December 2005

A Protection Motivation Theory Approach to Home Wireless Security

Irene Woon
National University of Singapore

Gek-Woo Tan
National University of Singapore

R. Low
National University of Singapore

A PROTECTION MOTIVATION THEORY APPROACH TO HOME WIRELESS SECURITY

I. M. Y. Woon, G. W. Tan, and R. T. Low
School of Computing
National University of Singapore
Singapore
iwoon@comp.nus.edu.sg **tangw@comp.nus.edu.sg**
lowrentz@comp.nus.edu.sg

Abstract

Research in socio-technical factors in computer security has traditionally focused on employees and their work practice within the premises of the organization. However, with universal access to computing and the diverse means of connecting such devices to each another and to the global Internet, work carried out has shifted outside one central physical location to encompass a variety of possible points-of-access that include homes, modern cafés, and public libraries. Given the ubiquity of wireless devices used for last-hop access to the Internet from home, we look at the security of home wireless networks. In this work, we identify the variables that affect the decision of home wireless network users to implement security features on their networks. Our study is based on the protection motivation theory. A survey was conducted on 189 home users to identify and characterize predictors that differentiate between users who secure their home wireless networks and those who don't. Results of the analysis identified the following variables as significant: perceived severity, response efficacy, self efficacy, and response cost.

Keywords: Protection motivation theory, wireless security, computer security, logistic regression analysis

Introduction

Research in socio-technical factors in computer security has traditionally focused on employees and their work practice within the premises of the organization (Dhillion and Torkzadeh 2001; Galletta and Polak 2003; Siponen 2000). However, universal access to computing and the diverse means of connecting such devices to each another and to the global Internet has significantly altered the location-based work paradigm. To examine its impact on information security, we consider two sets of users: (1) organizational employees who use the organization's computer network resources, and (2) the academic researcher and his students. In each case, work carried out has shifted outside one central physical location to encompass a variety of possible points-of-access that include homes, modern cafés, public libraries, and even modes of transport such as trains. This means that prior assumptions about information security valid under the old model of work pattern may no longer be tenable. Newer work practices and environments where work is carried out may have introduced newer threats or weaknesses, or invalidated prior assumptions for security. Therefore, these newer environments should be reevaluated for information security strengths and weaknesses. This may result in newer security policies needed to realize the same level of security. However, because of the breadth and scope of the study needed to answer this question in sufficient depth, we focus in this paper on one significant aspect of the newer environment, namely the last-hop wireless access from the home.

The demarcation between work at-work and work at-home is rapidly and increasingly dissolving. Organizations increasingly offer employees the ability to work from home, and large organizations frequently have project members that live in different geographic areas. Furthermore, as time-to-market has become critical, employees are encouraged to work from home. In this new work model, home is at least as important a location as the office where work happens. A similar situation exists in the academic world, in disciplines such as mathematics and information systems. Researchers in these disciplines do not need to conduct

physical experiments that require their physical presence to manipulate equipment or carry out experiments. Instead, the software applications that they use can easily be installed on notebooks and desktops. Indeed, the favored work pattern of these academic researchers is to work from notebooks that give them the portability to easily carry their work between office and home. This convenience is further increased by the ubiquitous access to computing devices connected by wireless networks. This facilitates access, but at the same time adds additional "links" to the chain of access to data and computing.

With the premise of ubiquitous wireless access in every walk of life, it then becomes important to study how well employees, academic researchers, and students protect computing systems at home that they use directly or indirectly for their work or to access their parent organization's network and data repositories. If the premise that "security is as strong as its weakest link" is accepted, then we argue that modern work patterns have (likely) shifted the weakest link to an amorphous periphery that at least includes employee's, researcher's, or student's homes. Now we consider how these people at home connect to the organization's network and where insecurity can be introduced.

A U.S. Census Bureau survey (2000) show that 41 percent of households have Internet access. Broadband internet access in the home and the use of wireless local area networks (WLANs) to share home broadband Internet connections skyrocketed in 2004 and are expected to triple in the next 5 years (Ipsos Insight 2005). The popularity of wireless networks at home can be explained in terms of its convenience and flexibility. Unlike wired networks, wireless networks use radio signals to communicate. This allows users easy as well as multiple access to the Internet from anywhere in their home, and to share files and resources like printers. However, because radio signals travel outside the user's network, other wireless devices can pick up unprotected signals and either connect to the user's network (uninvited) or capture information being sent across it (i.e., sniff data such as e-mail messages, passwords, user names, etc.). Using this information, a hacker may be able to access and modify the user's data, access the user's organizational resources, hijack the home-user's wireless network, or remotely control the unprotected home computer to attack critical infrastructures (Office of Homeland Security 2002). The CSI/FBI Computer Crime and Security Survey (Gordon et al. 2004) reports that damages arising from abuse of wireless networks alone amounted to USD10 million in 2004. The recommendations given to minimize security risks in wireless networks include restricting access, encrypting data, and protecting the service set identifier (SSID) (McDowell et al. 2005). Although the dangers from wireless hacking are well documented (Arbaugh et al. 2002; Thomas 2004), several studies have shown that many users of WLANs make no effort to enable security measures on their networks (Mimoso 2003; Poulsen 2001).

Given the ubiquity of wireless devices used for last-hop access to the Internet, we tackle the following slice of the overall problem. We attempt to discover those cognitive factors that differentiate between people who secure their wireless access devices from those who do not make such efforts. The results of the study can then be used to devise measures that ameliorate the danger of using unprotected wireless access. The factors considered in this study are proposed by the protection motivation theory (Rippetoe and Rogers 1987; Rogers 1975, 1983). This theory has been used extensively for successfully predicting behavior in the fields of health (Hall et al. 2004; Kanvil and Umeh 2000; Searle et al. 2000) and social research (Allen 1993; Axelrod and Newton 1991; Campis et al. 1989).

Theoretical Background

The protection motivation theory (PMT) measures the coping behavior of a person when he/she is informed of a threatening event (e.g., cigarette smoking is linked to lung cancer) (Rippetoe and Rogers 1987). This behavior is directly influenced by the coping response which refers to a person's willingness to perform a recommended behavior (this could be to quit smoking totally, reduce the number of cigarettes per day, etc.). The coping response is the net result of the person's evaluation of the threat appraisal and coping appraisal.

Threat appraisal refers to a person's assessment of the level of danger posed by the threat. It consists of *perceived vulnerability* (the person's assessment of the probability of the threatening event), *perceived severity* (the severity of the consequences of the event), and *rewards* (*intrinsic* and *extrinsic rewards* of ***not*** adopting a recommended coping response). For example, the rewards for continued smoking (i.e., not stopping smoking) are psychological pleasure and peer approval (Prentice-Dunn and McClendon 2001).

The second cognitive process, coping appraisal, refers to the person's assessment of his ability to cope with and avert the potential loss or damage resulting from the danger. It consists of *self efficacy* (the person's confidence in his/her own ability to perform the recommended behavior), *response efficacy* (the efficacy of the recommended behavior), and *response cost* (the perceived opportunity costs—monetary, time, effort—in adopting the recommended behavior). In the smoking example, self efficacy refers

to the person's confidence in his/her ability to quit smoking, response efficacy to the health benefits of not smoking, and response cost to the withdrawal symptoms that the smoker suffers when he/she stops smoking.

Research Model

We adapt our research model (see Figure 1) from the 1987 version of PMT in two ways. The first is that as we are doing a cross sectional rather than a longitudinal study; we do not investigate the *coping response* construct (i.e., the person's intention to adopt a recommended behavior). We consider only behavior and model it as a binary variable distinguishing between home users who have enabled security features and those who have not. Regarding the *rewards* construct, we find that the person does not derive any *intrinsic* pleasure nor *extrinsic* approval for not enabling security features. Hence this construct was not included in the model.

Recommended Behavior

Behavior refers to the person's actual response to a recommended behavior and is the net effect of threat appraisal and coping appraisal. In this study, the recommended behavior is to enable the security features on the home wireless network.

Threat Appraisal

The two components of this construct are *perceived vulnerability* and *perceived severity*.

Perceived vulnerability refers to a person's assessment of his/her own probability of being exposed to a threat (Rogers 1983). In this study, threat refers to unauthorized access to the user's wireless networks. Many studies (Rippetoe and Rogers 1987; Wurtele 1988; Wurtele and Maddux, 1987) have shown a significant main effect of *perceived vulnerability* on coping response, with people who exhibit high levels also showing increased intention to adopt a recommended coping response. Thus we hypothesize that

> *H1: Perceived vulnerability will be significant in determining if a respondent running a home wireless network will enable security measures.*

Perceived severity measures the magnitude of the consequences to an individual if the threat succeeds (Milne et al. 2000). In this context, loss of personal information and online identity are considered as possible consequences. Previous health related studies (Maddux and Rogers 1983; Milne et al. 2000) found *severity* to be the least significant of the four cognitive mediating factors.

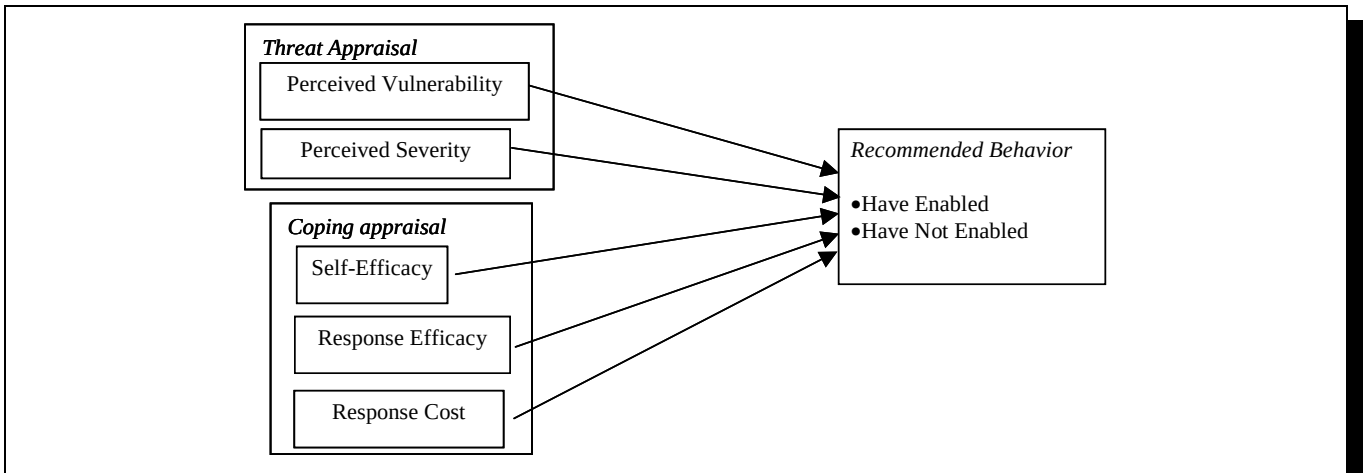

Figure 1. Research Model

On the other hand, best practices in IT security management advocate a risk assessment approach to managing security risks (ISO/IEC 1998; Stoneburner et al. 2002). According to this approach, action to reduce the level of risk should be taken when they (risks) become unacceptably high. Since risk levels will increase when the severity of the loss from a threat increases, we hypothesize that

> *H2: Perceived severity will be significant in determining if a respondent running a home wireless network will enable security measures.*

Coping Appraisal

The three components in this construct are *response efficacy*, *self efficacy*, and *response cost*.

Response efficacy is defined as the belief that a recommended coping response will be effective in protecting the self or others from a threat. Guidelines from cyber-security experts such as US-CERT (McDowell et al. 2005) advocate that home users take measures such as filtering media access control addresses, changing the default service set identifier, and enabling encryption on WLANs to secure home wireless networks. Past studies have shown positive correlation between response efficacy and coping response ranging from significant (Maddux and Stanley 1986) to medium (Wurtele 1988) effects. Thus we hypothesize that

> *H3: Response efficacy will be significant in determining if a respondent running a home wireless network will enable security measures.*

Self efficacy is defined as the expectancy of a person's capability in performing a recommended coping behavior (i.e., enabling the security features in this case). In studies based on self efficacy theory (Bandura 1977), self efficacy has been found to have a significant positive correlation on behavioral change (Bandura et al. 1980; Condiotte and Lichtenstein 1981). In addition, significant correlations between *self efficacy* and *coping response* have also been found in a wide range of PMT related studies (Fruin et al. 1991; Maddux and Rogers 1983; Maddux and Stanley 1986). A quantitative study by Milne et al. (2000) has also shown that among all PMT independent variables, self efficacy has the most robust effect on intention. Hence, we hypothesize that

> *H4: Self efficacy will be significant in determining if a respondent running a home wireless network will enable security measures.*

Response costs are the costs perceived by an individual in performing a recommended coping behavior and may include monetary expense, inconvenience, difficulty, and the side effects of performing the coping behavior. Support for the link between response cost and coping response is given by Helmes (2002) and Neuwirth et al. (2000). Response cost in our case translates to slower response costs due to encryption overhead and the inconvenience of changing the encryption key regularly. Therefore, we hypothesize that

> *H5: Response cost will be significant in determining if a respondent running a home wireless network will enable security measures.*

Research Methodology

The model was tested using survey methodology to improve the generalizability of results (Dooley 2001). First a draft instrument was constructed by adapting scales from previous literature to measure the constructs. The instrument was pretested with three experts in computer security to ensure its content validity. An interview was conducted with each expert and changes suggested by the expert were reflected in the instrument, which was then used for the next interview, according to the procedure in Straub (1989). Items were added, reworded, and deleted in this pretest. To assess the construct validity of the various scales and to identify any ambiguous items, judges were asked to sort the various items into construct categories according to the procedure in Moore and Benbasat (1991). A total of two sorting rounds were conducted until items were stable and a high item placement ratio and acceptable Cohen's kappa (> 0.65) was achieved. This resulted in a 31-item questionnaire.

Table 1. Demographic and Knowledge Profile of Respondents

Descriptor	Percentage	Descriptor	Percentage
Gender		Security Feature Enabled	
• Male	60%	• Yes	60%
• Female	40%	• No	40%
Profession		Knowledge Quiz Scores	
• Academic	55%	• High knowledge	39.2%
• Industry	45%	• Low knowledge	60.8%

Data Collection

Besides the 31-item survey instrument, we also administered a 7-item knowledge quiz. This quiz gave us an objective indication of the respondent's knowledge of the domain, which we used to validate the perceptual measures on *self efficacy*.

The questionnaire and a 7-item knowledge quiz was administered to the respondents at a large university. We checked the respondents for the ownership of home wireless networks by asking them for the brand of their wireless router. Of these respondents, 45 percent are full-time employees who were pursuing part-time postgraduate diplomas or degrees as well as those pursuing continuing courses; 55 percent of the respondents were academic researchers who are employees of the university as well as students at the same institution. The survey consists of three sections: a demographic section, the main research instrument, and a knowledge quiz. To encourage participation in the survey, a small monetary incentive was provided to all respondents. All questionnaire items were measured using a seven-point Likert scale. A total of 215 responses were collected. Univariate outlier analysis reduced the sample size by 26, leaving a final sample of 189 sets of data for analysis. The profile of the survey respondents is shown in Table 1.

Knowledge Quiz

Knowledge has been used in a variety of studies to measure a respondent's awareness regarding a given subject matter, and its subsequent effect on preventive or risky behavior (Lukwago et al. 2003; Nyamathi et al. 1993). In this study, the respondent's knowledge of network security and specific actions to take to defend the wireless network was measured by a seven-item quiz designed with the help of two professors who taught computer security to undergraduates in the Computer Science Department. Cluster analysis was used to distinguish between the levels of knowledge of the respondents. The results showed that the low-knowledge group had a mean score of 1.67 out of a maximum of 7 while the high-knowledge group had a mean score of 5.2.

Data Analysis and Results

Reliability and Validity

With the data gathered, the individual constructs were tested for reliability, convergent, and discriminant validity. Reliability was tested using Cronbach's alpha (Cronbach 1951). Nunnally (1978) suggested that the reliability of the constructs be above 0.70 but also mentioned that reliabilities of 0.50 to 0.60 would suffice in early stages of research. Hence, for this study, reliability scores of more than 0.50 were considered acceptable.

Subsequently, the items were tested for validity using factor analysis with principal components analysis and varimax rotation. Convergent validity was assessed by checking loadings to see if items for the same construct correlate highly among themselves. Discriminant validity was assessed by examining the factor loadings to see if items loaded more highly on their intended constructs than on other constructs (Cook and Campbell 1979). Loadings of 0.45 to 0.54 are considered fair, 0.55 to 0.62 good, 0.63 to 0.70 very good, and above 0.71 excellent (Comrey 1973).

Next, reliability analysis was combined with discriminant and convergent validity analysis to eliminate items that had (1) low item-item and item-scale correlation (< 0.5), (2) increased alpha if deleted, or (3) cross-loaded onto more than one factor. This process resulted in the elimination of 7 items. However, before these items were eliminated, checks were made to ensure that content validity of constructs was not compromised. The refined items are given in Table 2.

Table 2. Final Items		
Construct	**Items**	**Source**
Perceived Vulnerability	• I could be subjected to a malicious wireless hacking attempt (PerVul1) • I feel that I could be vulnerable to wireless hacking (PerVul2)	Cox et al. 2004; Milne et al. 2002
Perceived Severity	• Having my online identity stolen as a result of wireless hacking is a serious problem for me (PerSer1) • E-mail eavesdropping resulting from wireless hacking is a serious problem for me (PerSer2) • Losing data privacy as a result of wireless hacking is a serious problem for me (PerSer3) • Loss resulting from wireless hacking is not a serious problem for me (PerSer4)	Cox et al. 2004; Milne et al. 2000; Milne et al. 2002
Response Efficacy	• Enabling security measures on my home wireless network will prevent hackers from stealing network bandwidth (ResEff1) • Enabling the security measures on a home wireless network is an effective way of deterring hacker attacks (ResEff2) • Enabling security measures on my home wireless network will prevent hackers from gaining important personal or financial information (ResEff3) • Enabling security measures on my home wireless network will prevent hackers from stealing my identity (ResEff4)	Self Developed
Self efficacy	• It would be easy for me to enable security features on the home wireless network by myself (SelfEff1) • I could enable wireless security measures if there was no-one around to tell me what to do as I go along (SelfEff2) • I could enable wireless security measures if I only had manuals for reference (SelfEff3)	Compeau and Higgins (1995)
Response Cost	• The cost of enabling security measures decreases the convenience afforded by a home wireless network (ResCost1) • There are too many overheads associated with trying to enable security measures on a home wireless network (ResCost2) • Enabling security features on my wireless router would require considerable investment of effort other than time (ResCost3) • Enabling security features on a wireless router would be time consuming (ResCost4)	Fruin et al. 1991; Milne et al. 2002; Tanner et al. 1991

Table 3. Reliability of Constructs		
Construct	**No of Items**	**Cronbach Alpha**
Perceived Vulnerability (PerVul)	2	0.67
Perceived Severity (PerSer)	4	0.80
Response Efficacy (ResEff)	4	0.84
Self efficacy (SelfEff)	3	0.82
Response Cost (ResCost)	4	0.74

The reliability values for the final instrument is given in Table 3 and all constructs exceeded the minimum acceptable value of 0.5.

Factor analysis of the final instrument yielded five components with eigenvalues above 1 (see Table 4). All questions had at least good loadings on their intended constructs. These five components explained 66.88 percent of total cumulative variance and give an indication of the low level of collinearity between the independent variables of our study, since all items load cleanly into their respective construct categories.

Table 4. Validity of Constructs					
	Component				
	1	**2**	**3**	**4**	**5**
PerVul1	.11	.14	.19	.05	.79
PerVul2	.16	.03	.08	-.07	.85
PerSer1	-.03	.78	.02	.00	-.04
PerSer2	.13	.76	.13	.03	.04
PerSer3	.11	.75	.06	-.02	.23
PerSer4	.21	.81	-.03	.00	.02
ResEff1	.76	.04	-.03	.12	.23
ResEff2	.79	.04	.20	.06	.05
ResEff3	.85	.13	.01	-.00	.07
ResEff4	.81	.19	.00	-.01	.01
SelfEff1	.01	.06	.84	-.20	.23
SelfEff2	.15	.12	.78	.01	-.02
SelfEff3	.00	-.01	.85	-.19	.14
ResCost1	-.15	.07	.14	.73	.09
ResCost2	.03	.01	-.10	.82	.08
ResCost3	.18	.03	-.27	.71	-.13
ResCost4	.12	-.08	-.18	.67	-.10
Eigenvalues	3.74	2.83	1.98	1.67	1.13
Variance	22.00	16.68	11.67	9.83	6.69
Cumulative Variance	22.00	38.68	50.36	60.19	66.88

Testing the Relationships

The relationships given in the research model (Figure 1) are tested using logistic regression. The independent variables are *perceived vulnerability, perceived severity, response efficacy, response cost* ,and *self efficacy.* As each individual variable consists of multiple items, a summated scored across the items is taken as the score for that variable. The dependent variable is behavior which is a binary measure of yes/no depending on whether security features are enabled.

Logistic Regression

Regression is a statistical analysis method whereby the independent variables in a regression model are able to distinguish between pairs of groups (Hair et al. 1998). Although discriminant analysis can also be used for this study, logistic regression has several advantages. First, logistic regression does not rely on the strict assumptions of multivariate normality and equal variance, assumptions that are not met in many real life situations (Hosmer and Lemeshow 1989). Second, logistic regression is preferred because of its similarity to regression, with the ability to incorporate nonlinear effects and a wide range of diagnostics functions, including variance inflation factor (VIF) and tolerance diagnostics (Neter et al. 1996). Finally, logistic regression does not require the dependent variable to be normally distributed, the most important reason for choosing logistic regression as our analysis tool. We also fulfill the recommended level of 10 sets of data per independent variable (Hosmer and Lemeshow 1989) for Logistic Regression analysis.

To obtain reliable results from the logistic regression analysis, independent constructs must not be multicollinear, meaning two or more independent constructs should not have a high level of correlation with each other (Hair et al. 1998). A definitive indication of multicollinearity can be drawn from the VIF, with VIF values ranging from 1 to 1.8 being indicative of non-multicollearity (Gammie et al. 2003). As all the independent variables in our model have VIF values within the accepted range (see Table 5) they are not multicollinear.

Table 5. Collinearity Statistics for All Independent Variables				
Variables	**t**	**Sig.**	**Tolerance**	**VIF**
Perceived Vulnerability	.30	.77	.95	1.05
Perceived Severity	2.52	.01	.91	1.10
Response Efficacy	2.44	.02	.91	1.09
Self Efficacy	3.18	.00	.88	1.14
Response Cost	-2.95	.00	.87	1.15

Table 6. Model Fitting Information				
Model	**-2 Log Likelihood**	**X^2**	**df**	**Sig.**
Final	209.55	42.58	5	.00

Table 7. Parameter Estimates									
Behavior		**B**	**Std Error**	**Wald**	**df**	**Sig**	**Exp(B)**	**-2 Log likelihood**	**X^2**
NOT ENABLED	Perceived Vulnerability	.01	.06	.05	1	.82	1.01	209.61	.05
	Perceived Severity *	.11	.04	6.27	1	.01	1.12	216.02	6.46
	Response Efficacy *	.12	.05	5.66	1	.02	1.13	215.59	6.03
	Self efficacy *	.17	.06	8.82	1	.00	1.19	218.96	9.41
	Response Cost *	-.14	.05	8.34	1	.00	.87	218.71	9.16

Reference Category = Enabled Group, * $p < 0.05$

The presence of an overall relationship between the dependent variable and combination of the independent variables is based on the statistical significance of the final model χ^2 in the SPSS table named "Model Fitting Information." The probability of the model χ^2 (42.58) is 0.00 (see Table 6), less than or equal to the level of significance of 0.05. While the model χ^2 assesses the overall logistic model, it does not tell us if particular independent variables are more important than others. This can be done by looking at the information on the parameter estimates given in Table 7. All relationships between the independent variables except *perceived vulnerability* and behavior are significant.

Exp(B) is the odds ratio that assesses the risk of a particular outcome. In this study, it shows the likelihood of a respondent who has not secured his home wireless network, securing it. The table shows that *self efficacy* has the highest odds (1.19-1 = 19%) versus *response cost* (1-.87 = 13%) *response efficacy* (1.13-1 = 13%), and *perceived severity* (1.12-1 = 12%) of a respondent who has not secured his home wireless network doing it. This can be interpreted to mean that we may be able to get a user to secure his networks if we are able to promote the user's self efficacy or convince the user of effectiveness of the security measures or reduce the response cost of the security measures. Note that *response cost* has a negative relationship with behavior as reducing the response cost will increase the likelihood of the respondent performing the recommended behavior.

Table 8. Classification Table			
Observed	**Predicted**		
	Enabled	Not Enabled	Percent Correct
Enabled	95	21	81.9%
Not Enabled	35	38	52.1%
Overall Percentage	68.8%	31.2%	70.4%

Table 9. Case Processing Summary			
		N	**Marginal %**
Behavior	Enabled	116	61.4%
	Not Enabled	73	38.6%
Valid		178	100.0%

Table 10. Summary of Findings		
Hypothesis	**Significance**	**Result**
Perceived vulnerability will be significant in determining if a respondent running a home wireless network will enable security measures	.82	Not Supported
Perceived severity will be significant in determining if a respondent running a home wireless network will enable security measures	.01	Supported
Response efficacy will be significant in determining if a respondent running a home wireless network will enable security measures	.02	Supported
Self efficacy will be significant in determining if a respondent running a home wireless network will enable security measures	.00	Supported
Response cost will be significant in determining if a respondent running a home wireless network will enable security measures	.00	Supported

To accurately assess the utility of the regression model, we compare predicted group membership (see Table 8) to known membership (see Table 9). To determine if our model is useful in prediction, the classification percentage of 70.4 percent (see Table 8) has to exceed the chance accuracy rate by 25 percent (Hand et al. 2001). The chance accuracy rate is calculated by summing the squared value of the proportion of each case in the dependent variable (see Table 9), then multiplying that value by 1.25. Since the minimum model acceptance rate is calculated to be 0.65 ($(0.614^2 + 0.386^2) * 1.25$), which is less than 70.4 percent, the classification accuracy criterion for this regression model is accepted.

Conclusions from the logistic regression are summarized in Table 10, showing that all of the proposed hypotheses except H1 are supported

Discussion and Findings

This section discusses the observations and key findings with respect to the hypotheses of this study and suggests possible implications that the results of this study have in theory and practice. The regression model had classification rates that are higher than its respective *proportion by chance accurate rates*, indicating an acceptable level of predictive power for the model at 70.4 percent. Analysis also shows that four out of the five proposed hypotheses were supported. Our findings did not support our hypothesis that *perceived vulnerability* would be a significant predictor of behavior (H1). This is similar to the finding by Plotnikoff and Higginbotham (2002), who attribute the lack of positive association to substantial differences in which a person perceives different health threats. This explanation may also be used to explain the situation here. Although the media, mainstream newspapers, and publications report security breaches, they usually do not specifically highlight if these breaches arise from the use of undefended wireless networks. In contrast, virus attacks feature prominently in the news. Taken together with the results of the other independent variables, we can also explain that a person who feels vulnerable may not take action to avert the danger as he does not feel he is able to do it (*self efficacy*).

All of the other four independent variables were found to have significance in influencing the decision to enable security features. Table 11 shows the effect sizes of each of these variables using Cohen's ***d*** statistic (Cohen 1988). It is generally accepted that 0.2 constitutes a small effect size, 0.5 is considered moderate, and 0.8 is considered as a large effect size. The magnitude of the effect sizes indicates that the people who have not enabled security wireless tend to have greatest concern about self efficacy (effect size = 26.9).

Table 11. Effect Sizes		
Behavior		**Effect Size**
NOT ENABLED	Perceived Severity	15.4
	Response Efficacy	14.7
	Self efficacy	26.9
	Response Cost	13.2

Table 12. Knowledge Versus Security State					
Count		**Not Enabled**	**Own Enabled**	**Others Enabled**	**Total**
Cluster Number of Cases	Low Knowledge	60	15	41	116
	High Knowledge	13	47	13	73
Total		73	62	54	189

Self efficacy was found to be a statistically significant predictor (H4); findings are consistent with those of several previous studies (Fruin et al. 1991; Maddux and Rogers 1983; Maddux and Stanley 1986). We expected that *self efficacy* would be linked to a respondent's knowledge and this was confirmed by the results of the Spearman correlation analysis, which showed that the correlation between *self efficacy* and knowledge is good and significant ($r = 0.58$, $p = 0.00$). A further analysis into this link was performed by a considering each respondent's answer as to whether he/she enabled the security features themselves. From Table 12, we see that those who secure their wireless networks on their own ("own enabled" group) possess higher levels of knowledge compared to those who had others secure it for them ("others enabled" group). Although the "others enabled" group do not have required knowledge, they are motivated enough to get others to do the job for them.

Response efficacy was found to be a statistically significant predictor (H3); findings are consistent with those of several previous studies (Maddux and Stanley 1986; Wurtele 1988). Similar to studies by Neuwirth et al. (2000) and Helmes (2002), *response cost* (H5) was also found as a significant predictor of *behavior*. However, unlike existing studies in the health domain (Maddux and Rogers 1983; Milne et al. 2000), *perceived severity* (H2) was found to be a significant predictor. A possible explanation could be that the severity of health threats differs according to the genetic makeup of the person or other personal characteristics such as age or occupation (e.g., alcohol abuse may be more detrimental to a person who has a liver problem). However, in computer security, the impact is more uniform.

In our questionnaire, respondents who did not enable the security features were directed to answer two questions regarding their intention:

1. I intend to take some form of precaution against wireless hacking.
2. I intend to do nothing as I am unlikely to be a target of wireless hacking attempts.

Based on these two questions, K-means clustering was used to divide the "not enabled" group into two clusters. There were 23 respondents in the first cluster and 50 in the second cluster. Pearson correlation analysis (see Table 13) of these two groups and the group who had others enable the security features on their home wireless yielded more insights.

Table 13. Correlations of Three Subgroups			
	Intend to Do Nothing (N = 23)	**Intend to Take Precaution (N = 50)**	**Others Enable (N = 54)**
Perceived Severity Sig	-.18 ** .01		
Response Efficacy Sig	-.20** .00		.21** .00
Self efficacy Sig		-.29** .00	-0.29** .00
Response Cost Sig		.19** .00	

*Correlation is significant at the 0.01 level

Respondents who intend to do nothing may be persuaded otherwise if they can perceive that the impact of wireless security breaches may affect them indirectly and not just directly or if they can be convinced that enabling the security features will protect them. Respondents who have had other people enable their security settings for them are those who recognize the threat but do not feel comfortable doing the job themselves, as seen from the *self efficacy* correlation. This explanation is also consistent with the result shown by the *response efficacy* correlation. Since these respondents have low levels of knowledge, they do not know if the recommended measures will be effective. Thus for this group of people, specific step-by-step instructions and their rationale issued by CERT teams may be beneficial. Since *response cost* is negatively related to *behavior* (see Table 7), the *response cost* correlation is interpreted as the group intending to take precaution will do so if *response cost* is reduced; a commonly held opinion by most end-users is that security should be as transparent as possible. *Self efficacy* is also a barrier to enabling security settings for this group, as seen by the negative correlation.

In summary, the results of our research are somewhat consistent with the findings of previous studies (Cox et al. 2004; Wurtele 1988; Wurtele and Maddux 1987) that found significant main effects for coping appraisal but not threat appraisal variables. We determine that educating home wireless network users about the vulnerability that they are exposed to from wireless hacking may not be the most effective way of getting them to secure their networks. However, we establish that *perceived severity* has a significant effect on behavior. This means that although they do not think that they are likely targets, overall they perceive that the impact of a security breach would have a detrimental impact on them (e.g., slow response from the Internet).

For the factors that we found significant, we conducted a more in-depth analysis by clustering the "enabled" group into the "own enabled" the "others enabled" group and the "not enabled" group into "intend to do nothing" group and "intend to take some precaution" group. This finer level of analysis produced interesting findings and implications for practitioners. Although different groups of users have different concerns that have to be addressed differently, the findings suggest that *self efficacy* is a common factor that needs to be addressed. Self efficacy is usually promoted through education and training programs but as these are home users, a more effective way would be to deliver customized installation material at the point of sale or possibly to refer users to websites that give a step-by-step installation procedure. Currently, the user guides given are daunting to a novice as they are comprehensive and cover all platforms and possibilities of connection. In addition, CERT worldwide could host training sites that show the users what to do and why they should do it. *Response efficacy,* which is the concern of those in the "others enabled" group, could be addressed this way as well. Finally, it would appear that users who "intend to take precautions" feel that time and effort to secure their networks is challenging. This suggests that manufacturers would have to automate the set-up procedures further or provide more intuitive interfaces to the set-up programs.

Limitations and Implications for Research

This study explored the cognitive psychological factors that influence the decision of home wireless network users to implement security features on their wireless networks. We adapted our research model from the protection motivation theory and examined prior research in order to formulate a research instrument that allowed us to measure *perceived vulnerability, perceived severity, self efficacy, response efficacy,* and *response cost*. We built and analyzed the regression model from the data collected from a survey of 189 home users. This number represents only a small fraction of the total number of home users. As such, the results and findings from this research would need to be validated by enlarging the sample size. In particular, we would need to ensure that we have an equal number of samples from each set of users (employees and researchers) and that the composition of the samples in each subgroups ("others enabled," "intend to do nothing," "intend to take precaution") is uniformly distributed.

Although our PMT-based model is largely successful in predicting behavior, further research could examine other factors to increase its explanatory power. Of particular interest would be organizational security policies regarding access from out-of-office and the respondent's general computer security attitude (e.g., whether he installs anti-virus protection or a firewall on his home computer). Another avenue of exploration would be to include situational factors such as existing legal sanctions and the home user's past experiences with security breaches.

Conclusion

This research is a preliminary effort to examine the phenomena of employees and researchers working out-of-the office, accessing organizational networks and resources, and the impact on security. In particular, we focused on the security of wireless access from home. We use the protection motivation theory as our theoretical base as it is intuitively appealing and has been successfully

applied to health threats. As part of the empirical validation of PMT, a survey instrument was developed to measure the independent predictors of behavior. The final instrument was used to collect responses from different sets of home users. We applied logistic regression analysis to the data as the dependent variable is dichotomous. We found that, overall, *self efficacy*, *response efficacy*, *response costs*, and *perceived severity* were the most significant predictors of a user's behavior. Our regression model had a hit ratio of 70.4 percent. Our research also yielded unexpected results, finding perceived severity to be significant in predicting behavior, a finding that is inconsistent with health-related studies. This validates risk management guidelines suggested by best practices in IT security management. Implications for practitioners include the need to make security know-how easier, more accessible, and more transparent to the user. Implications for research focus on how the model can be further validated and extended.

References

Allen, B. "Frightening Information and Extraneous Arousal: Changing Cognitions and Behavior Regarding Nuclear War," *Journal of Social Psychology* (133), 1993, 133, pp. 459-467.

Arbaugh, W. A., Shankar, N. Wang, J., and Zhang, K. "Your 802.11 Network Has No Clothes," *IEEE Wireless Communications Magazine* (9), December 2002, pp. 44-51.

Axelrod, L. J., and Newton, J. W. "Preventing Nuclear War: Beliefs and Attitudes as Predictors of Disarmist and Deterrentist Behavior," *Journal of Applied Social Psychology* (21), 1991, pp. 29-40.

Bandura, A. "Self Efficacy: Toward a Unifying Theory of Behavioral Change," *Psychological Review* (84), 1977, pp. 191-215.

Bandura, A., Adams, N., Hardy, A., and Howells, G. "Tests of the Generality of Self Efficacy Theory," *Cognitive Therapy and Research* (4), 1980, pp. 39-66.

Campis, L. K., Prentice-Dunn, S., and Lyman, R. D. "Coping Appraisal and Parents' Motivation to Inform Their Children About Sexual Abuse: A Protection Motivation Theory Analysis," *Journal of Social and Clinical Psychology* (8), 1989, pp. 304-316.

Cohen, J. statistical Power Analysis for the Behavioral Sciences (2nd ed.), Lawrence Earlbaum Associates, Hillsdale, NJ, 1988.

Comrey, A. L. A First Course in Factor Analysis, Academic Press, New York, 1973.

Compeau, D. R, and Higgins, C. A. "Computer Self Efficacy: Development of a Measure and Initial Test," *MIS Quarterly* (19:2), 1995, pp. 189-212.

Condiotte, M. M., and Lichtenstein, E. "Self Efficacy and Relapse in Smoking Cessation Programs," *Journal of Consulting and Clinical Psychology* (49), 1981, pp. 648–658.

Cook, T. D., and Campbell, D. T. *Quasi-Experimentation: Design and Analysis for Field Setting*, Houghton Mifflin, Boston, MA, 1979.

Cox, D. N., Koster, A., and Russell, C. G. "Predicting Intentions to Consume Functional Foods and Supplements to Offset Memory Loss Using an Adaptation of Protection Motivation Theory," *Appetite* (43), 2004, pp. 55-64.

Cronbach L. J. "Coefficient Alpha and the Internal Structure of Tests," *Psychometrika* (16), 1951, pp. 297- 334.

Dhillon, G., and Torkzadeh, G. "Value-Focused Assessment of Information System Security in Organizations" in *Proceedings of the 22nd International Conference on Information Systems*, V. Storey, S. Sarkar, and J. I. DeGross (Eds.), New Orleans, LA, 2001, pp. 561-565.

Dooley, D. *Social Research Methods* (4th ed.), Prentice-Hall, Upper Saddle River, NJ, 2001.

Fruin, D. J., Pratt, C., and Owen, N. "Protection Motivation Theory and Adolescents' Perceptions of Exercise," *Journal of Applied Social Psychology* (22:1), 1991, pp. 55-69.

Galletta, D. F., and Polak, P. "An Empirical Investigation of Antecedents of Internet Abuse in the Workplace," in *Proceedings of the Second Pre-ICIS Annual Workshop on HCI Research in MIS*, F. F-H. Nah (Ed.), Seattle, WA, December 2003, pp. 47-51 (available online at **http://melody.syr.edu/hci/pre_icis03_wksp/hci03_proceedings_only.pdf**).

Gammie, E., Jones, P. L, and Robertson-Miller, C. "Accountancy Undergraduate Performance: A Statistical Model," *Accounting Education* (12:1), 2003, pp. 63-78.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. "2004 CSI/FBI Computer Crime and Security Survey," Computer Security Institute, 2004 (available online at **www.theiia.org/iia/download.cfm?file=9732**).

Hair, J. F., Anderson, R. E., Tatham, R. L., and Black, W. C. *Multivariate Data Analysis* (5th ed.), Prentice Hall, Inc., Upper Saddle River, NJ, 1998.

Hall, S., Weinman, J., and Marteau, T. M. "the Motivating Impact of Informing Women Smokers of a Link Between Smoking and Cervical Cancer: The Role of Coherence," *Health Psychology* (23:4), 2004, pp. 419-424.

Hand, D., Mannila, H., and Smyth P. *Principles of Data Mining*, MIT Press, Cambridge, MA, 2001.

Helmes, A. W. "application of the Protection Motivation Theory to Genetic Testing for Breast Cancer Risk," *Preventive Medicine* (35), 2002, pp. 453-462.

Hosmer, D. W., and Lemeshow, S. *Applied Logistic Regression*, John Wiley and Sons, New York, 1989.

Ipsos Insight. "Wireless Internet Access Climbs Nearly 30% in 2004," Press Release, Ipsos Insight Marketing Research Consultancy, 2004 (available online at **http://www.ipsos-insight.com**).

ISO/IEC TR1335. Information Technology: Guidelines for the Management of IT Security—Part 3: Techniques for the Management of IT Security, International Organization for Standardization, Geneva, Switzerland, June 1998.

Kanvil, N., and Umeh, K. F. "Lung Cancer and Cigarette Use: Cognitive Factors, Protection Motivation and Past Behavior," *British Journal of Health Psychology* (5), 1996, pp. 235-248.

Lukwago, S. N., Kreuter, M. W., Holt, C. L., Steger-Mey, K., Bucholtz, D. C., and Skinner, C. S. "Sociocultural Correlates of Breast Cancer Knowledge and Screening in Urban African American Women," *American Journal of Public Health* (93:8), 2003, pp. 1271-1275.

Maddux, J. E., and Rogers, R. W. "Protection Motivation Theory and Self Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* (19), 1983, pp. 469-479.

Maddux, J. E., and Stanley, M. "Self Efficacy Theory in Contemporary Psychology: A Review," *Journal of Social and Clinical Psychology* (4:3), 1986, pp. 249-255.

McDowell, M., Householder, A., and Lytle, M. "Securing Wireless Networks," Cyber Security Tip ST05-003, National Cyber Alert System, United States Computer Emergency Readiness Team, 2005 (available online at **http://www.us-cert.gov/cas/tips/ST05-003.html**).

Milne, S., Orbell, S., and Sheeran, P. "Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and Implementation Intentions," *British Journal of Health Psychology* (7), 2002, pp. 163-184.

Milne, S., Sheeran, P., and Orbell, S. "Prediction and Intervention in Health-related Behavior: A Meta-analytic of Protection Motivation Theory," *Journal of Applied Social Psychology* (30:1), 2000, pp. 106-143.

Mimoso, M. S. "Gartner: War Drive Illustrates Wireless Problem," SearchSecurity.com, June 4, 2003 (available online at **http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci904547,00.html**).

Moore, G. C., and Benbasat, I. "Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation," *Information Systems Research* (2:3), 1991, pp. 192-222.

Neter J., Kutner, M. H., Nachtsheim, C. J., and Wasserman, W. *Applied Linear Statistical Models* (4th ed.), Irwin, Homewood, IL, 1996.

Neuwirth, K., Dunwoody, S., and Griffin R. J. "Protection Motivation and Risk Communication," *Risk Analysis* (20:5), 2000, pp. 721-734.

Nunnally, J. C. *Psychometric Theory* (2nd ed.), McGraw-Hill Book Company, New York, 1978.

Nyamathi, A., Bennett, C., Leake, B., Lewis, C., and Flaskerud, J. "AIDS-Related Knowledge, Perceptions, and Behaviors Among Impoverished Minority Women," *American Journal of Public Health* (83:1), 1993, pp. 65-72.

Office of Homeland Security. *National Strategy for Homeland Security*, July 2002 (available online at **http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf**).

Plotnikoff, R. C., and Higginbotham, N. "Protection Motivation Theory and Exercise Behavior Change for the Prevention of Coronary Heart Disease in a High-Risk, Australian Representative Community Sample of Adults," *Psychology, Health and Medicine* (7:1), 2002, pp. 87-98.

Poulsen, K. "War Driving by the Bay," SecurityFocus, April 12, 2001 (available online at **http://www.securityfocus.com/news/192**).

Prentice-Dunn, S., and McClendon, B. T. "Reducing Skin Cancer Risk: An Intervention Based on Protection Motivation Theory," *Journal of Health Psychology* (6:3), 2001, pp. 321-328.

Rippetoe, S., and Rogers, R. W. "Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat," *Journal of Personality and Social Psychology* (52:3), 1987, pp. 596-604.

Rogers, R. W. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation Theory," in *Social Psychophysiology*, J. Cacioppo and R. Petty (Eds.), Guilford, New York, 1983.

Rogers, R. W. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91), 1975, pp. 93-114.

Searle, A., Vedhara, K., Norman, P., Frost, A., and Harrad, R. "Compliance with Eye Patching in Children and its Psychosocial Effect: A Qualitative Application of Protection Motivation Theory," *Psychology, Health and Medicine* (5:1), 2000, pp. 43-54.

Siponen, M. T. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security* (8:1), 2000, pp. 31-41.

Stoneburner, G., Goguen, A., and Feringa, A. "Risk Management Guides for Information Technology Systems," Special Publication 800-30, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, July 2002 (available online at **http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf**).

Straub, D. W. "Validating Instruments in MIS Research," *MIS Quarterly* (13:2), 1989, pp. 147-169.

Tanner J. F., Hunt, J. B., and Eppright, D. R. "The Protection Motivation Model: A Normative Model of Fear Appeals," *Journal of Marketing* (55), 1991, pp. 36-45.

Thomas, T. M. *Wireless Security*, Cisco Press, Indianapolis, IN, 2004.

U.S. Census Bureau. "Home Computers and Internet use in the United States: August 2000," U.S. Department of Commerce, September 2001 (available online at **http://www.census.gov/prod/2001pubs/p23-207.pdf**).

Wurtele, S. K. "Increasing Women's Calcium Intake: The Role of Health Beliefs, Intentions, and Health Value," *Journal of Applied Social Psychology* (18), 1988, pp. 627-639.

Wurtele, S. K., and Maddux, J. E. "Relative Contributions of Protection Motivation Theory Components in Predicting Exercise Intentions and Behavior," *Health Psychology* (6), 1987, 453-466.