured using the Risk Behavior Diagnosis Scale, which encompasses severity of threat, susceptibility to threat, self-efficacy and response efficacy [42]. Additionally, much work has been done in IS research developing a way to measure computer self-efficacy [11, 30]. PMT research regularly measures response cost [20, 43]. Relying on the previously validated instruments results in the questions to measure the items in this context (see Table 2). Perceived security vulnerability, perceived security threat, and response efficacy were measured as reflective constructs, while security self-efficacy, prevention cost, and the backing up of data were measured as formative

constructs. Security self-efficacy contained seven items, representing seven different security tasks that could be performed, prevention cost contained three items, representing three different costs associated with backing up data and backing up data contained three items, representing three different types of data that could be backed up.

3.1. Pre-Test and Pilot Study

Four Ph.D. students reviewed the resulting survey to identify unclear wording and determine the approximate amount of time each survey will take to complete. Modifications were made to the items based on feedback during the Pre-Test.

The pilot study was conducted by recruiting 24 graduate level business students in the same class and administering the survey to them. SmartPLS Version 2.0.M3 was used to analyze the reliability and validity of the items. It is necessary to use Partial Least Squares (PLS) to perform this process as the research model is composed of reflective and formative constructs. To test the reliability and validity of the items in the pilot study, a PLS algorithm was conducted. All constructs demonstrated acceptable reliability greater than 0.7. Validity analysis revealed that all of items loaded as expected.

3.2. Full Scale Survey

Finally, a large-scale survey was conducted. It is suggested that the use of PLS requires a sample size of 10 times either the number of structural paths to a particular construct in a model or 10 times the number of formative indicators to a particular construct [44]. The security self-efficacy construct has the greatest number of formative indicators at seven, suggesting it is necessary to have at least a sample size of 70. However, it is also necessary to conduct a power analysis to ensure that a large enough sample size is used. A power analysis based on previous PMT research [10], which found a medium effect size of .15, an alpha of .05, and power of .80, suggests that 97 responses are necessary to ensure enough power [45]. Data was collected by using paper and web-based surveys. Paper-based surveys were used for manual data collection at events, while web-based surveys were used to collect data from people within a business. Both event data collection and solicitations from businesses were used to ensure a large enough population for data analysis.

4. Data Analysis and Results

Online and paper-based versions of the survey were administered to participants. Different sources completed each version of the survey. The paper version of the survey was administered to attendees of a soccer tournament in Virginia, USA. Distribution of the online version of the survey occurred in a number of ways. Initially, data was collected by emailing a number of contacts of the researcher a request to participate in the survey and then forward on the request. Collection of additional data occurred through the distribution of a request to participate in the survey to subscribers of the graduate student listserv at Virginia Polytechnic Institute and State University. Finally, a number of small businesses disseminated a request to have their employees complete the survey. 112 surveys were received, 17 on paper and 95 online. Response rates varied by group and are approximated. Approximately 50 percent of the people approached at the soccer tournament completed the survey, while approximately 25 percent of the small business employees who received the survey responded and 3.5 percent of graduate students responded. Response rates are not estimated from the forwarding of the email as the total population it was sent to is unknown. These response rates are rather low, but expected. The response rate from the graduate listserv is consistent with previous Information Systems research using this particular source [46]. Previous security research found a response rate of 1.6% for a paper-based mail survey [47]. Research also shows that web-based surveys have a lower response rate than paper-based surveys [48].

Differences between online and paper responses, as well as between the responses collected from small businesses and at the sporting event were analyzed using independent sample t-tests. The samples did not display significant differences, so the following data analyses uses a combined sample.

After combining the samples, the data were tested for outliers and normality. Outliers can significantly alter the outcome of analysis. Outliers can occur due to errors of data entry, missing values, unintended sampling, and non-normal distribution [49]. Outliers were identified by proofreading the data for obvious data entry errors. This was followed by checking the data for missing values and then running statistical tests. A response was considered an outlier if it was more than three standard deviations away from the expected value of the variable [49]. All cases were within the suggested range.

Over half of the respondents are female (61.3%). The majority of respondents are Caucasian (81.3%).

The average age of respondents was 32.12 with a minimum age of 20 and a maximum age of 76. Respondents have been using computers for an average of 15.86 years with a minimum of five years and a maximum of 40. The average number of hours respondents spend on the Internet is 26.73 ranging from one hour to 100 hours. The average number of hours respondents spend on their computer is 34.23 ranging from two hours to 100 hours per week.

4.1. Measurement Model

The data was analyzed using Partial Least Squares (PLS), which is necessary when testing formative constructs because it allows for the proper identification of relationships in the model. This translates into a proper assessment of both the measurement model as well as the structural model [41]. The independent variables in this model are latent variables that measure the inferred values from a person's response about themselves. The dependent variable is a self-report of actual behavior.

Prior to testing the hypotheses in the proposed model, it is necessary to assess the accuracy of the measurement model. This process ensures that the measures are valid and properly reflect the theoretical constructs. The reliability, or the internal consistency, of the model is tested along with the convergent and discriminant validity of the measurement items. Reliability is assessed using Cronbach's Alpha and composite reliability. All of the constructs displayed satisfactory reliability above the 0.70 threshold [50].

Convergent and discriminant validity were assessed by examining whether items intended to measure one construct were more highly correlated with themselves or with other constructs. Items that loaded the most strongly on their own constructs were considered to have convergent validity. Convergent validity was also tested by calculating the Average Variance Extracted (AVE) for each construct, which is the amount of variance that a latent variable component captures from its indicators in relation to the amount due to measurement error. The AVE value for all constructs were above the recommended threshold of 0.50 [51], indicating good convergent validity of the items in each construct.

Discriminant validity was tested by assessing whether the AVE from a construct was greater than the variance shared with other constructs in the model [52]. The AVE is greater than the squared pair-wise correlation of the latent variables indicating satisfactory discriminant validity.

Discriminant validity was additionally assessed using the cross-loading method [52]. All the items loaded higher in their own columns than in the column for other constructs. Furthermore, when evaluating the items across rows, the items loaded most strongly on their intended constructs. Therefore, the measurements satisfy the criteria recommended by Chin [52].

For formative items it is necessary to ensure that they are not highly correlated with one another [41]. Each of the formative items in this study displayed VIF values of less than 3.3, which shows that they were not highly correlated with one another.

4.2. Structural Model

Based on the acceptable analysis of the measurement model, testing of the structural model and proposed hypotheses can ensue. The structural model was tested using SmartPLS to estimate the path coefficients, which calculates the strength of the relationships between independent and dependent variables. R-squared values were also estimated, in order to display the variance explained by the independent variables. The proposed hypotheses were tested using t-statistics for the standardized path coefficients, by specifying the same number of cases as existed in the dataset and bootstrapping 500 re-samples. One-tailed t-tests were used, as the hypotheses were all direction specific.

Figure 3 presents the results from running the model. Hypotheses 1, 2, and 5 were not supported, but significant findings were found in the opposite direction hypothesized for Hypotheses 1 and 2. Hypothesis 3 and 4 significantly explained backing up data on a regular basis. The variance in behavior explained for backing up data regularly was 47%.

5. Discussion

The model tested investigated the use of backing up software to protect files from being lost on a computer, studying direct relationships from perceived security vulnerability, perceived security threat, security self-efficacy, response efficacy, and prevention costs to the frequency of backing up data. Security Self-Efficacy and Response Efficacy both have a significant positive relationship in determining whether individuals backup data on their personal computer. This suggests that people will be more likely to backup the files on their personal computer as they gain confidence in their ability to secure their computer and in the effectiveness of running backups to prevent file loss. Kim [2] found that people who received security training were twice as likely to backup their data. This suggests that when people

receive training on security the likelihood they are backing up their data should increase. Future research could use an experiment to determine whether the increase in data backup is due to changes in security self-efficacy response efficacy or some other factors.

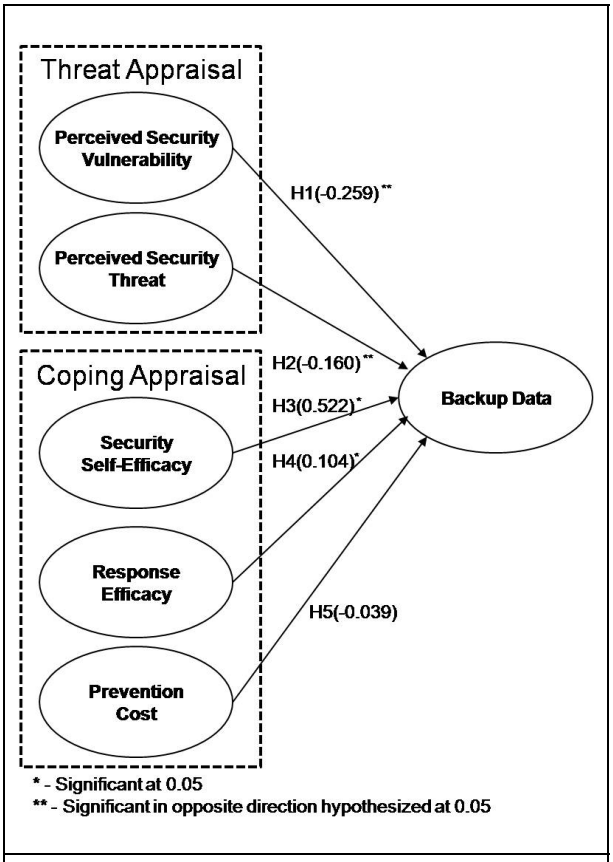

Figure 3. Research model results

Computer self-efficacy is a regularly studied construct within the information systems field [11] and these findings confirm the influence that this characteristic has on backing up data on personal computers. As research in the realm of information security moves forward, one avenue of research should be to explore what individual characteristics explain differences in people's security self-efficacy. To begin with, researchers could look at antecedents to computer self-efficacy found in previous research to determine if they apply within an information security setting. Researchers could then develop and test further theoretical explanations for what determines differences in security self-efficacy.

Perceived security vulnerability and perceived security threat had a significant relationship with backing up data, but in the opposite direction than hypothesized. This suggests that people who feel that they are vulnerable to losing files on their computer and that the threat is severe are less likely to backup files on their comptuer. These findings are contrary to the findings by Woon et al. [9], who found all the constructs except perceived vulnerability significantly impacted home wireless security. These studies investigated different dependent variables as well as different threats being protected by the behavior of interest, but did so studying security in an IS context. Even with these differences, it is interesting to note that there is no similarity in findings. This implies that the explanation of security behaviors is going to differ depending on the threat and behavior being studied. Further research is necessary to determine the true relationship between threats people are concerned about protecting themselves from when performing different security tasks.

The findings of Perceived Security Vulnerability and Threat in the opposite direction than hypothesized is an important finding for security researchers as it indicates that when people recognize they are vulnerable to a given threat, or that it is severe, they are less likely to be performing a task to protect from the threat. These findings are contrary to findings in the social psychology literature where increases in the threat appraisal process led to a greater likelihood to perform a recommended behavior [10, 20]. It is possible that this occurred due to the influence that perceived security vulnerability and threat had on the coping appraisal process, suggesting that the threat appraisal constructs are antecedents to the coping appraisal constructs and not directly related to the performance of security behaviors. Alternatively, those people who backup frequently perceive less risk because they have already done something to deal with the threat.

Prevention Cost not having a significant relationship with backing up data (H5) suggests that the costs individuals perceive to backing up their data are not significant enough to make a big difference on whether or not they do them. Future research could explore whether there are other costs associated with backing up data that impact whether it is done or if the cost associated with doing it is time specific and only applies when individuals first decide to begin backing up their data.

The findings that are contrary to the hypothesized relationships suggest that PMT may not be fully appropriate to explain differences in security behavior. To understand fully the relationship between security behaviors and the appraisal process people go through, future research could explore the process individuals go through further and gain an understanding of causality, either experimentally or

through a qualitative study. Experimentally, researchers could set up a study that manipulates the threat appraisal constructs and test the impact that changes have on the coping appraisal constructs compared to the individual security behaviors. Qualitatively, researchers could interview computer users to ferret out the relationship between a perceived threat and behaviors performed to mitigate the threat. If people are not performing the behaviors because they do not feel like they can perform the task or that the behavior will address the threat, it will confirm the findings in this study. It may also be that people who are less knowledgeable about a threat perceive the threat to be higher, but are less likely to act on to protect themselves. As further understandings of people's behavior are uncovered qualitatively, follow up studies can be conducted to empirically test the newly uncovered relationships between individual characteristics and behaviors.

6. Conclusion

This study utilized Protection Motivation Theory to empirically test why people backup files on their personal computer. The results showed that security self-efficacy and response efficacy positively influenced the backing up of data, while the threat appraisal constructs had a negative relationship with this behavior. While these latter findings were contrary to expectations, it does raise questions as to how a person's perception of threats interacts with their beliefs in their abilities to protect themselves from threats. This study illustrated the need to study this relationship further, in the context of backing up files to protect from file loss. However, future research could explore these relationships with a number of other combinations of threats and behaviors. Some potential relationships that may be particularly interesting in exploring is the use of anti-spyware software to prevent identity theft and the use of firewall software to prevent file loss.

7. References

[1] R. Richardson, "2008 CSI Computer Crime and Security Survey," Computer Security Institute2007 2008.

[2] E. B. Kim, "Information Security Awareness Status of Full Time Employees," *The Business Review, Cambridge,* vol. 3, p. 219, 2005.

[3] B. Karabacak and I. Sogukpinar, "ISRAM: information security risk analysis method," *Computers & Security,* vol. 24, p. 147, 2005.

[4] D. W. Straub, "Effective IS Security: An Empirical Study," *Information Systems Research,* vol. 1, pp. 255-276, 1990.

[5] S. J. Harrington, "The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions," *MIS Quarterly,* vol. 20, p. 257, 1996.

[6] A. Kankanhalli, H.-H. Teo, B. C. Y. Tan, and K.-K. Wei, "An integrative study of information systems security effectiveness," *International Journal of Information Management,* vol. 23, p. 139, 2003.

[7] M. Workman and J. Gathegi, "Punishment and ethics deterrents: A study of insider security contravention," *Journal of the American Society for Information Science and Technology,* vol. 58, p. 212, 2007.

[8] J. Choobineh, G. Dhillon, M. R. Grimaila, and J. Rees, "Management of Information Security: Challenges and Research Directions," *Communications of the Association for Information Systems,* vol. 20, pp. 958-971, 2007.

[9] I. M. Y. Woon, G. W. Tan, and R. T. Low, "A Protection Motivation Theory Approach to Home Wireless Security," in *Twenty-Sixth International Conference on Information Systems (ICIS)*, 2005, pp. 367-380.

[10] 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, pp. 407-429, 2000.

[11] G. M. Marakas, R. D. Johnson, and P. F. Clay, "The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time," *Journal of the Association for Information Systems,* vol. 8, p. 15, 2007.

[12] Y. Lee, J.-Y. Lee, and Y. Liu, "Protection Motivation Theory in Information System Adoption: A Case of Anti-Plagiarism System," in *13th Annual Americas Conference on Information Systems*, Keystone, CO, 2007.

[13] R. E. Crossler, F. Belanger, and W. Fan, "Determinants of Information Security End User Behavior," in *2006 Annualy Internation Workshop (WISA 2006) of the AIS Special Interest Group on Netowrk and Internet Security (SIG-SEC)* Milwaukee, WI, 2006.

[14] A. I. Nicolaou and D. H. McKnight, "Perceived Information Quality in Data Exchanges: Effects on Risk, Trust, and Intention to Use," *Information Systems Research,* vol. 17, p. 332, 2006.

[15] P. A. Pavlou and D. Gefen, "Building Effective Online Marketplaces with Institution-Based Trust," *Information Systems Research,* vol. 15, p. 37, 2004.

[16] J. Jia, J. S. Dyer, and J. C. Butler, "Measure of perceived risk," *Management Science,* vol. 45, p. 519, 1999.

[17] J. Lee and H. R. Rao, "Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: An exploratory study of government-citizens online interactions in a turbulent environment*," *Decision Support Systems,* vol. 43, p. 1431, 2007.

[18] S. Youn, "Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach," *Journal of Broadcasting & Electronic Media,* vol. 49, pp. 86-110, 2005.

[19] M. Keil, B. C. Y. Tan, K.-K. Wei, T. Saarinen, V. Tuunainen, and A. Wassenaar, "A cross-cultural study on

escalation of commitment behavior in software projects," *MIS Quarterly,* vol. 24, p. 299, 2000.
[20] K. Neuwirth, S. Dunwoody, and R. J. Griffin, "Protection Motivation and Risk Communication," *Risk Analysis,* vol. 20, pp. 721-734, 2000.
[21] A. Bandura, "Self-efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological Review,* vol. 84, pp. 191-215, February 1977 1977.
[22] D. Compeau, C. A. Higgins, and S. Huff, "Social cognitive theory and individual reactions to computing technology: A longitudinal study," *MIS Quarterly,* vol. 23, p. 145, 1999.
[23] M. H. Fagan, S. Neill, and B. R. Wooldridge, "AN EMPIRICAL INVESTIGATION INTO THE RELATIONSHIP BETWEEN COMPUTER SELF-EFFICACY, ANXIETY, EXPERIENCE, SUPPORT AND USAGE," *The Journal of Computer Information Systems,* vol. 44, p. 95, 2003.
[24] P. Stephens, "A DECISION SUPPORT SYSTEM FOR COMPUTER LITERACY TRAINING AT UNIVERSITIES," *The Journal of Computer Information Systems,* vol. 46, p. 33, 2005.
[25] T. Fenech, "Using perceived ease of use and perceived usefulness to predict acceptance of the World Wide Web," *Computer Networks and ISDN Systems,* vol. 30, pp. 629-630, 1998.
[26] Y. Lee, K. A. Kozar, and K. R. T. Larsen, "The Technology Acceptance Model: Past, Present, and Future," *Communications of the Association for Information Systems,* vol. 12, pp. 752-780, 2003.
[27] D. R. Compeau and C. A. Higgins, "Application of social cognitive theory to training for computer skills," *Information Systems Research,* vol. 6, pp. 118-143, 1995.
[28] R. D. Carlson and B. L. Grabowski, "The Effects of Computer Self-Efficacy on Direction-Following Behavior in Computer Assisted Instruction," *Journal of Computer-Based Instruction,* 1992.
[29] R. D. Johnson and G. M. Marakas, "Research Report: The Role of Behavioral Modeling in Computer Skills Acquisition: Toward Refinementof the Model," *Information Systems Research,* vol. 11, p. 403, 2000.
[30] D. R. Compeau and C. A. Higgins, "Computer self-efficacy: Development of a measure and initial test," *MIS Quarterly,* vol. 19, p. 189, 1995.
[31] V. Venkatesh, M. Morris, G. Davis, and F. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quarterly,* vol. 27, pp. 425-478, 2003.
[32] V. Venkatesh and F. D. Davis, "A model of the antecedents of perceived ease of use: Development and test," *Decision Sciences,* vol. 27, p. 451, 1996.
[33] M. A. Bolt, L. N. Killough, and H. C. Koh, "Testing the interaction effects of task complexity in computer training using the social cognitive model," *Decision Sciences,* vol. 32, pp. 1-20, 2001.
[34] A. Bandura, "Guide for constructing self-efficacy scales," in *Self-efficacy Beliefs of Adolescents*, 2001, pp. 7-37.
[35] J. C. Y. Lam and M. K. O. Lee, "Digital Inclusiveness - Longitudinal Study of Internet Adoption by Older Adults," *Journal of Management Information Systems,* vol. 22, p. 177, 2006.
[36] S. H. Chung, P. H. Schwager, and D. E. Turner, "An empirical of students' computer self-efficacy: Differences among four academic disciplines at a large university," *The Journal of Computer Information Systems,* vol. 42, p. 1, 2002.
[37] W. Lee, W. Fan, M. Miller, S. J. Stolfo, and E. Zadok, "Toward cost-sensitive modeling for intrusion detection and response," *Intrusion Detection,* vol. 10, pp. 5-22, 2002.
[38] J. L. Reardon and E. Davidson, "An organizational learning perspective on the assimilation of electronic medical records among small physician practices," *European Journal of Information Systems,* vol. 16, p. 681, 2007.
[39] J.-H. Wu and S.-C. Wang, "What drives mobile commerce? An empirical evaluation of the revised technology acceptance model," *Information & Management,* vol. 42, p. 719, 2005.
[40] K. E. Ghorab, "The impact of technology acceptance consideration on system usage, and adopted level of technological sophistication: An empirical investigation," *International Journal of Information Management,* vol. 17, p. 249, 1997.
[41] S. Petter, D. Straub, and A. Rai, "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly,* vol. 31, p. 623, 2007.
[42] K. Witte, "Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale," *Journal of Health Communication,* vol. 1, pp. 317-342, 1996.
[43] P. Sheeran and S. Orbell, "How confidently can we infer health beliefs from questionnaire responses?," *Psychology & Health,* vol. 11, pp. 273-290, 1996.
[44] W. Chin, "Partial least squares for IS researchers: an overview and presentation of recent advances using the PLS approach," in *International Conference on Information Systems*, Brisbane, Australia, 2000.
[45] J. Cohen, "A Power Primer," *Psychological Bulletin,* vol. 112, p. 155, 1992.
[46] L. Carter, "Political Participation in a Digital Age: An Integrated Perspective on the Impacts of the Internet on Voter Turnout," in *Accounting and Information Systems Department*. vol. Ph.D. Blacksburg, VA: Virginia Tech, 2006.
[47] A. G. Kotulic and J. G. Clark, "Why there aren't more information security research studies," *Information & Management,* vol. 41, p. 597, 2004.
[48] T. Shih and X. Fan, "Comparing Response Rates from Web and Mail Surveys: A Meta-Analysis," *Field Methods,* vol. 20, p. 249, 2008.
[49] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*. NY: Academic Press, 1969.
[50] J. Nunnally, *Psychometric Theory*. New York: McGraw Hill, 1978.
[51] C. Fornell and D. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research,* pp. 39-50, 1981.
[52] W. W. Chin, "The partial least squares approach to structural equation modeling," in *Modern Methods for Business Research*, G. A. Marcoulides, Ed. Mahway, New Jersey: Lawrence Erlbaum, 1998, pp. 295-33.