VICTORIA UNIVERSITY OF WELLINGTON

Te Whare Wananga o te Upoko o te Ika a Maui

A Protection Motivation Theory Approach to Home Wireless Network Security in New Zealand:

Establishing If Groups of Concerned Wireless Network Users Exist And Exploring Characteristics of Behavioral Intention.

MMIM 592 Research Report

by

Dennis Michael DiGiusto
ID 300130360

Supervisor: Dr. David Mason

Submitted to the School of Information Management,

Victoria University of Wellington

in partial fulfilment of the requirements for the degree of

Master of Information Management

June 27, 2008

Table of Contents

Abstract

Threats arising from wireless hacking have been recently acknowledged both within academic literature and in the mainstream media. Additionally, it has been reported that many users of wireless networks make no attempt to activate security measures on their networks.

This report replicates and expands upon research found in Woon, Tan and Low (2005) in order to ascertain characteristics of home wireless network users in New Zealand.

The first research area asks the question: aside from the people who activate and those who do not, are there also people who are worried about wireless security and those who are not? This was proven to be true and that there is indeed a sub-group of wireless router users in New Zealand who are worried about wireless security.

The second research area seeks to determine what factors affect a person's intention to enable or not enable security features on a home wireless network. The results showed that:

- *The more people notice an increase in the degree of risk posed by wireless hacking, the more they feel like they could autonomously enable security features.*
- *The more people feel vulnerable to threats of wireless hacking, the more they feel that they would need help in setting up security features on their wireless network.*
- *The more people feel susceptible to wireless hacking, the more they feel that enabling security features would require extra efforts of time and money on their part.*
- *In order to get users to secure wireless networks, they must be convinced that enabling security features will deter hacker attacks.*
- *In order to get users to secure networks they need to feel that they could actually enable security features by themselves without some form of human assistance to help them do it.*

Preface

This report is not confidential.

I wish to thank Slingshot Telecommunications Company for posting a link to the online survey for this report within their website community forums pages.

I would like to acknowledge the support of several people for the guidance and support offered to me during the research and writing of this report. First, I thank my good friend Jeremy Greenbrook-Held for his encouragement and reassurance. Second, I thank Dr. David Mason of Victoria University for his guidance and direction. Finally and most importantly, I would like to thank my wife Emily Hermesch for her proofreading efforts and general support and forbearance.

I certify that except as noted above, this report is my own work and all references are accurately reported.

Dennis M. DiGiusto

Introduction

Results from a 2006 Statistics New Zealand survey showed that almost two-thirds (or 1 million) of New Zealand homes are connected to the Internet (Welch, 2007). Wireless local area networks (WLANs) have been growing in popularity recently in a number of vertical markets among OECD countries, including New Zealand (OECD, 2003). The flexibility presented by WLANs has been the most important reason in their widespread deployment and popularity (Srikanth, 2004).

Although both wired and wireless communications contain security risks, wireless requires special deliberation because of its "air" medium (Royster, 2005). WLANs use radio frequencies which contain the same features and benefits of conventional LAN technologies but without the restrictions of a cable (Srikanth, 2004). This convenience however, brings with it certain risks. Examining the technical specifications of currently available wireless routers reveals that WLAN radio frequencies can often travel anywhere from 20 to over 200 meters away from their source. This means that wireless signals go beyond the physical property of the user and are present to everyone and everything that is within range. Unprotected wireless signals can be detected by wireless devices outside a user's physical home network and information being sent across it can be seen by uninvited hackers.

There are simple and cheap hacking tools available in today's market that have slanted the balance of price, complexity, and deterrence in favor of the novice wireless attacker (Royster, 2005). Additionally, wireless technology is increasingly found as standard hardware within many off-the-shelf computers on the market today – accessing wireless signals (a.k.a., Wi-Fi) with these machines simply involves flipping a switch. Looking at the situation globally, a 2008 Accenture survey report states that despite Wi-Fi piggybacking being classified as criminal hacking in the U.S. and the U.K., 12% of the survey respondents from those countries admit to having logged on to someone else's unsecured Wi-Fi connection (McMillan, 2008). Furthermore, in the 2007 CSI/FBI Computer Crime and Security Survey 17% of the 2007 respondents reported abuse of wireless networks within their organizations (Richardson, 2007). This is noteworthy because nearly all categories of attacks or misuse measured in the survey indicate a decreasing

trend in the number of attacks detected. Misuse of wireless networks, however, is one of the few types of attack on the rise.

The concept of businesses adopting teleworking for their employees is a growing trend in New Zealand (Bland, 2004; Griffin, 2005) and the government has recently begun advocating the idea as well (Sustainability NZ, 2008). Wireless network security has been shown to be a significant concern for New Zealand businesses (Bryce, 2004) and justifiably so. Teleworkers using home based unsecured wireless networks to connect to their organizations' networks present the possibility of compromising company systems and information.

The threats arising from wireless hacking have been acknowledged in recent research (Arbaugh, Shankar, Wang & Zhang, 2002; Thomas 2004); however, other recent research has documented that oftentimes users of WLANs make no attempt to activate security measures on their wireless networks (Mimoso 2003; Poulsen 2001).

This report replicates and expands upon research found in Woon, Tan and Low (2005) but will focus on ascertaining characteristics of home wireless network users in New Zealand. To begin with, the research is based upon the simple reality that some people enable security features and some do not.

The first research question of this report expands upon this idea and looks at a different dimension of groups of wireless network users. That is, based upon certain clues contained within Woon, Tan and Low (2005) there appears to be a group of people who are worried about security in general and there is a group who are not. Woon, Tan and Low (2005) do not specifically acknowledge these details within their research; this report seeks to find if there really is an underlying group of concerned wireless network users in New Zealand.

The second research question in this report is similar to the theme of the research presented by Woon, Tan and Low (2005) and seeks to discover the factors that influence the behavioral intentions of wireless network users in New Zealand.

In order to determine whether there is indeed an underlying group of people who are worried about security, this report will analyze and assess patterns of responses to the independent variable scale item data. Likewise, in order to identify the elements which set apart people who

enable wireless network security from those who do not, this report will focus on measuring the concept of behavioral intention. Behavioral intention was selected because it is understood to be the immediate precursor to actual behavior (Ajzen, 2002).

To facilitate the objective of measuring behavioral intention, this report will provide background on certain motivational theories and then use that information to develop a series of tests to determine the intentions of wireless network users. The protection motivation theory (which is a health behavior theory) is used to develop six independent variables which help to assess the dependent variable of behavioral intention. Additionally, the transtheoretical model (a stage theory) is added to further help analyze the behavior intentions of the dependent variable.

The report then presents the methodology of the data collection for the independent variables and the coping stages. That is, a thirty-three item online questionnaire which incorporated the test questions was made available electronically to New Zealand-based respondents.

Next, the report presents some of the overall statistics of the survey respondents and tests the data for both main hypotheses with various statistical analyses using SPSS. The findings emerging from these tests are then discussed with a particular focus on whether they support the statements made in the two main hypotheses.

Finally, some of the implications and limitations of the research are discussed and the results of the report are summarized.

The results emerging from this report are important for two reasons. First, they will add to the academic legitimacy of the original work done by Woon, Tan and Low (2005). Secondly, they will contribute data to Wellington area public officials, academics and area businesses that could be used to develop policies, procedures or other educational mechanisms to address and reduce the risks posed to the users of unprotected wireless devices.

Research Issue One

The basis for this research item emerges from several unaddressed factors within the report by Woon, Tan and Low (2005). Regardless of whether or not they have enabled security measures,

is there another way to categorize wireless network users: those who are worried about wireless security versus those who are not?

The Woon, Tan and Low (2005) report was based upon a 189 response sample set. Out of the 189 respondents, 73 people had not enabled their security features and 116 people had enabled their security features. What is noteworthy about this sample set is that the researchers also asked respondents to reveal who enabled the security features on their wireless networks. The aim of this question was to help assess the behavioural intention of study respondents and the researchers used the data for that purpose only. Their results showed that only 62 of the 116 enablers performed the enabling actions themselves while the remaining 54 enablers had someone else perform the enabling actions for them. This means that only 33% of the 189 responders actually made the effort to perform any actions by themselves. This is important for two reasons: it suggests that there may in fact be two different types of people using home wireless routers; and that these two groups cannot necessarily be identified by assessing enabled versus not enabled.

Woon, Tan and Low (2005) do not address this issue in their report; although it appears they unwittingly provide supporting evidence for it in their research with what they describe as a technical “knowledge quiz” assessment of the respondents. The statistical tests on the quiz data, as completed by Woon, Tan and Low (2005), show that the quiz resulted in two clear groups of study respondents. The quiz was intended to identify a low knowledge group and a high knowledge group; it would be expected then that the number of low knowledge respondents would be about equal to the number of non-enablers and likewise that the number of high knowledge respondents would be about equal to the number of enablers. Since this did not occur, their knowledge quiz may not actually have been testing technical knowledge. Rather, it may suggest that there are two different types of people using home wireless networks: those who seem worried (or concerned) about wireless security and those who do not. Establishing if this categorical determinant exists is the first primary research objective of this report.

Research Issue Two

The second objective of this report seeks to replicate the overall theme of the research found within Woon, Tan and Low (2005): determining the factors that influence behavioral intention. Simply put, what factors affect a person's intention to enable or not enable security features on home wireless networks?

This section of the report discusses two theories which help to explain behavioral intention (i.e., why people engage in unsafe practices and whether they plan on changing those behaviors):

- The PMT (Protection Motivation Theory);
- The TTM (Transtheoretical Model).

Research suggests that protection motivation is an inferred mental state (i.e., it cannot be observed directly), but it can be measured by behavioral intention (Neuwirth, Dunwoody & Griffin, 2000). Likewise, TTM supports the assessing of and analyzing of behavioral intention by categorizing an individual into one of a series of decision stages.

Since behavioral intention is thought to be a reasonable predictor of behavior (Neuwirth, Dunwoody & Griffin, 2000), identifying the behavioral intentions of home wireless router users will reveal the characteristics that set apart users of wireless routers who secure their wireless routers from those who do not.

Protection Motivation Theory

Components of PMT

PMT posits that environmental and personal factors combine to create potential threat inputs to an individual. These inputs initiate two cognitive mediating processes within an individual: the threat-appraisal pathway and the coping-appraisal pathway. (See Figure 1). Each pathway addresses certain responses to threats: the maladaptive response in the threat-appraisal pathway and the adaptive response in the coping-appraisal pathway. The overall outcome of the two appraisal processes is the coping response, or coping mode – which could be either adaptive coping or maladaptive coping (Rippetoe & Rogers, 1987; Tanner, Day & Crask, 1989).

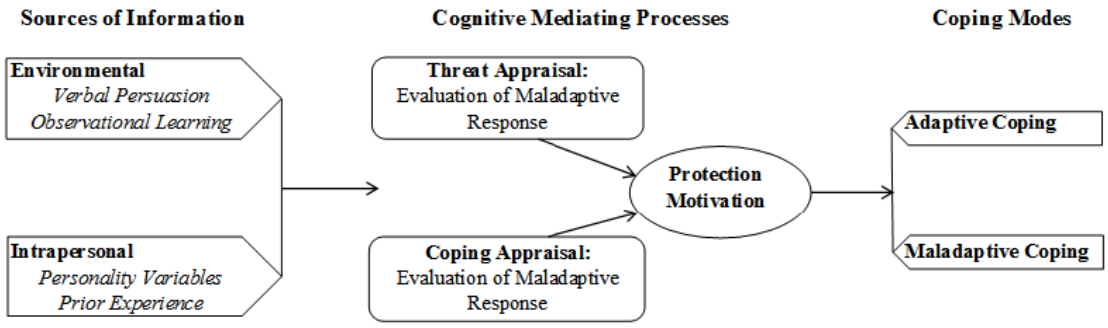


Figure 1: Overall model of PMT (Source: Floyd et al, 2000).

It is important to note that though the sources of information (environmental and personal factors) are essential within the PMT model, the background of and features comprising these elements are out of scope of this report.

Threat-Appraisal

Threat-appraisal is an individual's judgment of the amount of risk presented by a threat. In the PMT model, a maladaptive response means something that is counterproductive to the individual. In the context of reacting to a threat, a maladaptive response is one in which *no* measures are taken to protect oneself from the risk presented by the threat. The threat-appraisal process is addressed first, since a threat must be perceived or identified before there can be an evaluation of the coping options (Floyd, Prentice-Dunn & Rogers, 2000).

The three components of threat-appraisal:

- Perceived vulnerability (the individual's assessment of the chances of the threatening event occurring);
- Perceived severity (the severity of the repercussions of the event); and,
- Perceived rewards (intrinsic and extrinsic incentives related to the threatening event).

See Figure 2. Rewards will increase the likelihood of choosing the maladaptive response (not to protect the self or others), while threat (i.e., vulnerability and severity) will decrease the likelihood of choosing the maladaptive response (Floyd, Prentice-Dunn & Rogers, 2000).

Coping-Appraisal

Coping-appraisal is an individual's perceived ability to contend with and prevent the potential loss or damage resulting from a risk. In the PMT model, an adaptive response is something that is productive to the individual. In the context of reacting to a threat, an adaptive response is one in which protective measures *are* taken to reduce the risk posed by the threat.

The three components of coping-appraisal:

- Self efficacy (the individual's belief in his/her own competence to accomplish the adaptive response);
- Response efficacy (the potential success of the adaptive response); and,
- Response cost (the envisioned expenditures—monetary, time, effort—in adopting the adaptive response).

See Figure 2. Response efficacy and self-efficacy will increase the likelihood of choosing the adaptive response, while response costs will decrease the likelihood of choosing the adaptive response (Floyd, Prentice-Dunn & Rogers, 2000).

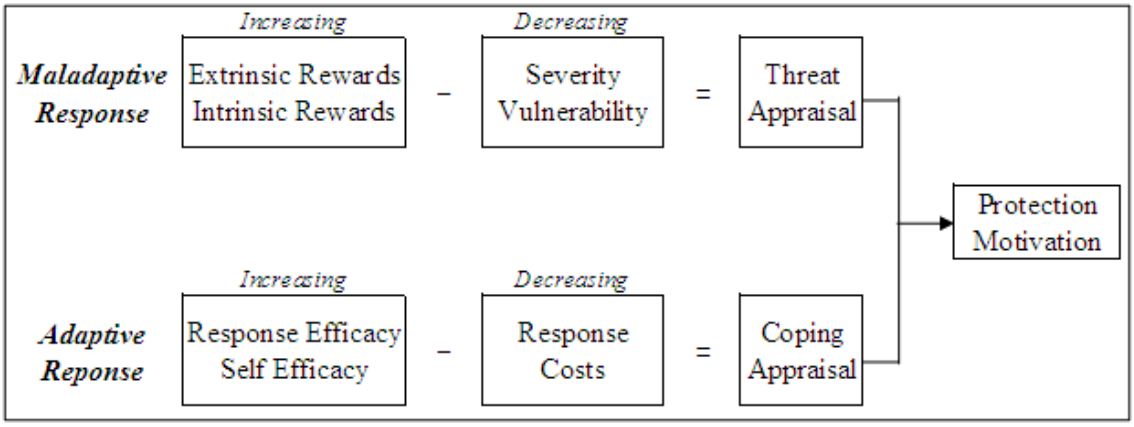


Figure 2: PMT Cognitive Mediating Process (Source: adapted from Rogers, 1983; Floyd et al, 2000).

Coping Response

The output of these appraisal-mediating processes is the coping response. Coping response refers to an individual's intentions to begin, maintain, or reduce the pertinent adaptive responses

(Floyd, Prentice-Dunn & Rogers, 2000). Coping response is "protection motivation". Measuring the coping response of an individual will reveal the behavioral intention, or coping mode of an individual.

Value of using PMT

PMT research has traditionally been carried out in health focused studies; however, numerous studies have identified and demonstrated its cross-functional utility outside of health related matters (Rogers & Prentice-Dunn, 1997). Such topics have included political issues, environmental concerns and protecting others (Floyd, Prentice-Dunn & Rogers, 2000). Additionally, PMT has been formally extended to include social risks (Ho, 1998). The PMT has been used effectively in social research for predicting behaviors (Stanton et al, 2005; Martin, Bender & Raish, 2007; Pahnila, Siponen & Mahmood, 2007; Woon, Tan & Low, 2005).

Bringing the PMT and TTM together

Recent research suggests that there is an implicit break in the linking of intention and behavior in non stage-based theories (Schwarzer, 2008). An integrated PMT-TTM model can lead to a more thorough assessment of the cognitive and motivational processes that individuals experience in mitigating risk, thus helping to bridge the gap between intention and behavior (Martin, Bender & Raish, 2007). The integrative model accomplishes this by revealing which risk variables are most successful at motivating individuals in the assorted decision stages (Martin, Bender & Raish, 2007). See Figure 3:

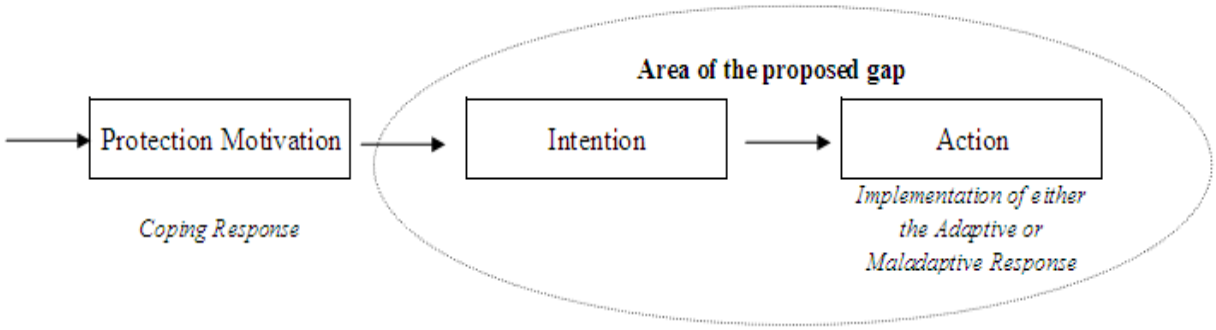


Figure 3: Need for Combining PMT & TTM

Transtheoretical Model (TTM)

Stage Theories

The degree of readiness to accept and act on a risk has been shown to impact individuals' motivation to protect themselves from a risk (Martin, Bender & Raish, 2007). Attaining a new healthy behavior or adjusting an unhealthy behavior is the consequence of a dynamic process involving advancing through a series of specific stages (Grimely, Williams, Miree & Baichoo, 2000). Stage theories put forth that individuals can be differentiated based upon assessing those who have not yet decided to change their behavior, those who have decided to change, and those already performing the new behavior (Martin, Bender & Raish, 2007).

Importance for this Research

The transtheoretical model (TTM) is a stage theory that analyzes behavior change by presenting an ordered set of categories into which individuals can be classified (Grimely et al, 2000). Based upon ordered classifications, it is then possible to recognize the factors (e.g., vulnerability, risk severity) that clarify how to more effectively communicate with each subgroup (Weinstein, Rothman & Sutton, 1998; Martin, Bender & Raish, 2007).

Components of TTM

The TTM consists of six decision-making stages that an individual encounters when exposed to a risk (See Figure 4); TTM research places individuals into one of the six stages (or some predetermined subset) according to their behavior and intentions to undertake risk-mitigating actions (Prochaska, Norcross & DiClemente, 1994).

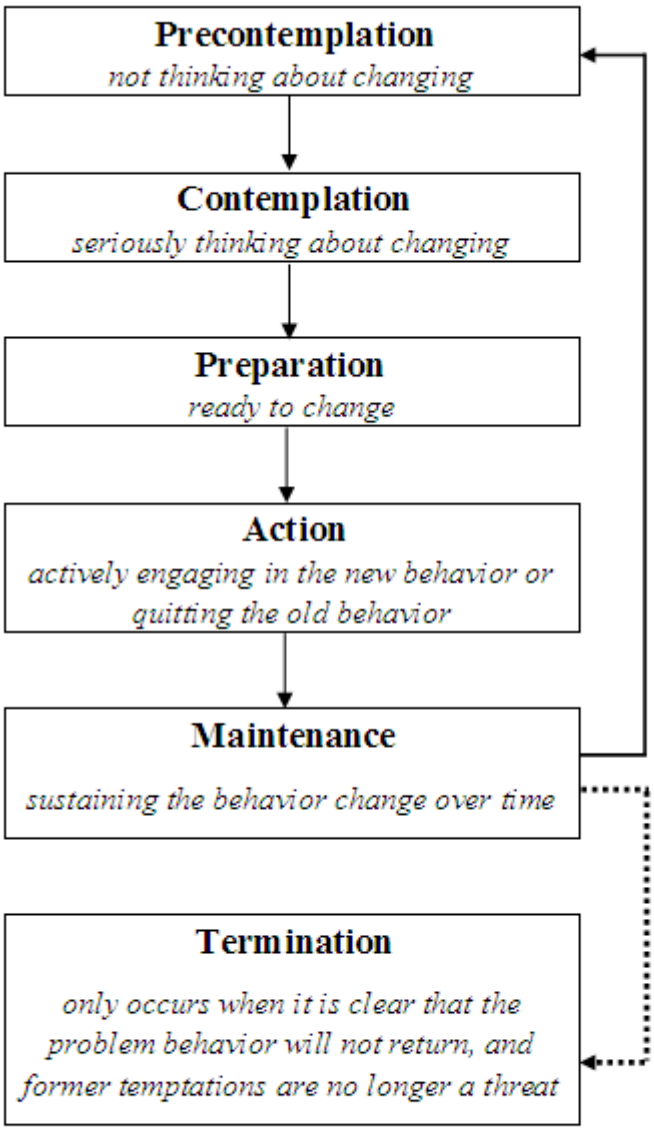


Figure 4: TTM Components
(Source: adapted from Block & Keller, 1998; Grimely et al, 2000)

Although the actual number of stages has fluctuated over the years of TTM development (Block & Keller, 1998), most empirical studies of the TTM reduce the assessment of individuals to a subset of these six stages based on their behavior and intentions to undertake risk-mitigating actions (DiClemente et al, 1991). The most typical model of reduced TTM stages is a three-tier subset. The method to create this type of subset of individuals usually requires using subjective

knowledge criteria (Martin, Bender & Raish, 2007) and the three resultant coping stages are characterized in Figure 5:

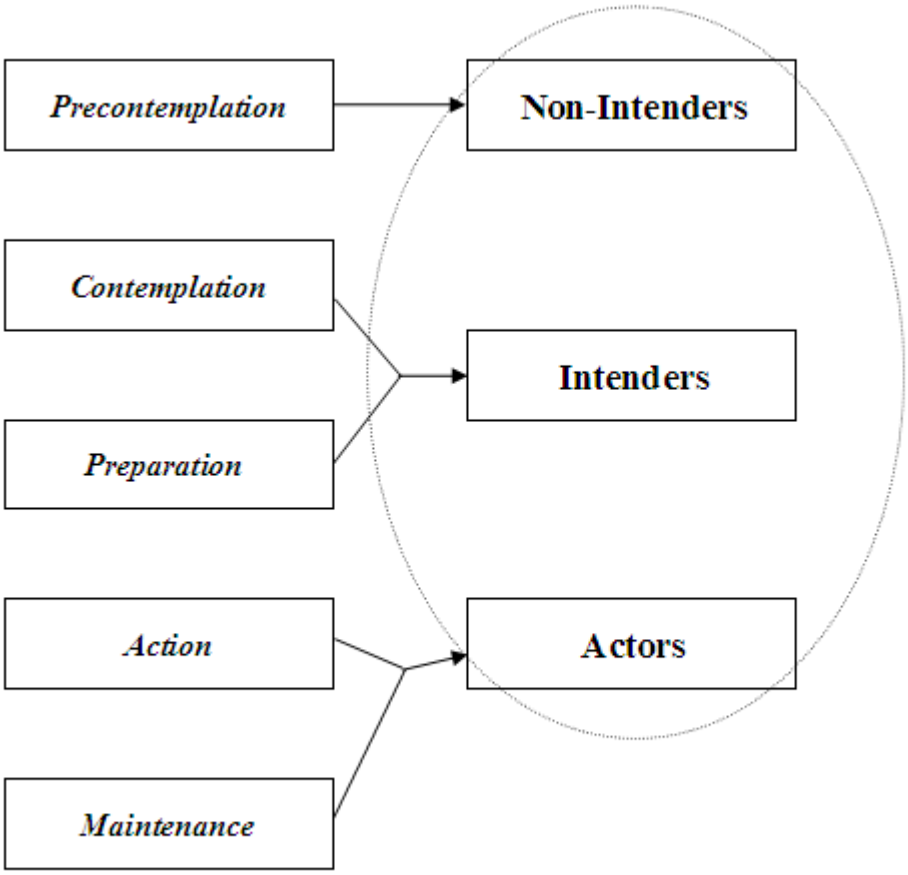


Figure 5: TTM 3-Tier subsets (Source: adapted from Velicer & Prochaska, 2008)

Value of using TTM

The transtheoretical model (TTM) of change has been utilized across a wide array of addictive and non-addictive health-related behaviors, such as smoking cessation, alcohol abuse, AIDS risk reduction, exercise adoption, weight control and diet, sunscreen use, condom and other contraceptive use, and medication adherence (Block & Keller, 1998; Grimely et al, 2000). Decision stage theories (such as TTM) have been used to study health behavior transformations based on the postulation that a set of variables will influence different people in different ways (Horwath, 1999).

First Main Hypothesis

The first research question seeks to determine whether a different category of home wireless network users exists beyond simply those enable security features versus those who do not.

Woon, Tan and Low (2005) unintentionally showed that supplemental quizzes may not in fact measure intended concepts. Therefore, this research report avoids that method and assesses the existence of the proposed sub-groups based upon data attained through more reliable devices: the independent variable scale items. Response values for each of the independent variable scale items would indicate two patterns, or groups, in the collected data. Diagram 1 (below) illustrates an example of this effect: a bunching of response values clustered on the high end of the scale and a bunching of response values clustered on the lower end of the scale.

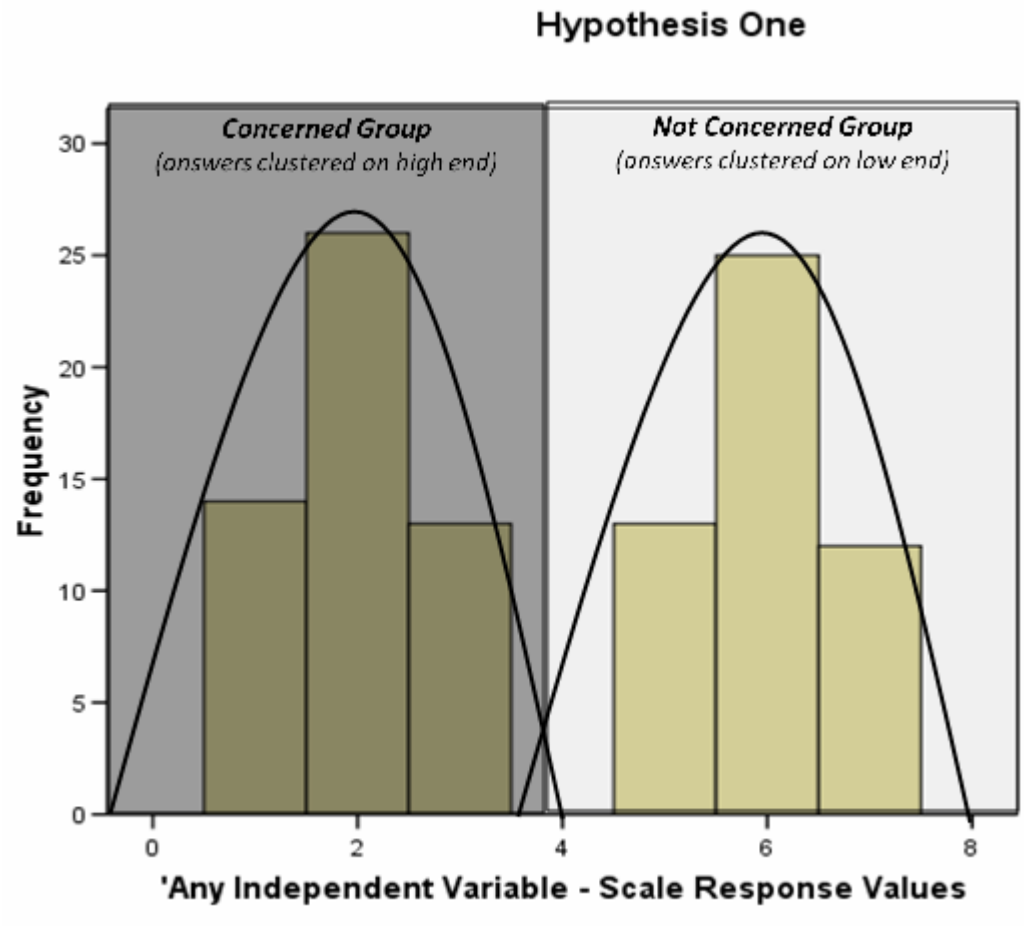


Diagram 1: Research Question One

The hypothesis for this first main research question is straightforward:

> *There are two significantly distinct groups of home wireless network users: those who are concerned about wireless security and those who are not.*

Note: The existence of this pattern of responses has implications for other types of statistical analyses and that will be addressed further on.

Second Main Hypothesis

The second research question focuses on determining the factors that influence behavioural intention. As such, this section of the report utilizes the components of the PMT to put forward six hypotheses that will help to identify the behavioral intentions (coping modes) of home wireless router users.

Defining the Dependent and Independent Variables

The coping response (i.e., an individual's intent to embrace a recommended behavior) is the measured (or dependent) variable in this study. The dependent variable is assessed by testing the six independent variables contained within the threat-appraisal and coping-appraisal elements of the PMT. Since these two elements are made up of opposing principles, the outcome of these independent variables tests will indicate two contrasting behavioral intentions.

Essentially this means that we end up with a dualistic dependent variable (i.e., a variable possessing two distinct aspects – parts from the threat appraisal and parts from the coping appraisal). See Figure 6:

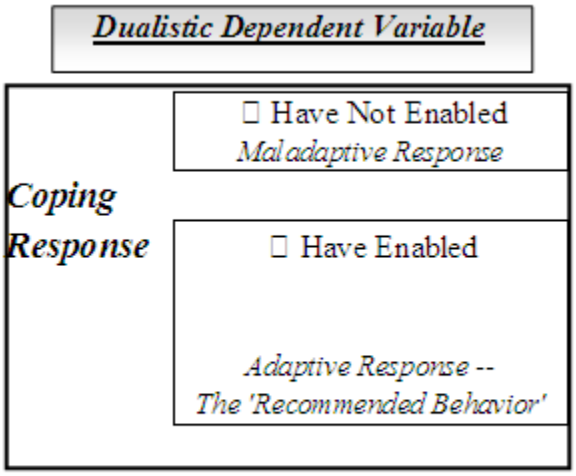


Figure 6: Coping Reponse - The Dependent Variable

Threat Appraisal Element

The outcome, or behavior, arising out of the threat-appraisal tests is called the maladaptive response. The maladaptive response is the behavioral intention of an individual to not protect his or her self from wireless network threats (i.e., not enable the security features on their home wireless router). See Figure 7:

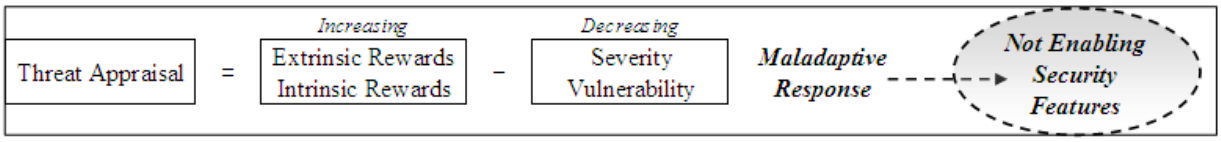


Figure 7: Maladaptive Response

Coping Appraisal Element

The outcome, or behavior, arising out of the coping appraisal tests is the adaptive response. The adaptive response is the behavioral intention of an individual to protect his or her self from wireless network threats (i.e., enable the security features on their home wireless router). In this study, the recommended behavior is this adaptive response. See Figure 8:

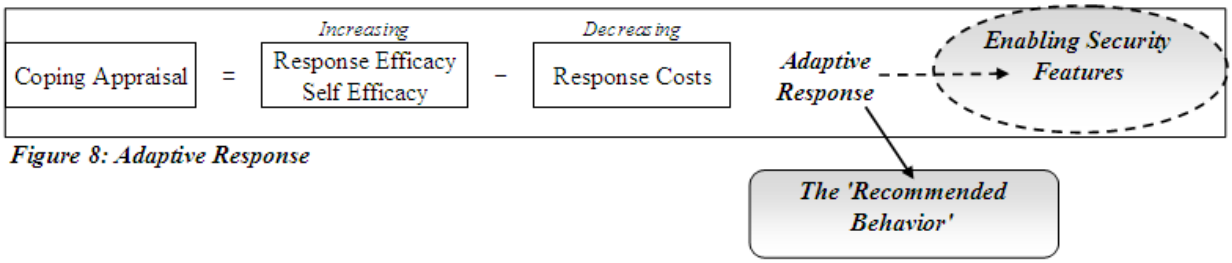


Figure 8: Adaptive Response

The following two sub-sections will discuss the details of the tests (or hypotheses) for each of the six independent variables contained within the threat appraisal and coping appraisal.

Threat Appraisal

The threat appraisal process evaluates behavior that is counterproductive to an individual (Floyd, Prentice-Dunn & Rogers, 2000). *Perceived vulnerability*, *perceived severity* and *perceived rewards* are the three constructs of the threat appraisal – the amount of threat experienced by an individual is a combination of severity and vulnerability, minus the rewards. Figure 9 provides an overview of how the maladaptive coping response is assessed for this study:

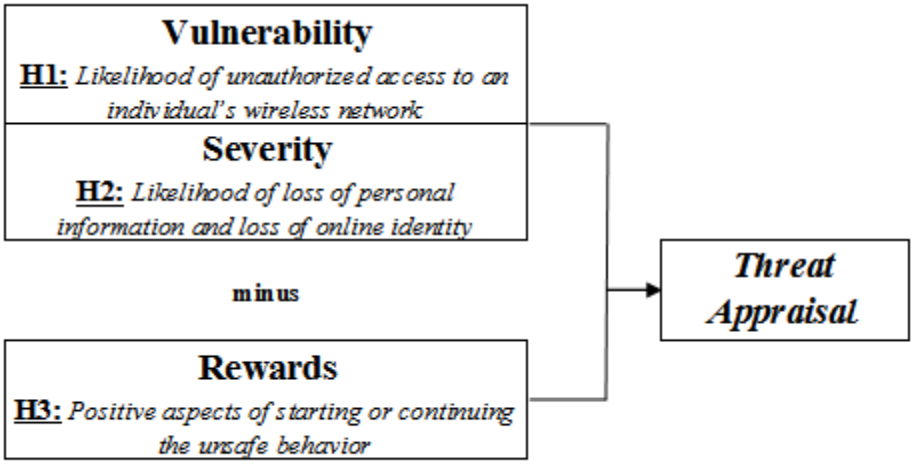


Figure 9: Threat Appraisal Hypotheses

Perceived Vulnerability

Perceived vulnerability refers to a person's assessment of his/her own chances of being exposed to a security threat (Rogers, 1983). The concept of 'threat' for this research report refers to unauthorized access to an individual's wireless network. PMT-based research has shown that individuals who exhibit high levels of perceived vulnerability also show increased intention to adopt a recommended coping response (Rogers, 1983; Rippetoe & Rogers, 1987; Wurtele, 1988; Wurtele & Maddux, 1987).

> *H1: Perceived vulnerability is significant in determining if an individual adopts the recommended behavior of enabling security measures on a home wireless network.*

Perceived Severity

Perceived severity refers to the consequences to individuals if a security threat occurs (Pahnila, Siponen & Mahmood, 2007). The concept of a 'consequence' for this research report refers to the loss of personal information and loss of online identity.

There are inconsistencies between the existing theory and practice in regards to this construct. Health related PMT research has found that severity is the least significant of the cognitive mediating factors (i.e., Maddux and Rogers, 1983; Milne, Sheeran & Orbell, 2000); conversely, the most commonly utilized IT security management frameworks (SIGS, 2002; Stoneburner,

Goguen & Feringa, 2002; ISO/IEC, 1998) promote a risk assessment (i.e., risk management) approach to handling security threats.

Risk management plans operate on the principle of perceived severity – since risk levels increase when the severity of a loss from a threat increases, risk reduction actions are taken only when those levels of risk become unsatisfactorily high.

> *H2: Perceived severity is significant in determining if an individual adopts the recommended behavior of enabling security measures on a home wireless network.*

Perceived Rewards

Perceived Rewards are intrinsic and extrinsic maladaptive (i.e., counterproductive) responses to a security threat (Floyd, Prentice-Dunn & Rogers, 2000). In this context, rewards refer to personal feelings of safety, personal comparisons to what others are doing and evaluation of future exposure to risk.

Whereas 'threat' decreases the chances of an individual selecting the maladaptive response, an intrinsic or extrinsic reward increases the chances of an individual selecting the maladaptive response (Floyd, Prentice-Dunn & Rogers, 2000).

There is a controversy in the social sciences as to the pros and cons of measuring intrinsic and extrinsic motivations in research (Cameron & Pierce, 2002). As such, there has been sparse PMT related research incorporating the *perceived rewards* construct (Abraham, Sheeran, Abrams, & Spears, 1994; Stanton et al, 2005). As the aim of this research report is to wholly analyze the behavioral intentions of individuals utilizing wireless router security features, the intrinsic satisfaction and extrinsic approval of taking on the recommended behavior are measured.

> *H3: Perceived rewards are significant in determining if an individual adopts the recommended behavior of enabling security measures on a home wireless network.*

Coping Appraisal

The coping appraisal process evaluates the ability of an individual to deal with and avert an exposed threat (Floyd, Prentice-Dunn & Rogers, 2000). *Response efficacy, self efficacy* and

response cost are the three constructs of the coping appraisal – the amount of coping ability experienced is a combination of response efficacy and self efficacy, minus response costs. Figure 10 provides an overview of how the adaptive coping response is assessed for this study:

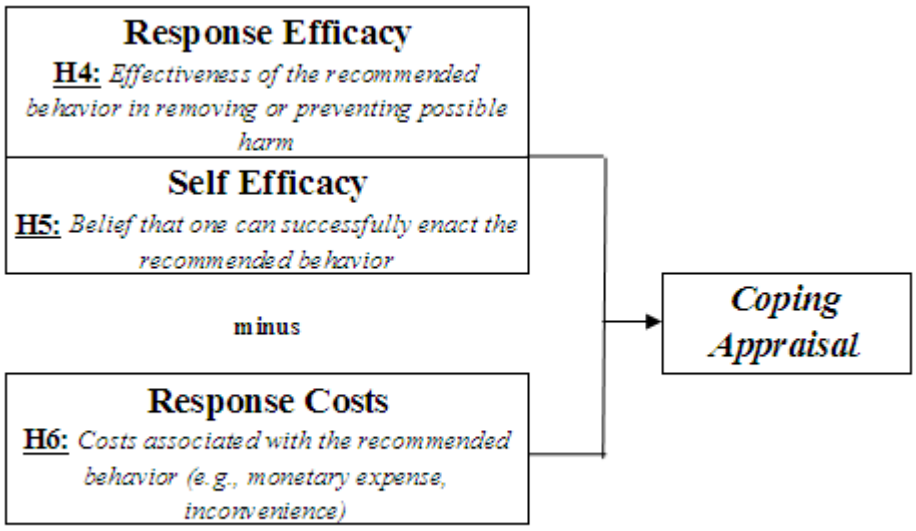


Figure 10: Coping Appraisal Hypotheses

Response Efficacy

Response efficacy relates to the belief in the perceived benefits of an action and that that action (i.e., the coping response) will be useful in providing protection from risks (Rogers, 1983; Pahnila, Siponen & Mahmood, 2007). The 'coping response' for this research report is contextualized using guidelines taken from US-CERT publications (Wireless Security, 2006; McDowell, Householder & Lytle, 2005) as these resources highlight many of the potential threats of wireless technology and suggest how to secure a home wireless network.

PMT-based research has shown that there are positive correlations between response efficacy and coping response ranging from significant to medium effects (Maddux & Stanley, 1986; Wurtele, 1988).

> *H4: Response efficacy is significant in determining if an individual adopts the recommended behavior of enabling security measures on a home wireless network.*

Self Efficacy

Self efficacy stresses an individual's judgment of their capabilities to cope with the task ahead (i.e., their ability to perform the coping response) (Pahnila, Siponen & Mahmood, 2007).

PMT-based research on self efficacy beliefs provides proof that self efficacy is a considerable controlling agent in motivational, cognitive, and affective processes (Floyd, Prentice-Dunn & Rogers, 2000).

For example, the following PMT-based research shows there are significant positive correlations with self efficacy on:

- Behavioral change (Bandura, 1977; Bandura, Adams, Hardy & Howells, 1980; Condiotte & Lichtenstein, 1981);
- Coping response (Fruin, Pratt & Owen, 1991; Maddux & Rogers, 1983; Maddux & Stanley, 1986); and,
- Intention (Milne, Sheeran & Orbell, 2000).

> *H5: Self efficacy is significant in determining if an individual adopts the recommended behavior of enabling security measures on a home wireless network.*

Response Costs

Response costs are the estimated expenditures an individual associates with a particular course of action (Woon, Tan & Low, 2005; Floyd, Prentice-Dunn & Rogers, 2000). In this context, costs refer to the expenditures involved with performing the coping response (e.g., monetary expenses, difficulty of the action, or personal inconvenience in terms of both time and effort).

Whereas 'efficacy' (i.e., sense of individual ability) increases the chances of an individual selecting the adaptive response, response costs decreases the chances of an individual selecting the adaptive response.

PMT-based research provides that there is a significant link between response cost and coping response (Helmes, 2002; Neuwirth, Dunwoody & Griffin, 2000).

H6: Response cost is significant in determining if an individual adopts the recommended behavior of enabling security measures on a home wireless network.

PMT-based Research Model

Figure 11 represents how the dualistic dependent variable is assessed by testing the six independent variables contained within the threat-appraisal and coping-appraisal elements of the PMT.

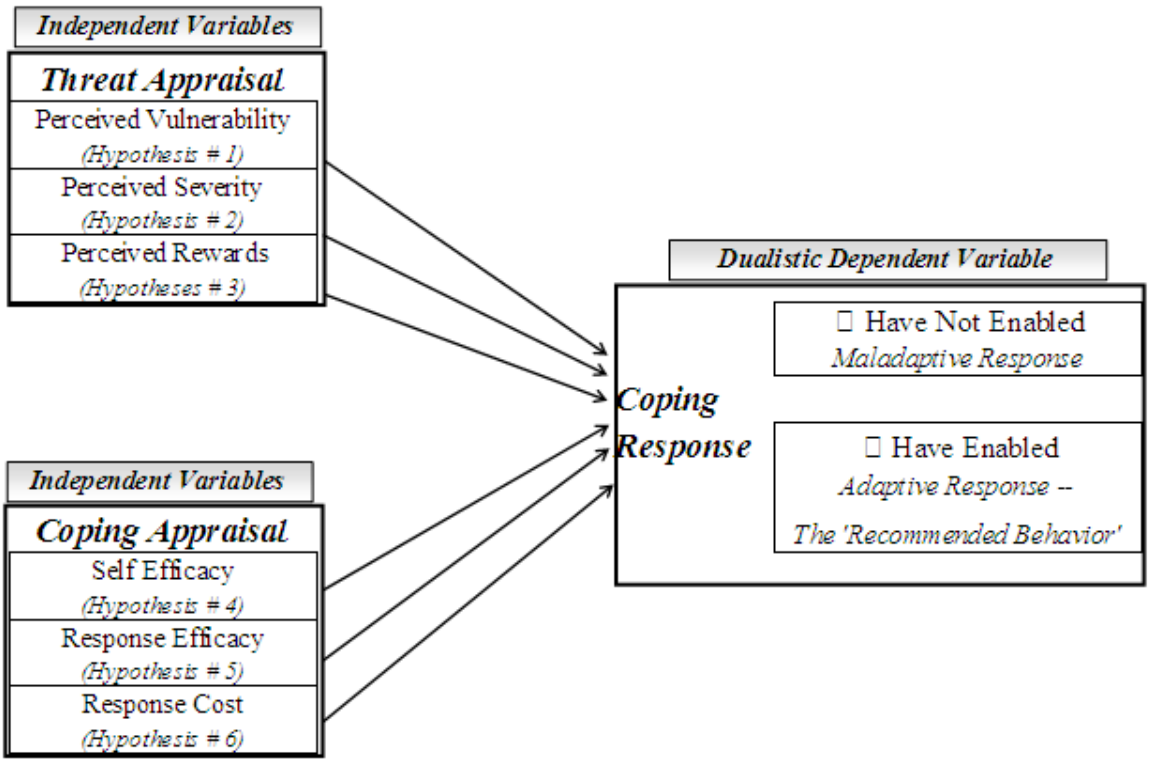


Figure 11: PMT-based Research Model

Incorporating TTM Elements

Adding TTM elements onto the PMT-based model allows for enhanced analysis and prediction of the dualistic dependent variable. In this study, this essentially means breaking down the

dependent variable into three components instead of two. The overall objective is to further analyze the intent of the individuals within the maladaptive (have not enabled) response.

Breaking down the dependent variable into three sub-components is accomplished by assessing the number of risk-reduction behaviors that individuals have already performed or intend to perform to protect their computer systems from threats. (The survey instrument assesses ten risk reduction behaviors). Based on these results, individuals are grouped into one of three possible coping stages:

- Non-Intenders (Individuals completing three or less risk-reduction behaviors);
- Intenders (Individuals completing four to six risk reduction behaviors); and
- Actors (Individuals completing seven or more risk reduction behaviors).

Figure 12 illustrates how the TTM elements are added onto the PMT-based model:

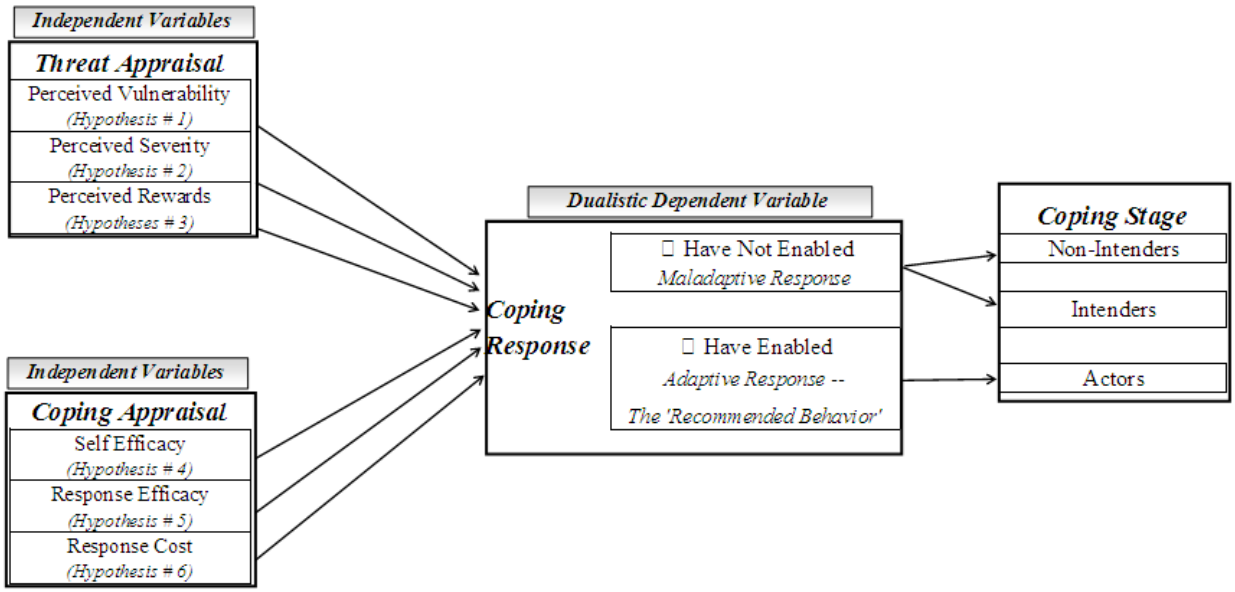


Figure 12: PMT-based Research Model with TTM added

Methodology

This section describes the approach to collecting the data concerning the independent variable test questions. It is important to reiterate that the data collected from the independent variable scale items are essential in analyzing both main hypotheses.

In order to collect the research data, a thirty-three item online questionnaire comprised of three sections was made electronically available to New Zealand-based users of home wireless routers. The survey consisted of three sections: demographics, PMT elements and TTM risk behavior assessment items. See Appendix – The Survey Instrument.

Demographics

The demographics section captures the brand of wireless routers used by the respondent, the duration of use of the router by the respondent and the age of the respondent. This was in part based upon Woon, Tan and Low (2005) who also checked the ownership of home wireless networks by asking respondents for the brand of their wireless network; thus, adding a sense of eligibility and suitability of a respondents' responses.

PMT Elements

The PMT research items are measured using a seven-point Likert scale. This level of measurement was based upon the design of the survey within Woon, Tan and Low (2005).

Previous PMT-based research has been successful in incorporating the use of surveys to measure all the cognitive variables and to examine the cognition intention links (Pechmann, Zhao, Goldberg & Reibling, 2003). The final wording and structure of the threat-appraisal and coping appraisal questions were based upon the validated design found within the survey of Woon, Tan and Low (2005).

TTM Stages

The research items that assess the risk reduction behaviors within the TTM portion of the research model are measured using five-point scales. Since these scales were not intended for direct comparison with or against the independent variable scales, the levels of measurement

were not based upon the same seven-point Likert scales. The assessment of risk behaviors is only intended to break down the dualistic dependent variable into three coping stages. The independent variable scales could then be used to measure the resultant three coping stages.

Each of the ten risk-reduction behaviors was measured using the following five-point scale: 1 = already done, 2 = will do next month, 3 = will do in 3–6 months, 4 = will do within the next year, and 5 = probably will not do.

Previous TTM-based research provides validity and purpose of structure regarding the primary TTM research components included in this survey (Martin, Bender & Raish, 2007). The ten risk-reduction behaviors included in this survey were developed based upon guidelines taken from US-CERT publications (Wireless Security, 2006; McDowell, Householder & Lytle, 2005).

Design & Respondents

The data collection within this report is set up cross-sectionally rather than longitudinally. Concerning eligibility, any person living in New Zealand (regardless of age, sex, race, ethnicity, education or citizenship) who used a wireless router in their home qualified as a respondent for the survey. There were no other qualifications or restrictions.

Collection Device

The data for the research report was collected by means of an electronic (web-based) survey questionnaire. The target sample of usable responses of this research survey was approximately 200 usable sets of data. The final collected usable sample set was 103 responses.

Sample Size

There are no reliable statistics available to indicate exactly how many households in New Zealand use a wireless router in their home network. It is known that, as of 2007, one million New Zealand homes are connected to the Internet. If we assume that just one-half of one percent of that population use a wireless router in their home, the estimated population in New Zealand would be about 5000 people. Using the formula established in Cochran (1977) for determining sampling size in continuous data, we would find that the minimum returned sample size would be 116 samples. This indicates that the sample size (103 responses) used in this study is most

certainly below a standard accepted amount. See Figure 13 for the estimated sample size calculation:

$$n_o = \frac{(t)^2 * (s)^2}{(d)^2} = \frac{(1.96)^2(1.167)^2}{(7*.03)^2} = 118$$

$$n = \frac{n_o}{(1 + n_o / \text{Population})} = \frac{(118)}{(1 + 118/5000)} = 116$$

Souce: based on Bartlett, Kotrlik, & Higgins, 2001

Figure 13: Using Cochran sample size calculations

In the next section, the several statistics concerning the independent variables will be examined to determine just how well this particular sample represents the overall population. But, it must be made explicitly clear that the sample size of 103 used in this research report is indeed below the minimum acceptable amount which would indicate statistical validity.

Data Analysis

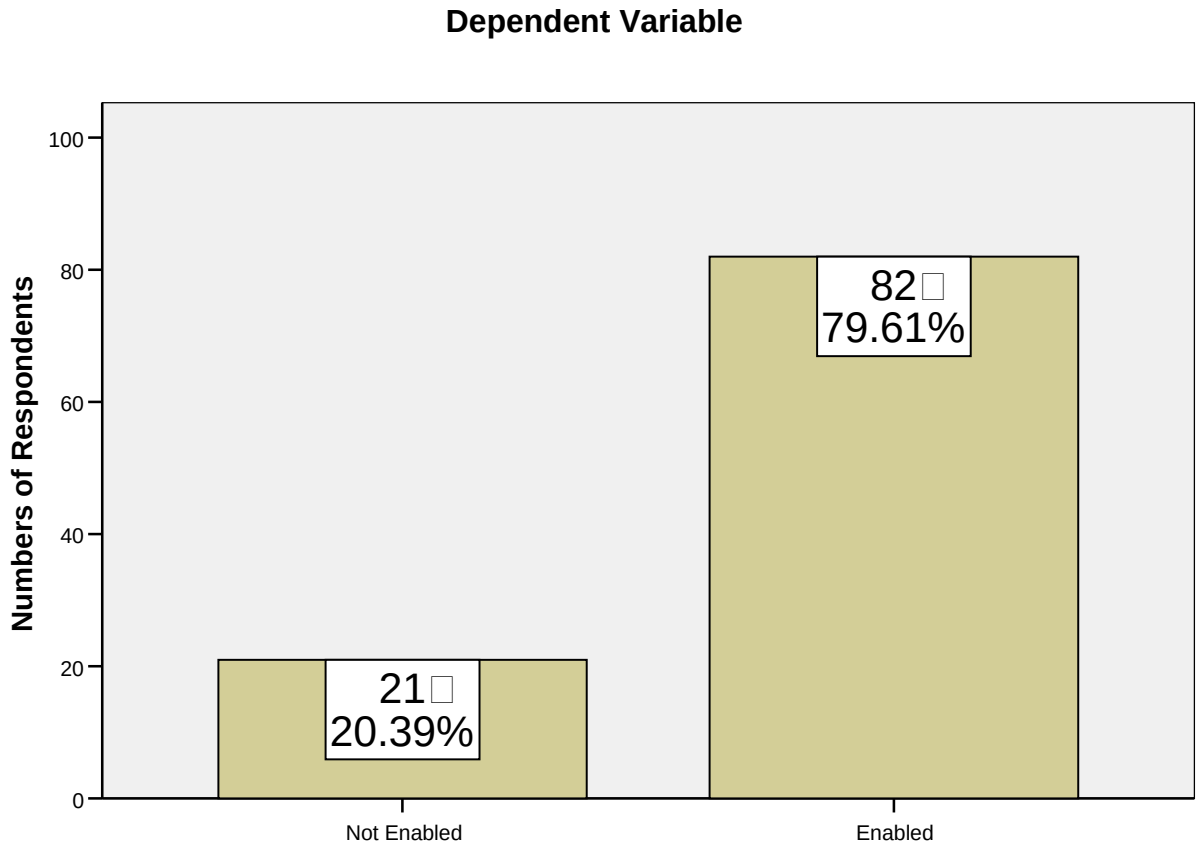
This first part of this section discusses the demographic data collected in terms of the dependent variable. The second part of this section describes the data collected relating to the independent variables through histograms. The third part of this section discusses and tests the data in context of Hypothesis One. The last part of this section carries out several statistical analyses in order to test the data in the context of the statements contained within Hypothesis Two.

Demographic Data

The first part of this section illustrates many of the basic details regarding the survey respondents. Frequency distributions were run on the dependent variable and then on the demographic measures in order to categorize the 103 respondents into those who have not

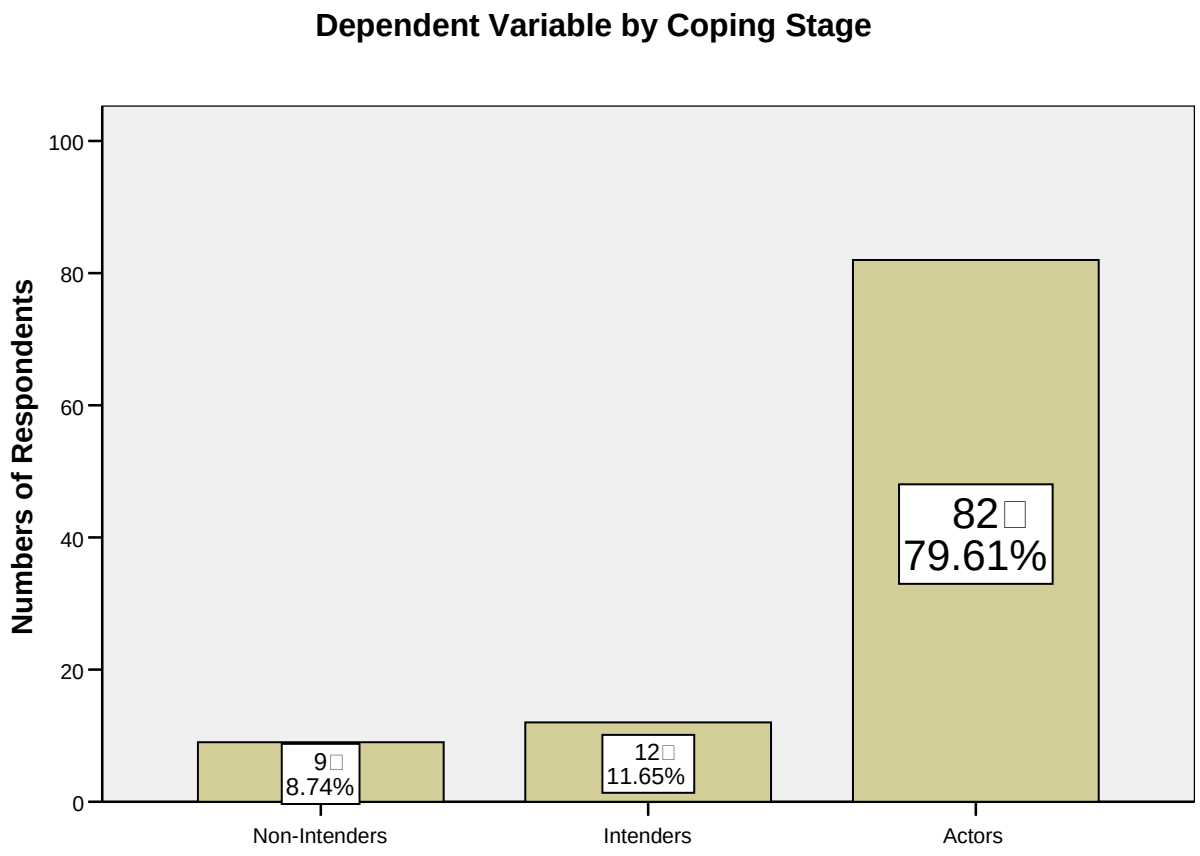
enabled the security feature on their home wireless routers and those who have enabled security features on their routers.

First, a bimodal distribution was generated with the dependent variable to determine exactly how many respondents have not enabled security features and how many respondents have enabled security features. The expectation was that the distribution of non-enablers to enablers would be more equal; but as the chart below illustrates, 21 respondents have not enabled and 82 have enabled security features. The fact that nearly 80% of respondents have enabled security features is higher than expected and indicates that people in this sample may be much more security conscious than the actual population.

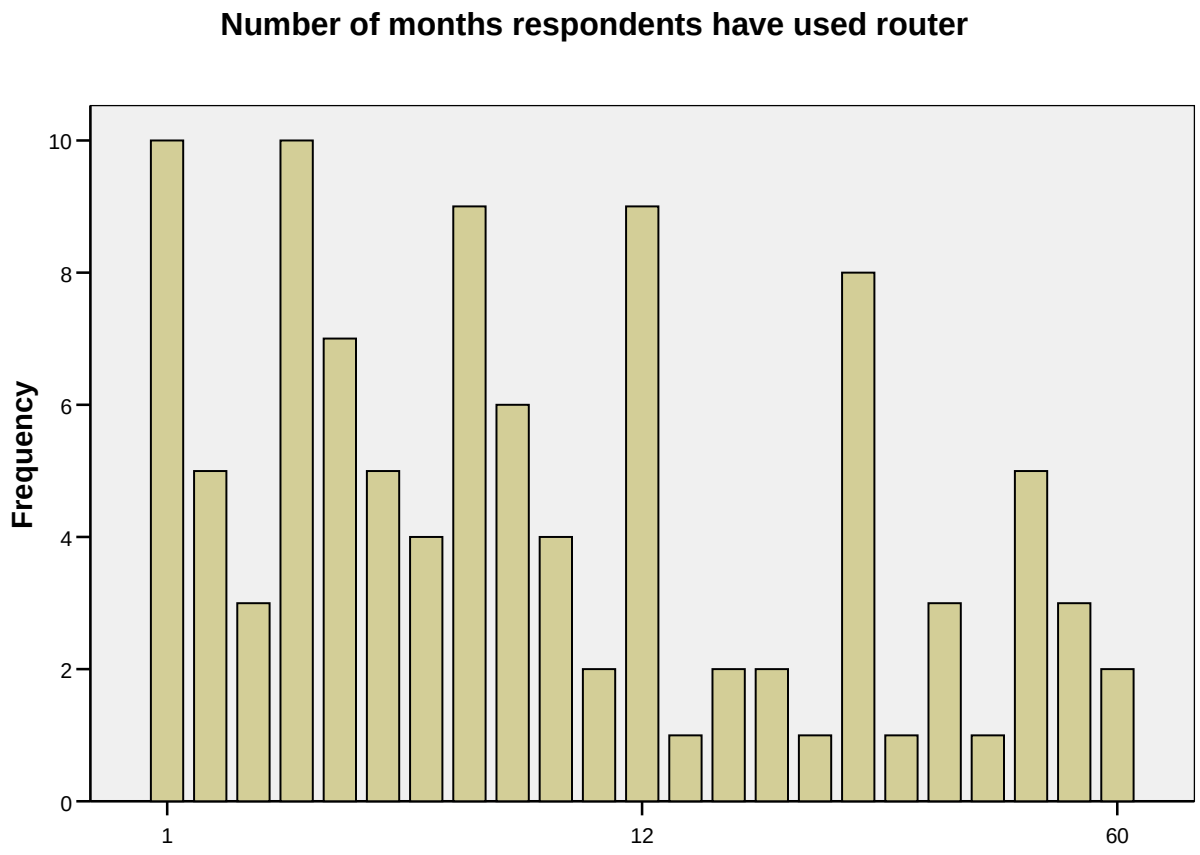


Similarly, a trimodal distribution was used to assess how the respondents fit into the three-tier subset of coping stages; this test concluded that there were Non-Intenders, Intenders, and Actors (n = 9, 12, 82, respectively). An individual was categorized as being in the "Actor" stage if that person had performed the recommended behavior (i.e., enabled the security settings on the wireless device); this was decision stage behavior (question) number seven in the survey instrument – see Appendix.

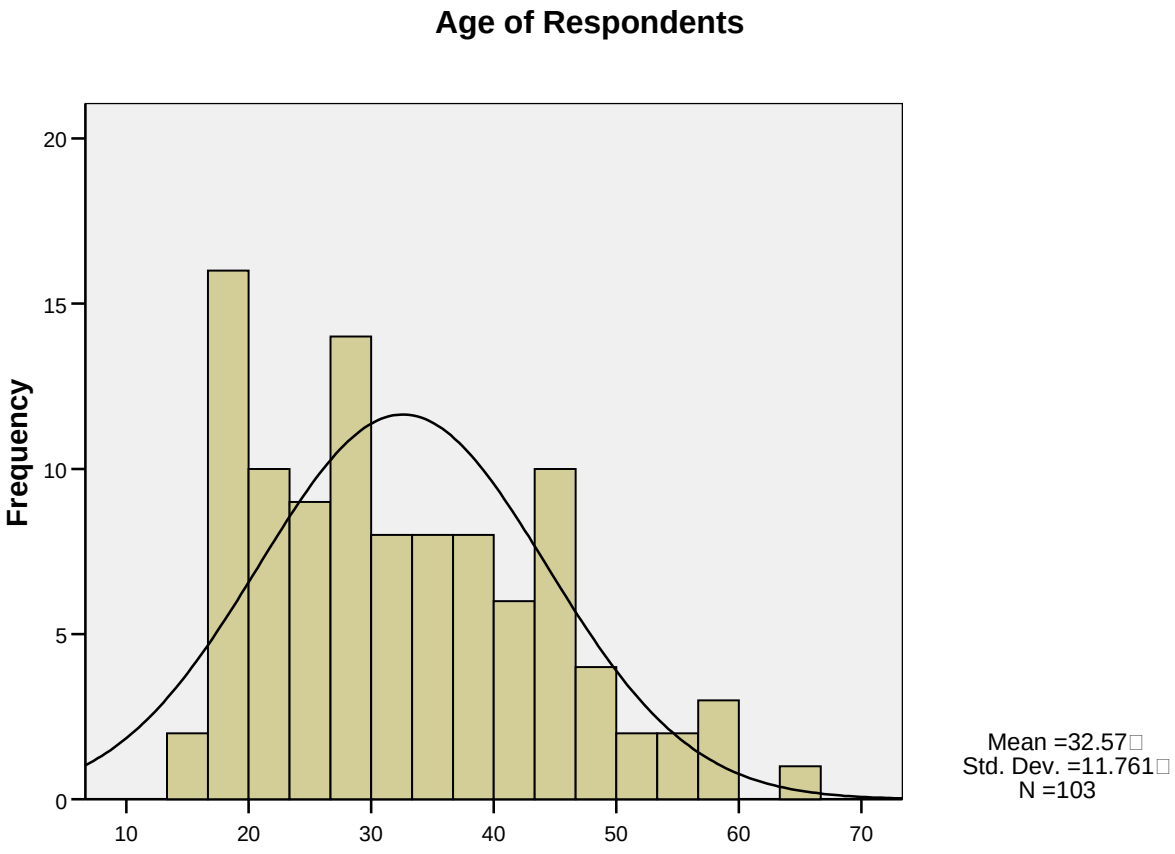
The remaining nine decision stage behaviors (questions) assessed the Non-Intenders and Intenders. An individual was categorized as a "Non-Intender" if that person had four or more behaviors that they answered as "will not do." All those who did not fall into the "Actor" or the "Non-Intender" categories were classified as "Intenders."



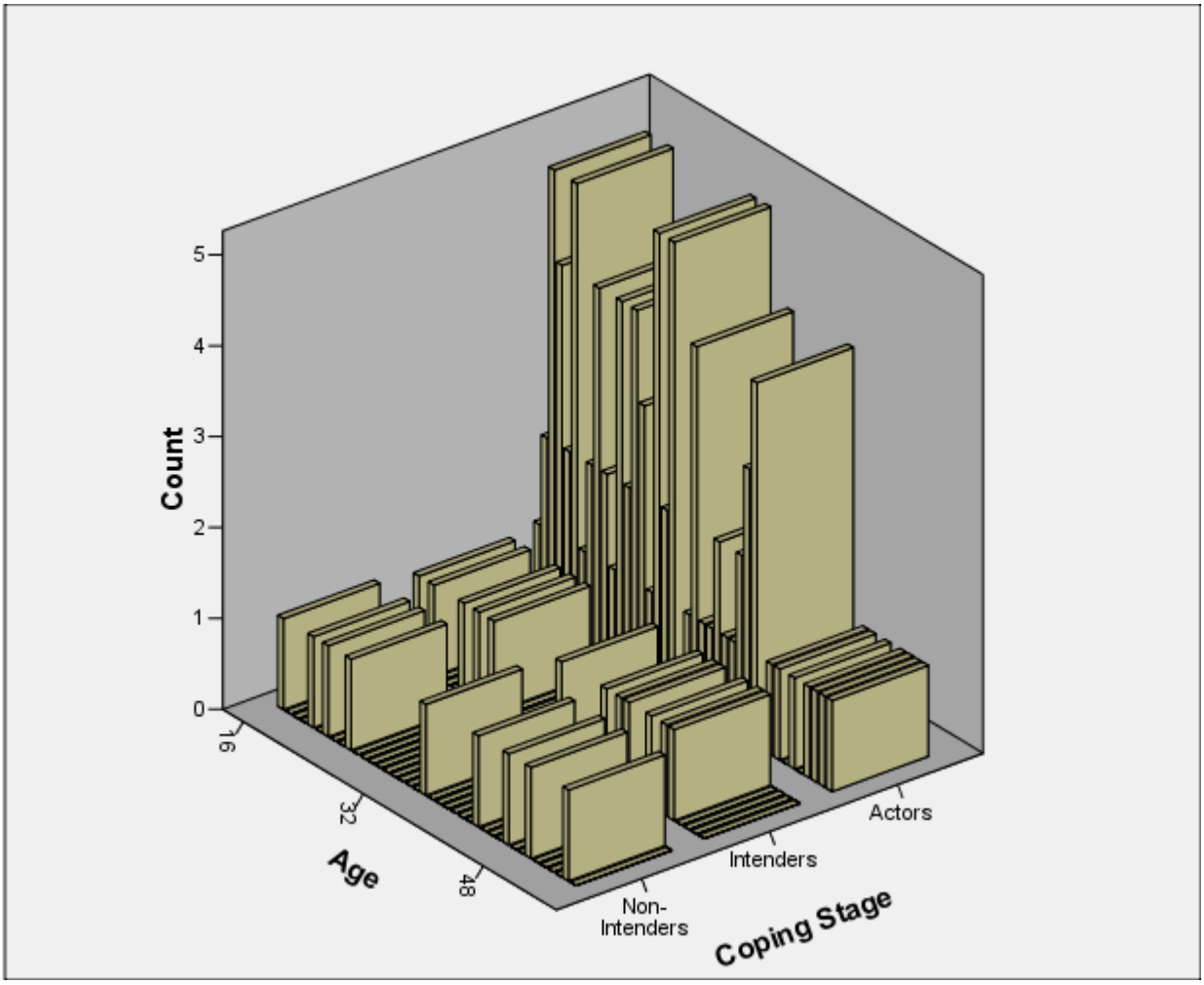
Respondents were asked how long they had been using a home wireless router. The average duration of use was 12.3 months.



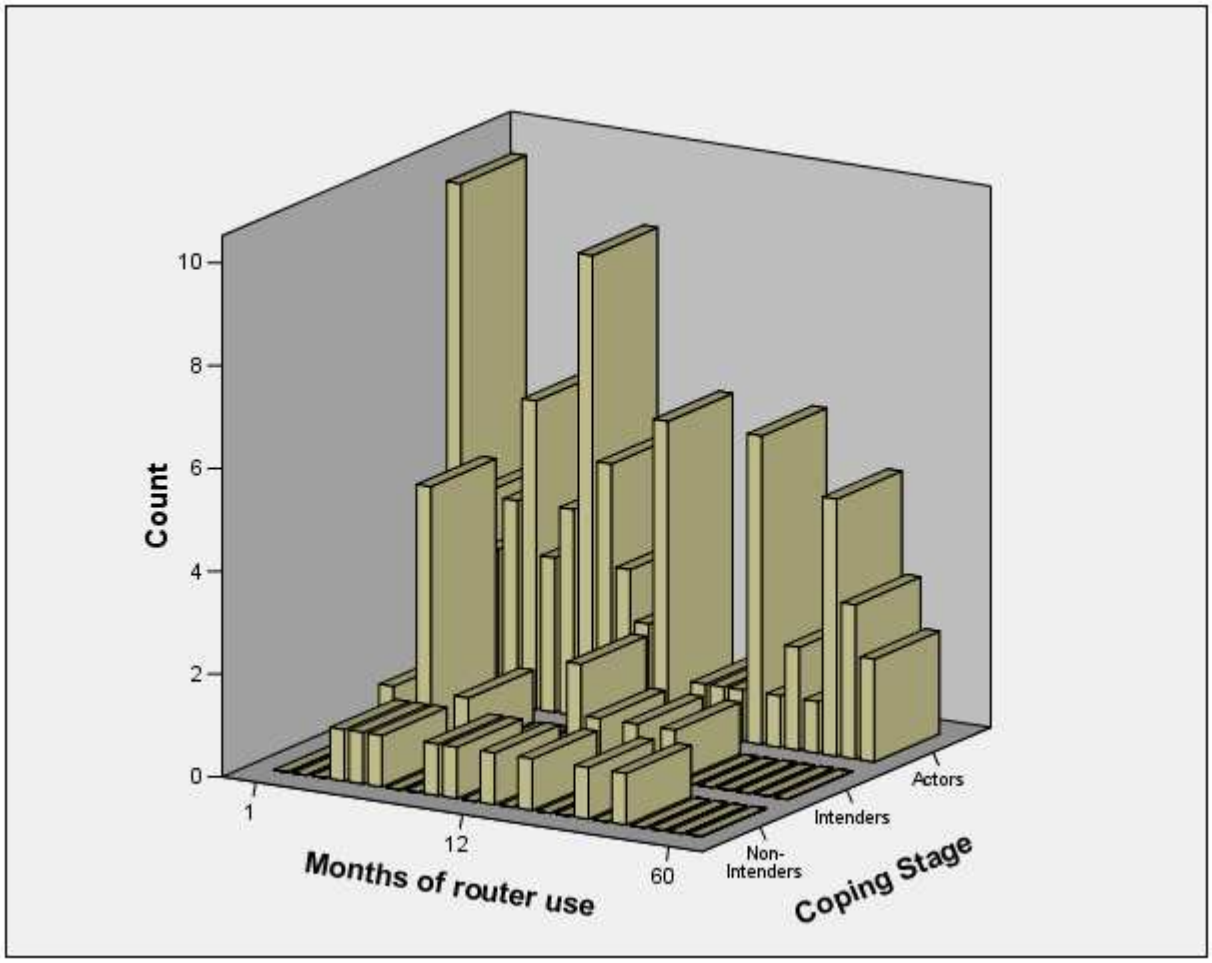
The results indicate the average age of the respondents was 32.



Comparing the age of the respondents to their respective coping stage reveals that there are relatively even distributions of ages within each stage. From this chart, it appears that age does not appear to be a factor in how respondents fit into a coping stage.



Comparing respondents' duration of use to their respective coping stages reveals that there are several respondents within the sample who have been using a home wireless router for more than 12 months, yet still do not intend on activating wireless security features.



Describing the Variables

The second part of this section describes the data collected relating to the independent variables through histograms.

Table 1 describes the test questions used in the survey instrument to gather data for each of the six independent variables (i.e., *perceived vulnerability, perceived severity, perceived rewards, response efficacy, self efficacy and response cost)*. Each question was assigned a code to aid in tracking and interpreting the data during statistical analysis. For example, there were two test questions used with *perceived vulnerability* independent variable; the first question was assigned the code 'PerVul1' and the second question was assigned the code 'PerVul2'. Each of the other questions used with the other five independent variables were coded in a similar manner.

To gather data concerning these test questions, the survey instrument used a seven-point Likert scale (where 1 = high/most and 7 = low/least).

Table 1: Independent Variable Test Questions	
Variable	**Items**
Perceived Vulnerability	I could be subjected to a malicious wireless hacking attempt *(Pervul1)*
	I feel that I could be vulnerable to wireless hacking *(PerVul2)*
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 of personal information resulting from wireless hacking is a serious problem for me *(PerSer4)*
Perceived Rewards	Enabling security measures on my home wireless network will make me feel safer (Rwrd1)
	In the next 6 months, how likely is it that your home wireless network will endure a hacking attempt (Rwrd2)
	Of the home wireless networks in New Zealand, how many do you think have enabled security measures (Rwrd3)
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 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)*
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)*

Histograms

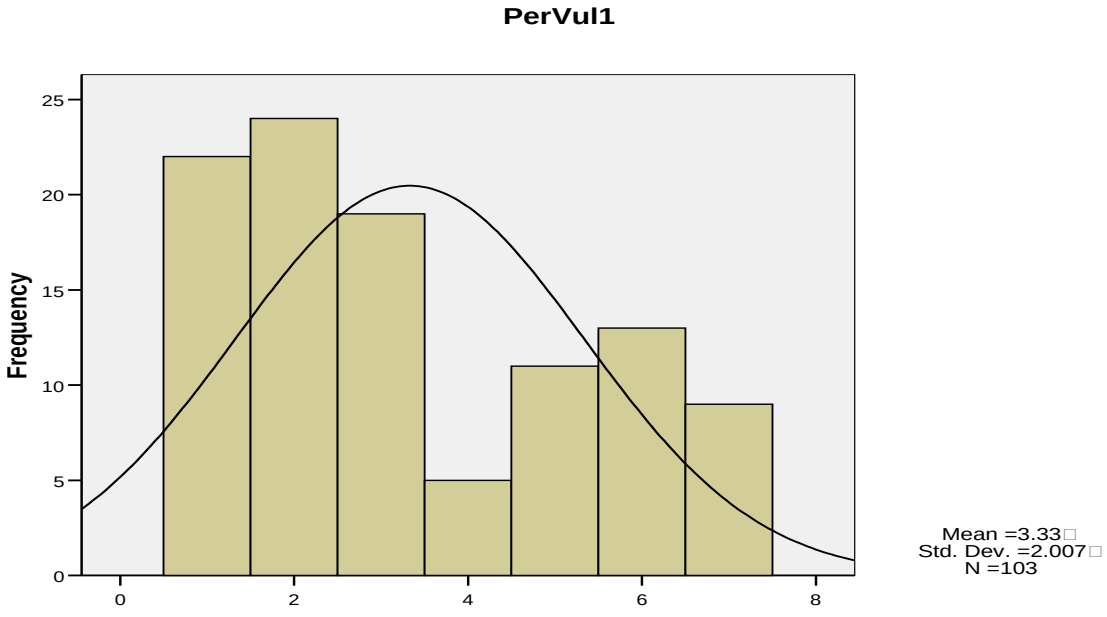
Simple histogram charts are used below to visual these results; the mean (average) of the scores as well as the standard deviation of the mean are also presented to help describe the data.

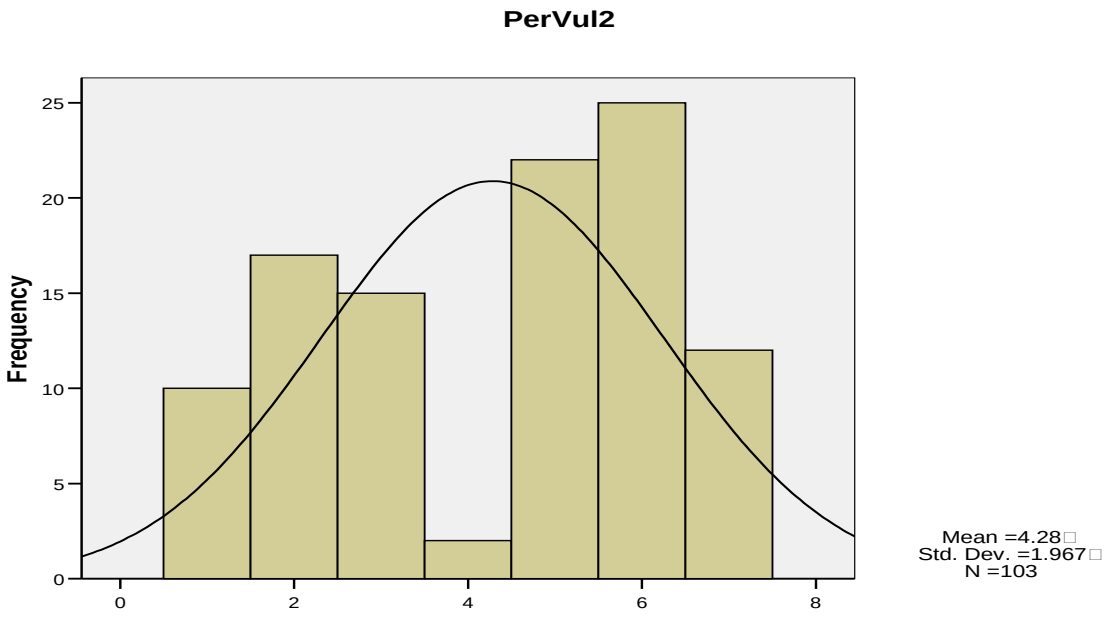
The mean represents a summary of the data for a scale item question. If that summary is not really representative of the actual scores, than the mean may not be completely reliable in representing the question in statistical analysis tests in which a 'poor' mean is compared against a more accurate mean.

To determine the accuracy of how well the mean represents the data for the question, the standard deviation is used. Small standard deviations (in relation to the value of the mean itself) indicate that data points are close to the mean (Field, 2005). Large standard deviations (in relation to the mean) indicate that the data points are distant from the mean (i.e., the mean is not an accurate representation of the data) (Field, 2005).

Based upon the theoretical investigation of these variables from the previous section, a positive skew should be present for *perceived vulnerability*; that is, the mean score would be on the higher end of the scale for each of these questions (i.e., most people would agree to feeling susceptible to wireless hacking).

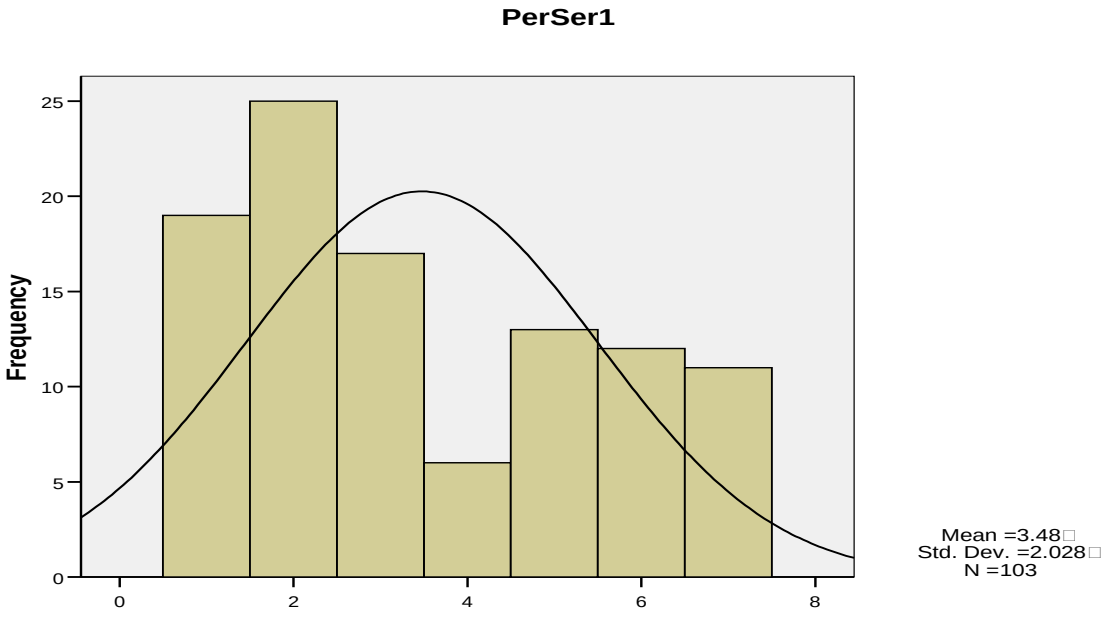
The histograms for PerVul1 and PerVul2 show that the positive skews did not occur; also, the high standard deviation scores (2.007 and 1.967, respectively) imply that the means (3.33 and 4.28, respectively) are not good fits for each question.

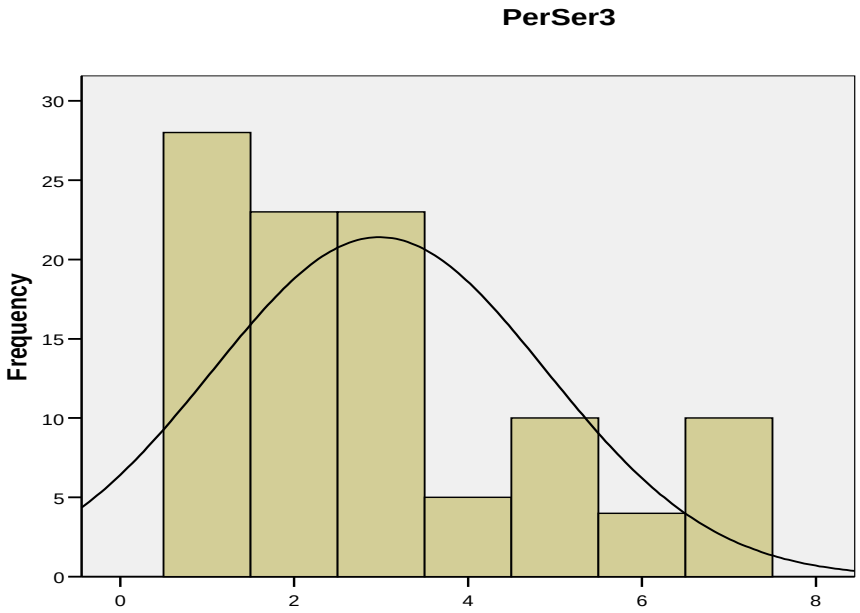


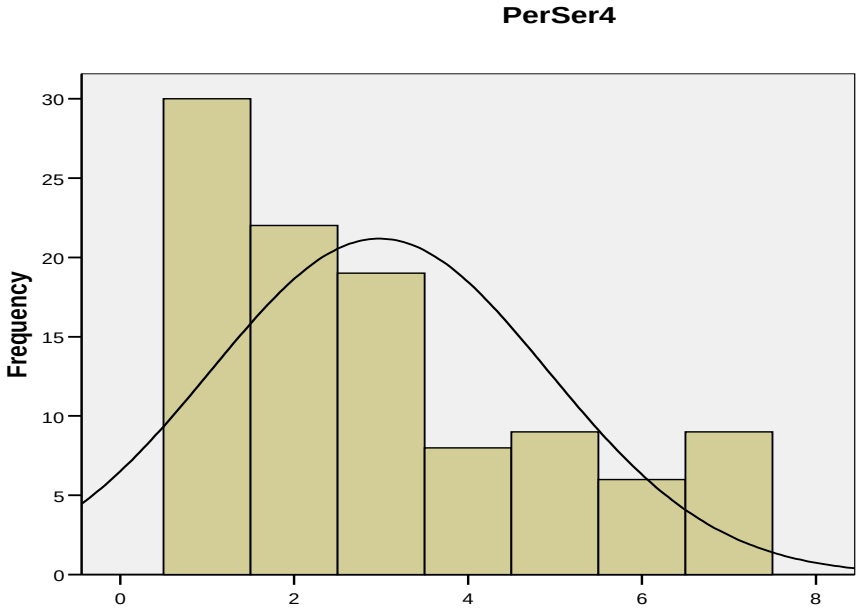


The PMT-based research suggests a positive skew should be present for *perceived severity*; that is, the mean score would be on the higher end of the scale for each of these questions (i.e., most people would agree that the threats posed from wireless hacking are a serious issue).

The histograms for PerSer1, PerSer2, PerSer3 and PerSer4 show that the positive skews did not occur; also, each scale item had a relatively high standard deviation scores compared to the mean. This implies that the means are not good fits for each item.

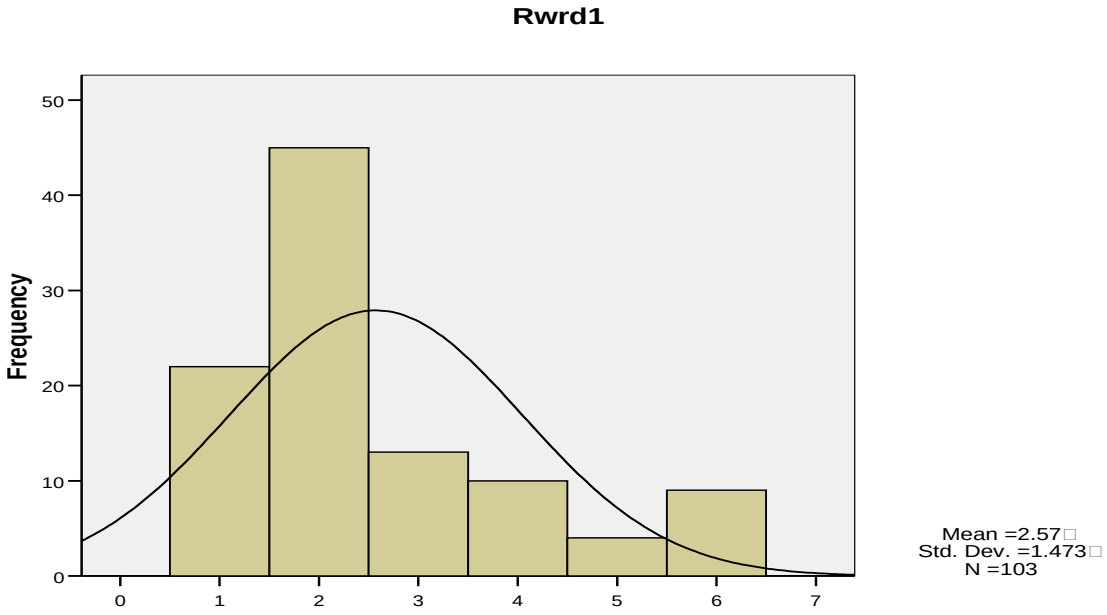


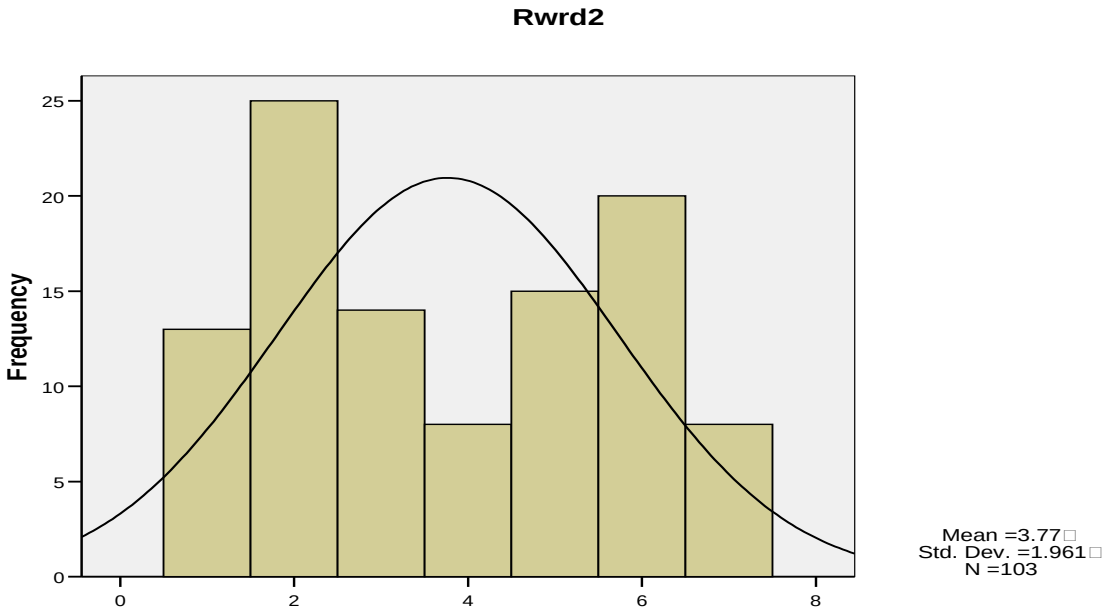

PerSer3
Frequency
30
25
20
15
10
5
0
0
2
4
6
8
Mean =2.98
Std. Dev. =1.92
N =103

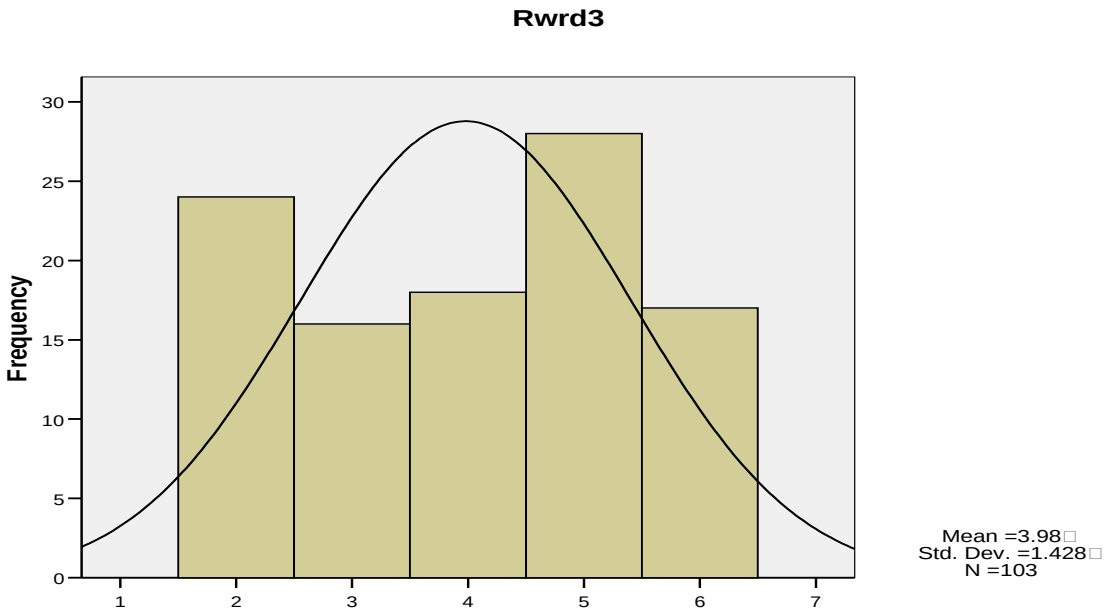

PerSer4
Frequency
30
25
20
15
10
5
0
0
2
4
6
8
Mean =2.98
Std. Dev. =1.94
N =103

The PMT-based research suggests a negative skew should be present for *perceived rewards*; that is, the mean score would be on the lower end of the scale for each of these questions.

The histograms for Rwrd1, Rwrd2 and Rwrd3 show that the negative skews did not occur; also, each scale item had relatively high standard deviation scores compared to the mean. This implies that the means are not good fits for each item:

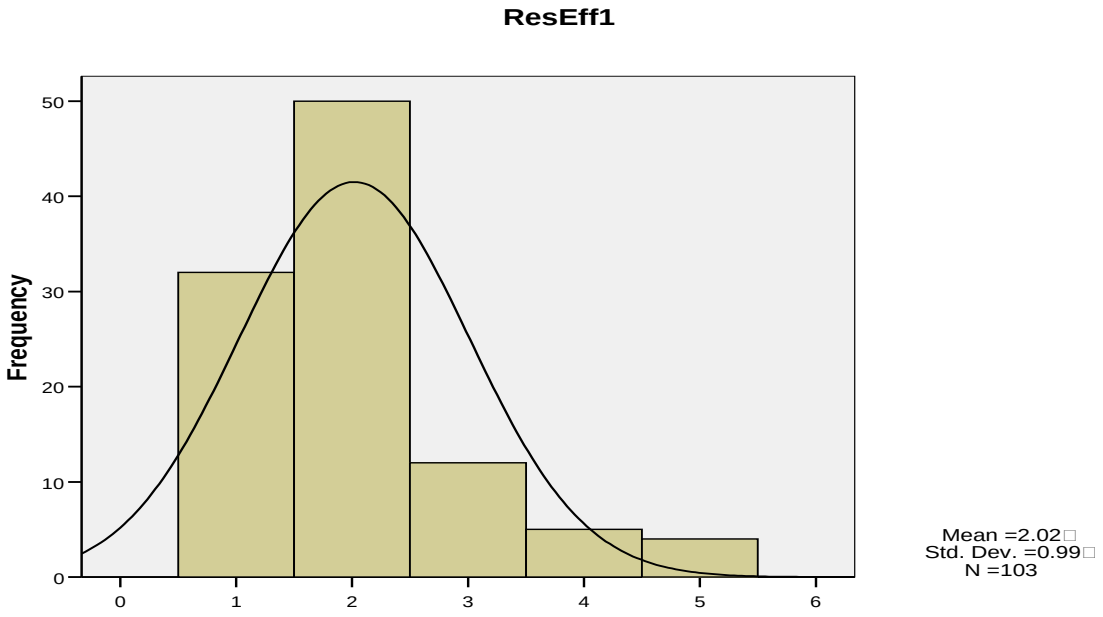


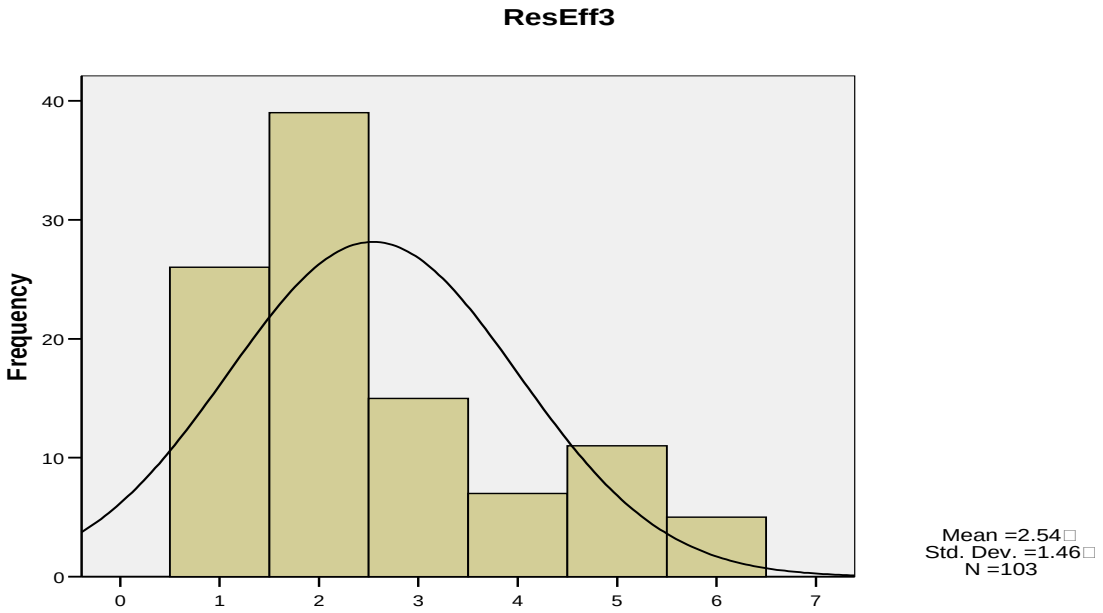


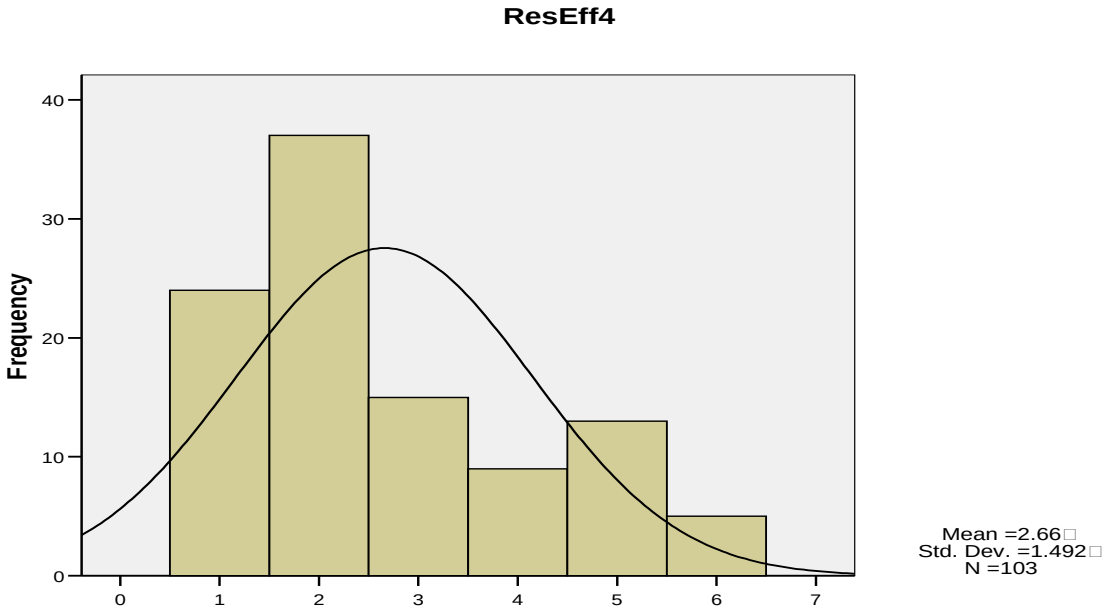


The PMT-based research suggests a positive skew should be present for *response efficacy*; that is, the mean score would be on the higher end of the scale for each of these questions (i.e., most people would agree that enabling security features will deter hacker attacks).

The histogram for the ResEff1 question shows the expected positive skew and the other three items (ResEff2, ResEff3, ResEff4) show a slightly positive skew. However, each of the four scale items had a relatively high standard deviation score compared to its mean. This implies that the means are not good fits for each item.



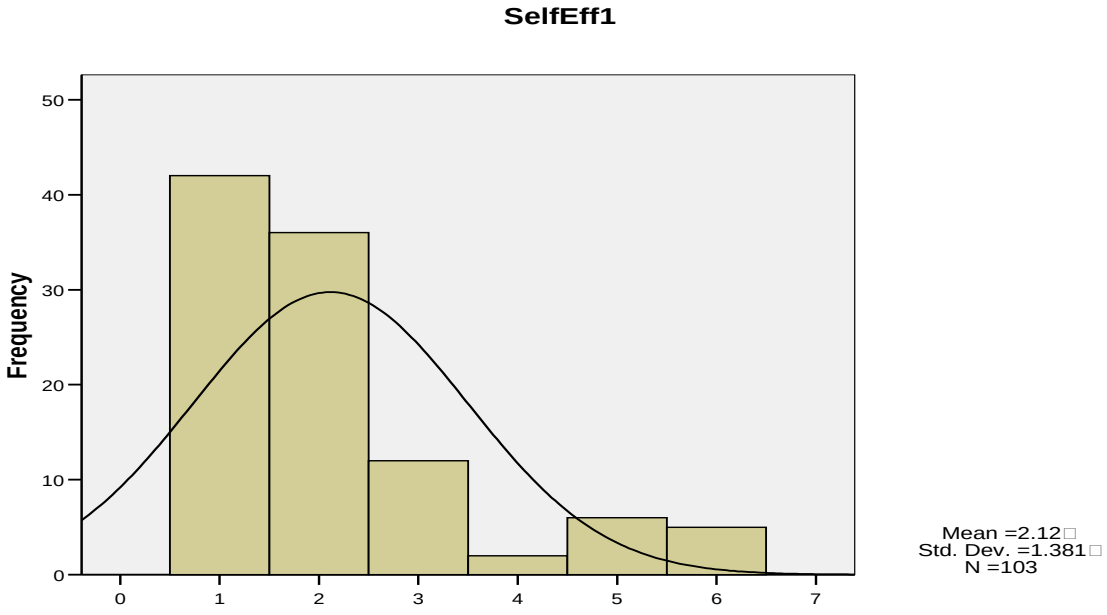


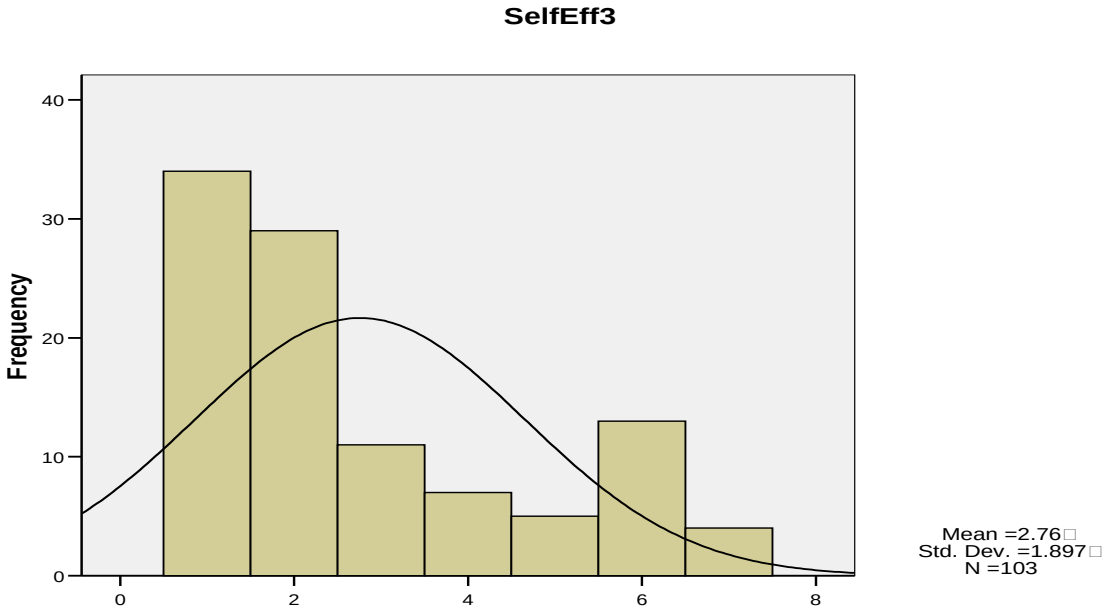


The PMT-based research suggests a positive skew should be present for *self efficacy*; that is, the mean score would be on the higher end of the scale for each of these questions (i.e., most people

would probably feel like they could enable security features by themselves and not need some form of human assistance to help them getting enabled).

The histograms for SelfEff1, SelfEff2 and SelfEff3 show that slightly positive skews did occur. However, each scale item had a relatively high standard deviation scores compared to the mean. This implies that the means are not good fits for each item.

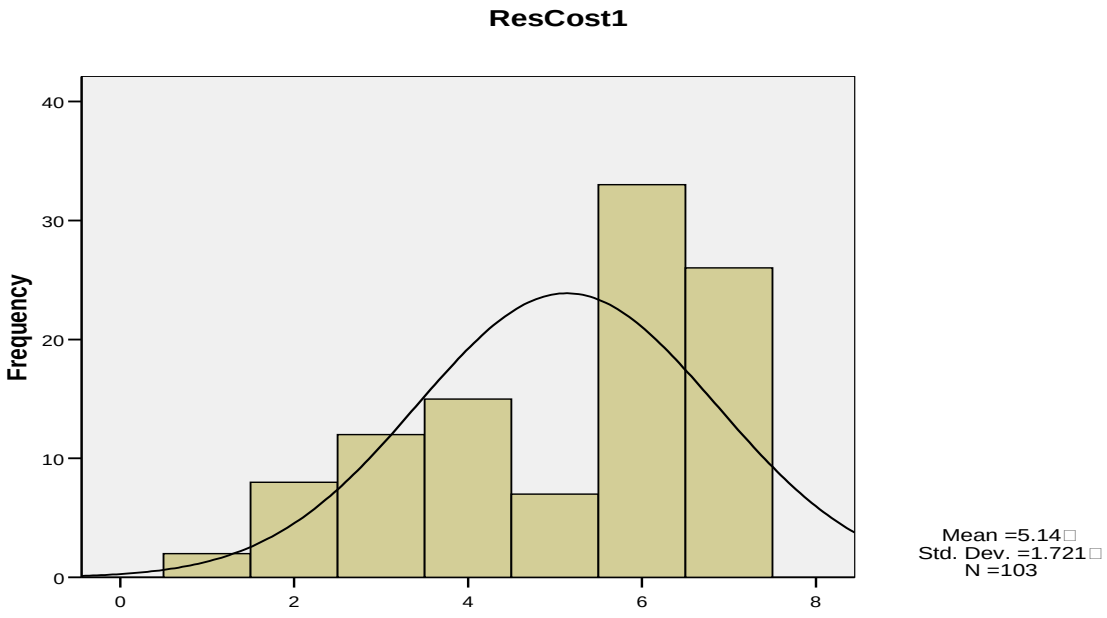


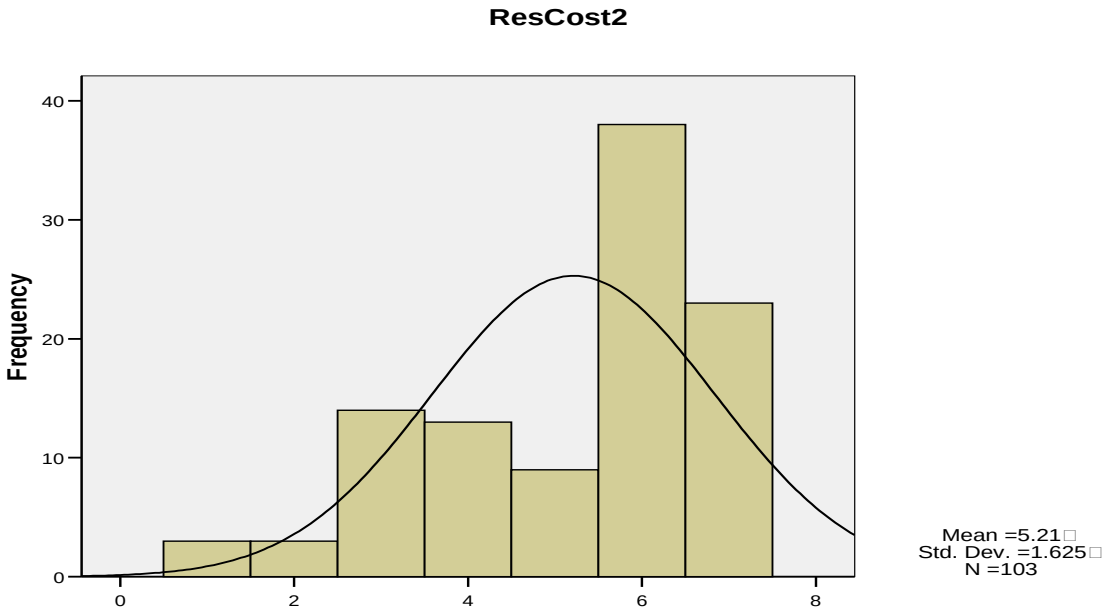


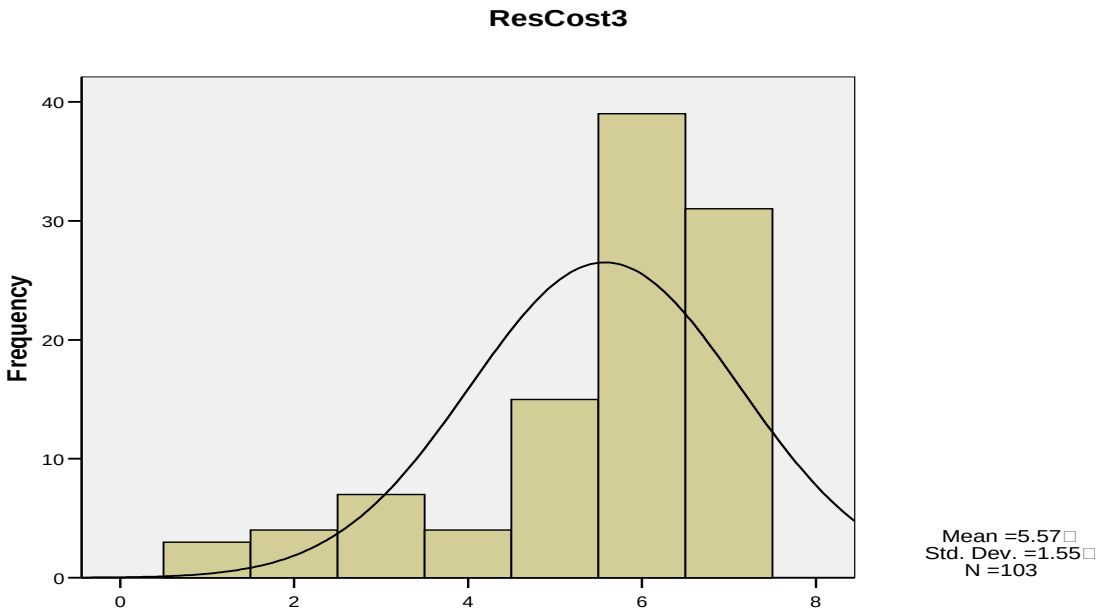
The PMT-based research suggests a negative skew should be present for *response cost*; that is, the mean score would be on the lower end of the scale for each of these questions (i.e., most

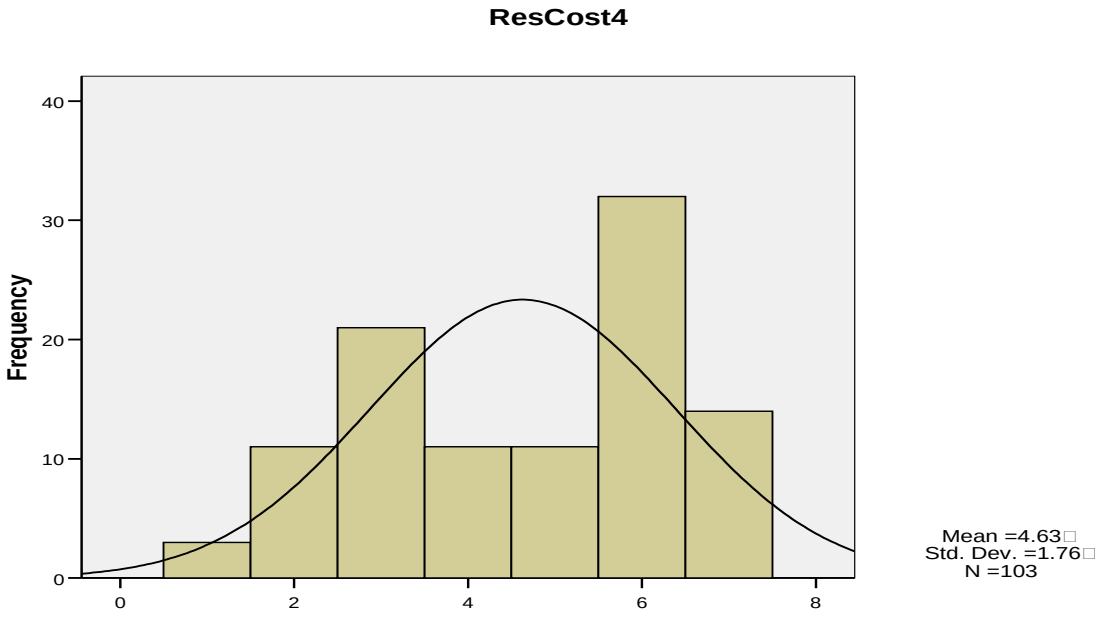
people would agree that enabling security features would be easy and would not require extra efforts of time and money on their part).

The histograms for ResCost1, ResCost2 and ResCost3 show that slightly negative skews did occur, but ResCost4 does not show this trend. Each scale item however, had a relatively low standard deviation score compared to its mean. This implies that the means could possibly be good fits for each item.




ResCost2
Frequency
40
30
20
10
0
0
2
4
6
8
Mean =5.21
Std. Dev. =1.625
N =103


ResCost3
Frequency
40
30
20
10
0
0
2
4
6
8
Mean =5.57
Std. Dev. =1.55
N =103



Testing Hypothesis One

The third part of this section begins by examining the patterns illustrated within the above histograms to find out if there are in fact underlying groups of people who can be classified as concerned or not concerned about wireless security. These observations are then confirmed via statistical testing.

Each one of the above histograms shows a relatively uneven distribution of response values – only a handful of the items show strong means values. The most recognizable pattern emerging from nearly each scale item is one of a group of response values clustered on the high end of the scale and a group of response values clustered on the lower end of the scale. That is, two distributions appear on an individual scale: one group of responses distributed between 1-3 and another group of response distributed between 5-7. (For example, the PerVul2 question clearly showed two distributions on the response scale.) This helps to corroborate the belief that there is a dichotomy of respondents. But to validate the postulation that two (or more) series of these scale item readings represent basically the same or significantly different values, the T-Test is performed on the independent variables. The T-Test assesses whether the means of two groups are statistically different from each other (T-Test, 2008).

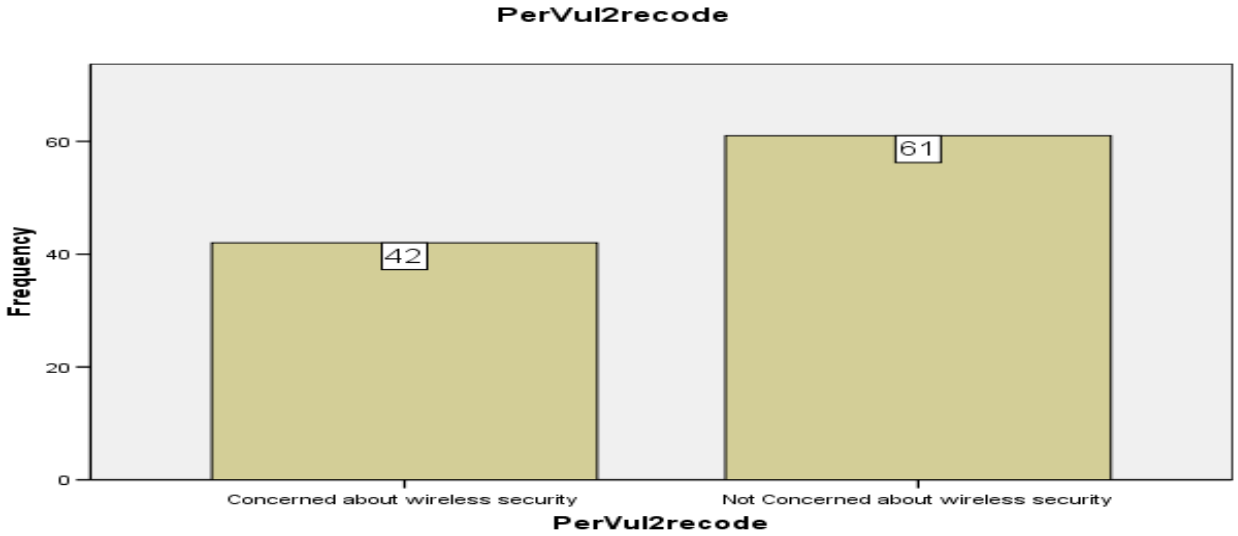
Independent Samples T-Test

The T-Test compares one grouping variable against the twenty independent variables. For this research, the grouping variable is constructed by taking the PerVul2 scale item (i.e., because the original histogram clearly showed two distributions on the response scale) and recoding as a grouping or classification variable. The resulting variable categorizes responses 1-3 as the people who feel concerned about wireless security and responses 4-7 as the people who do not feel concerned about wireless security.

With an Independent Samples T-Test, the equality of variances must first be assessed to determine whether the variances from the two samples are different (Levene's F-Test for Equality of Variances). If the p-value is greater than .05 than the two variances are approximately equal – the 'equal variances assumed' output is used for interpreting the T-Test. If the "Sig.", or p-value, is less than .05 than the two variances are significantly different – the 'equal variances not assumed' output is used for interpreting the T-Test.

The t-value itself will be positive if the first mean is larger than the second and negative if it is smaller. The larger the t-value, the less likely it occurred by chance (Field, 2005).

The recoded PerVul2 variable classifies 42 respondents as 'concerned' (the distribution of respondents in the high end of the scales) and 61 respondents as 'not concerned' (the distribution of respondents in the low end of the scales).



The below Group Statistics and Independent Samples T-Test tables indicate:

- Eight of the twenty scale items do not have statistically different groups in their means: Rwrd1-3, ResEff1-4 and SelfEff3.
    - For each of these items it is apparent in the Group Statistics table that the reported means for each item appear too close to be dissimilar. Plus in the Independent Samples T-Test table, the F-Test results for each item show that the t-value is not significant (at $p < .01$ level [2-tailed]).
- Twelve of the twenty scale items do have two statistically distinct groups in their sample means: PerVul1-2, PerSer1-4, SelfEff1-2 and ResCost1-4.
    - Each of these items showed considerable differences in the means per item (Group Statistics Table) as well as significant results in the Independent Samples T-Test table within each F-Test (at the $p < .01$ level [2-tailed]).

Group Statistics

	PerVul2recode	N	Mean	Std. Deviation	Std. Error Mean
PerVul1	Concerned about wireless security	42	2.48	1.330	.205
	Not Concerned about wireless security	61	3.92	2.186	.280
PerVul2	Concerned about wireless security	42	2.12	.772	.119
	Not Concerned about wireless security	61	5.77	.804	.103
PerSer1	Concerned about wireless security	42	2.86	1.788	.276
	Not Concerned about wireless security	61	3.90	2.087	.267
PerSer2	Concerned about wireless security	42	2.95	1.794	.277
	Not Concerned about wireless security	61	4.02	2.117	.271
PerSer3	Concerned about wireless security	42	2.29	1.384	.214
	Not Concerned about wireless security	61	3.46	2.094	.268
PerSer4	Concerned about wireless security	42	2.26	1.432	.221
	Not Concerned about wireless security	61	3.48	2.094	.268
Rwrd1	Concerned about wireless security	42	2.52	1.452	.224
	Not Concerned about wireless security	61	2.61	1.498	.192
Rwrd2	Concerned about wireless security	42	3.71	1.979	.305
	Not Concerned about wireless security	61	3.80	1.965	.252
Rwrd3	Concerned about wireless security	42	3.88	1.485	.229
	Not Concerned about wireless security	61	4.05	1.396	.179
ResEff1	Concerned about wireless security	42	2.14	1.072	.165
	Not Concerned about wireless security	61	1.93	.929	.119
ResEff2	Concerned about wireless security	42	2.50	1.293	.199
	Not Concerned about wireless security	61	2.30	1.333	.171
ResEff3	Concerned about wireless security	42	2.71	1.519	.234
	Not Concerned about wireless security	61	2.43	1.420	.182
ResEff4	Concerned about wireless security	42	2.86	1.555	.240
	Not Concerned about wireless security	61	2.52	1.445	.185
SelfEff1	Concerned about wireless security	42	2.74	1.624	.251
	Not Concerned about wireless security	61	1.69	.992	.127
SelfEff2	Concerned about wireless security	42	3.00	1.753	.271
	Not Concerned about wireless security	61	1.80	1.222	.156
SelfEff3	Concerned about wireless security	42	2.93	1.731	.267
	Not Concerned about wireless security	61	2.64	2.009	.257
ResCost1	Concerned about wireless security	42	4.29	1.642	.253
	Not Concerned about wireless security	61	5.72	1.529	.196
ResCost2	Concerned about wireless security	42	4.55	1.549	.239
	Not Concerned about wireless security	61	5.67	1.524	.195
ResCost3	Concerned about wireless security	42	4.90	1.605	.248
	Not Concerned about wireless security	61	6.03	1.341	.172
ResCost4	Concerned about wireless security	42	3.95	1.780	.275
	Not Concerned about wireless security	61	5.10	1.599	.205

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
PerVul1	Equal variances assumed	30.905	.000	-3.814	101	.000	-1.442	.378	-2.192	-.692
	Equal variances not assumed			-4.155	99.688	.000	-1.442	.347	-2.130	-.753
PerVul2	Equal variances assumed	.240	.625	-23.023	101	.000	-3.651	.159	-3.966	-3.337
	Equal variances not assumed			-23.201	90.618	.000	-3.651	.157	-3.964	-3.339
PerSer1	Equal variances assumed	4.569	.035	-2.642	101	.010	-1.044	.395	-1.829	-.260
	Equal variances not assumed			-2.719	96.166	.008	-1.044	.384	-1.807	-.282
PerSer2	Equal variances assumed	5.298	.023	-2.664	101	.009	-1.064	.399	-1.856	-.272
	Equal variances not assumed			-2.746	96.632	.007	-1.064	.387	-1.833	-.295
PerSer3	Equal variances assumed	15.061	.000	-3.181	101	.002	-1.173	.369	-1.905	-.442
	Equal variances not assumed			-3.422	100.869	.001	-1.173	.343	-1.853	-.493
PerSer4	Equal variances assumed	11.662	.001	-3.264	101	.002	-1.214	.372	-1.951	-.476
	Equal variances not assumed			-3.492	100.999	.001	-1.214	.348	-1.903	-.524
Rwrd1	Equal variances assumed	.177	.675	-.279	101	.781	-.083	.297	-.671	.506
	Equal variances not assumed			-.281	90.032	.780	-.083	.295	-.669	.503
Rwrd2	Equal variances assumed	.023	.881	-.225	101	.822	-.089	.395	-.873	.695
	Equal variances not assumed			-.225	87.879	.823	-.089	.396	-.875	.697
Rwrd3	Equal variances assumed	.353	.554	-.586	101	.559	-.168	.287	-.738	.402
	Equal variances not assumed			-.579	84.640	.564	-.168	.291	-.746	.410
ResEff1	Equal variances assumed	1.437	.233	1.051	101	.296	.208	.198	-.185	.602
	Equal variances not assumed			1.023	79.744	.309	.208	.204	-.197	.614
ResEff2	Equal variances assumed	.110	.741	.776	101	.440	.205	.264	-.319	.729
	Equal variances not assumed			.781	90.059	.437	.205	.263	-.317	.727
ResEff3	Equal variances assumed	.150	.699	.984	101	.328	.288	.293	-.293	.869
	Equal variances not assumed			.971	84.316	.334	.288	.297	-.302	.878
ResEff4	Equal variances assumed	.578	.449	1.113	101	.268	.333	.299	-.260	.925
	Equal variances not assumed			1.098	83.947	.275	.333	.303	-.270	.935
SelfEff1	Equal variances assumed	14.408	.000	4.068	101	.000	1.050	.258	.538	1.561
	Equal variances not assumed			3.736	61.992	.000	1.050	.281	.488	1.611
SelfEff2	Equal variances assumed	9.955	.002	4.085	101	.000	1.197	.293	.616	1.778
	Equal variances not assumed			3.829	67.846	.000	1.197	.313	.573	1.820
SelfEff3	Equal variances assumed	1.038	.311	.759	101	.450	.289	.381	-.467	1.045
	Equal variances not assumed			.780	95.934	.437	.289	.371	-.447	1.025
ResCost1	Equal variances assumed	1.683	.198	-4.543	101	.000	-1.436	.316	-2.062	-.809
	Equal variances not assumed			-4.483	84.079	.000	-1.436	.320	-2.072	-.799
ResCost2	Equal variances assumed	2.321	.131	-3.655	101	.000	-1.125	.308	-1.735	-.514
	Equal variances not assumed			-3.644	87.359	.000	-1.125	.309	-1.738	-.511
ResCost3	Equal variances assumed	8.308	.005	-3.869	101	.000	-1.128	.292	-1.706	-.550
	Equal variances not assumed			-3.743	77.640	.000	-1.128	.301	-1.728	-.528
ResCost4	Equal variances assumed	1.182	.280	-3.413	101	.001	-1.146	.336	-1.812	-.480
	Equal variances not assumed			-3.345	81.934	.001	-1.146	.343	-1.827	-.464

Testing Hypothesis Two

The last part of this section explains and executes several statistical analyses with the aim of testing the data in the context of the statements contained within Hypothesis Two (i.e., determining the factors that influence behavioural intention).

It has been noted that the mean values emerging for many of the independent variables are not good summaries of their respective models. This does not necessarily imply that statistical analyses should not be performed with these mean values, rather it suggests that any test results coming out of these analyses may not accurately reflect what occurs in the actual population of wireless router users in New Zealand. Therefore, testing of the six postulations contained within Hypothesis Two continues below beginning with a factor analysis and a reliability analysis to assess the validity and reliability of the independent variables. Then, correlation analysis and regression analysis are used to relate the variables and predict outcomes for dependent variable from one or more of the independent variables.

Factor Analysis

Factor analysis is a technique for identifying groups or clusters of variables (Field, 2005). Performing a factor analysis on the independent variables will help to understand the structure of the set of variables; that is, it will help to visualize that the questions used to assess each independent variable are really measuring the concept within that variable which they are supposed to. For example, are the four questions regarding response efficacy all really measuring the concept of response efficacy.

KMO

The Kaiser-Meyer-Olkin (KMO) statistic is used to measure sampling adequacy. The KMO produces a statistical value between 0 and 1: a result close to 0 indicates dispersion in the pattern of relationships (consequently, factor analysis is likely an unsuitable for correlating factors); a result close to 1 indicates that patterns of relationships are relatively compact (as a result, factor analysis should yield distinct and reliable factors) (Field, 2005). Values between 0.5 and 0.7 are mediocre, values between 0.7 and 0.8 are good, values between 0.8 and 0.9 are great, and values

above 0.9 are superb (Hutcheson & Sofroniou, 1999). Therefore, values of more than 0.5 are considered acceptable in this study.

Validity

Testing for validity was done by utilizing factor analysis with principal component analysis and varimax rotation. Varimax rotation is a method of orthagonal rotation in statistical factor analysis. The calculation methods in orthagonal rotation try to keep the underlying factors independent (i.e., not correlated); this means that varimax calculations try to load a smaller numbers of variables highly onto each factor (Field, 2005). The result is simply more interpretable clusters of factors in the output scores. Output scores (or, loadings) of 0.45 to 0.54 are considered fair results; 0.55 to 0.62 good results; 0.63 to 0.70 very good results; and above 0.71 excellent results for assessing validity of the variables (Comrey 1973).

For this study, there are two methods to interpret and use these validity scores. The first is to test for convergent validity. Convergent validity defines the extent to which a scale item (question) is similar to (converges on) other scale items that it theoretically should also be similar to (Construct Validity, 2008). The second way is test for discriminant validity. Discriminant validity explains the degree to which the scale items do not correlate with other scale items that they theoretically should not be similar to (Cook and Campbell, 1979). These methods work together – if proof can be provided for both convergent and discriminant validity, then evidence for construct validity is demonstrated (Construct Validity, 2008).

Reliability Analysis

The concept of reliability suggests that a scale should consistently reflect the variable it is measuring (Field, 2005); Cronbach's alpha is used to test reliability (Cronbach, 1951). Cronbach's Alpha α describes whether or not the items in the resulting output factors are measuring the same thing. It does this by assessing the correlation between each item and the total of all items in the scale. Research suggests that the high reliability of variables can be seen with alpha results above 0.70; however, reliability results of 0.50 to 0.60 are sufficient in early stages of research (Nunnally, 1978). Therefore, alpha values of more than 0.50 are considered acceptable in this study.

Initial Analysis Results

Table 2 indicates the KMO for all six of the independent variables. The KMO value of 0.76 suggests that factor analysis should yield distinct and reliable factors and therefore is an acceptable score for this study.

Table 2: KMO	
Kaiser-Meyer-Olkin Measure of Sampling Adequacy	0.76

Table 3 indicates the validity loading scores for all six of the independent variables. The factor analysis of the twenty scale items resulted in five components. Near the bottom of the table, a row of output indicates that the five components have eigenvalues over 1.00 (eigenvalues greater than 1.00 are regarded as important as they account for a significant amount of the variability in the data). These five components explained 73.11% of the total cumulative variance; however, the two main factors account for slightly less than 40% of the total % of variance (ideally the two main factors should together account for at least 40-50% of the total % of variance).

Table 3: Validity of Variables					
	Component				
	1	2	3	4	5
PerVul1	0.63				0.48
PerVul2					
PerSer1	0.92				
PerSer2	0.90				
PerSer3	0.94				
PerSer4	0.92				
Rwrd1		0.75			
Rwrd2					0.57
Rwrd3					0.75
ResEff1		0.71			
ResEff2		0.82			
ResEff3		0.92			
ResEff4		0.93			
SelfEff1			0.91		
SelfEff2			0.88		
SelfEff3			0.56		
ResCost1				0.87	
ResCost2			-0.40	0.82	
ResCost3			-0.71	0.43	
ResCost4			-0.62	0.43	
Eigenvalues	4.29	3.63	3.25	2.08	1.38
% of Variance	21.44	18.15	16.24	10.40	6.89
% of Cumulative Variance	21.44	39.58	55.82	6.89	73.11

* values under 0.4 have been suppressed within the output.
Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

Convergent validity was tested by checking loadings to see if items for the same variables correlated highly among themselves. Testing for discriminant validity was done by assessing the factor loadings to see if items loaded more highly on their intended variables than on other variables.

Upon initial inspection of the scale item scores in Table 3 (above), the output indicates that there is a chance of collinearity between some of the independent variables – that is, several items did

not load cleanly into their respective variable categories. For example, the *perceived vulnerability* and *perceived severity* variables appear to have loaded onto the same component. The *perceived rewards* are spread across the table and do not appear to be valid for any single component. The last two scale items in the response cost variable appear to be loading across two different components; however the other remaining questions came close to having at least fair loadings on their proposed variables.

Table 4 indicates the reliability scores for all six of the independent variables. Five of the six variables have acceptable alpha scores; however, the *perceived rewards* variable is less than the minimum acceptable value of 0.5.

Table 4: Reliability of Variables

Variable	No. of Items	Cronbach Alpha
Perceived Vulnerability *(PerVul)*	2	0.64
Perceived Severity *(PerSer)*	4	0.95
Perceived Rewards *(Rwrd)*	3	0.42
Response Efficacy *(ResEff)*	4	0.90
Self Efficacy *(SelfEff)*	3	0.73
Response Cost *(ResCost)*	4	0.84

The results from Table 3 indicate that the last two scale items of the *response cost* variable should be removed from the analysis; the last two remaining items should then load cleanly onto that variable component. More importantly though, Tables 3 and 4 indicate that the *perceived rewards* variable should be removed entirely from the analysis since the three scale items are not necessarily measuring the same variable; plus, the reliability alpha result is below the acceptable level for this study.

The Re-Analysis Results

All three of the scale items from *perceived rewards* were removed plus two of the four scale items from *response cost* were removed and the factor analysis re-generated.

Table 2-A indicates the KMO went slightly down from previously. The score of 0.726 is still acceptable for this study though.

Table 2-A: KMO	
Kaiser-Meyer-Olkin Measure of Sampling Adequacy	0.726

Table 3-A indicates the newest factor analysis resulted in four components. All four of the components have eigenvalues over 1.00 (which is significant here) and they explain 76.88% of the total cumulative variance. Additionally, the two main factors account for slightly less than 49.3% which is ideal. The rows pertaining to the remaining fifteen scale items show that the scale items for *perceived vulnerability* and *perceived severity* are all falling into the same component (i.e., all six questions are actually measuring the same thing and not two different components). More importantly, the remaining three components within the table all load cleanly onto their respective variable categories – thus indicating that the scale items measure their intended component.

Table 3-A: Validity of Variables				
	Component			
	1	2	3	4
PerVul1	0.72			
PerVul2	0.49			
PerSer1	0.90			
PerSer2	0.90			
PerSer3	0.93			
PerSer4	0.93			
ResEff1		0.76		
ResEff2		0.85		
ResEff3		0.94		
ResEff4		0.93		
SelfEff1			0.88	
SelfEff2			0.85	
SelfEff3			0.65	
ResCost1				0.92
ResCost2				0.86
Eigenvalues	4.28	3.12	2.22	1.92
% of Variance	28.50	20.79	14.78	12.80
% of Cumulative Variance	28.50	49.29	64.07	76.88

* values under 0.4 have been suppressed within the output.
Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

Lastly, Table 4-A indicates that the reliability scores for the four different components all have acceptable alpha scores above the minimum satisfactory value of 0.5.

Table 4-A: Reliability of Variables		
Variable	**No. of Items**	**Cronbach Alpha**
Perceived Vulnerability *(PerVul)* + Perceived Severity *(PerSer)*	6	0.90
Response Efficacy *(ResEff)*	4	0.90
Self Efficacy *(SelfEff)*	3	0.73
Response Cost *(ResCost)*	2	0.86

Testing the Relationships

Correlation analysis is used to relate the dependent and independent variables. Regression analysis is used to predict outcomes for the dependent variable from one or more of the independent variables. To begin with, the bimodal dependent variable measures are assessed and discussed in the below analyses. The coping stages are then evaluated for important relationships and predictions; however the sample size presents some issues regarding the analysis tables.

It is important to note that the dualistic dependent variable of 'Enabled' – 'Not Enabled' is labeled as "*PMT*" in the following tables. The data for this variable from respondents is derived directly from the survey instrument (See Appendix) Decision Stage question number seven (i.e., the 'Already Done' response equals Enabled and all other responses equal Not Enabled). What's more, in keeping with the results emerging from the factor analysis, only the fifteen scale items for the independent variables are included in these analyses.

Correlation

The Pearson correlation statistic *r* is a standardized computation of the power of the relationship linking two variables (Pearson, 1896). This statistic can "take any value from -1 (as one variable changes, the other changes in the opposite direction by the same amount), through 0 (as one variable changes the other does not change at all), to +1 (as one variable changes, the other changes in the same direction by the same amount)" (Field, 2005). The resultant values are referred to as effect sizes. Cohen (1988, 1992) describes how the effect sizes can be interpreted as compared to the strength of the relationship they measure. For example:

R = .10: small effect (to the relationship);

R = .30: medium effect;

R = .50: large effect.

When performing correlational analyses it is important to use two-tailed significance tests when a relationship between two variables is expected, but the direction of the relationship is not predicted (Field, 2005) – as is the case in this study. Thus, the Correlation Table below lists the *r*

values plus the significance values of the relationships between the fifteen independent scale items to the dependent variable of the PMT.

The Correlation Table helps to confirm the results emerging from the reliability and validity testing: each of the scale items correlates well amongst their intended component items. For example, the *perceived vulnerability* and *perceived severity* items all showed strong significant correlations with each other (e.g., PerVul1 positively related to PerSer4 with $r = .515$, significant at $p < .01$ level [2-tailed]); and so forth for each of the scale items within the other three components.

The results from the correlation matrix also indicate that certain scale items correlated well across other independent variable items:

- The SelfEff3 item positively related to all four of the *perceived severity* items:
    - PerSer1 ($r = .280$; significant at $p < .01$ level [2-tailed]);
    - PerSer2 ($r = .211$; significant at $p < .05$ level [2-tailed]);
    - PerSer3 ($r = .279$; significant at $p < .01$ level [2-tailed]);
    - PerSer4 ($r = .225$; significant at $p < .05$ level [2-tailed]).
- The PerVul2 negatively related to both SelfEff1 ($r = -.395$) and SelfEff2 ($r = -.401$), both significant at $p < .01$ level (2-tailed). But, Pervul2 positively related to both ResCost1 ($r = -.391$) and ResCost2 $r = .294$), both significant at $p < .01$ level (2-tailed).
- More importantly though, the four ResEff items all showed negative relationships with the two ResCost items (e.g., ResEff2-ResCost2, $r = -.505$; yet all others significant at least at $p < .05$ level [2-tailed]).

The results also indicate that nine of the fifteen independent variable scale items showed important relationships with the dependent variable (*PMT*):

- PerVul2 to *PMT*, $r = -.257$, significant at $p < .01$ level (2-tailed);
- ResEff1 to *PMT*, $r = .381$, significant at $p < .01$ level (2-tailed);
- ResEff2 to *PMT*, $r = .443$, significant at $p < .01$ level (2-tailed);
- ResEff3 to *PMT*, $r = .391$, significant at $p < .01$ level (2-tailed);

- ResEff4 to *PMT*, $r = .424$, significant at $p < .01$ level (2-tailed);
- SelfEff1 to *PMT*, $r = .430$, significant at $p < .01$ level (2-tailed);
- SelfEff2 to *PMT*, $r = .368$, significant at $p < .01$ level (2-tailed);
- ResCost1 to *PMT*, $r = -.265$, significant at $p < .01$ level (2-tailed);
- ResCost2 to *PMT*, $r = -.305$ – both significant at $p < .01$ level (2-tailed).

Correlation Table

		PerVul1	PerVul2	PerSer1	PerSer2	PerSer3	PerSer4	ResEff1	ResEff2	ResEff3	ResEff4	SelfEff1	SelfEff2	SelfEff3	ResCost1	ResCost2	PMT
PerVul1	Pearson Correlation	1	.465(**)	.539(**)	.584(**)	.559(**)	.515(**)	0.036	0.093	0.039	0.038	-0.163	-0.152	0.184	0.027	-0.016	-0.047
	Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000	0.716	0.348	0.699	0.704	0.101	0.125	0.063	0.790	0.874	0.634
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
PerVul2	Pearson Correlation	.465(**)	1	.332(**)	.333(**)	.378(**)	.410(**)	-0.043	-0.038	-0.088	-0.104	-.395(**)	-.401(**)	-0.066	.391(**)	.294(**)	-.257(**)
	Sig. (2-tailed)	0.000		0.001	0.001	0.000	0.000	0.666	0.704	0.377	0.296	0.000	0.000	0.510	0.000	0.003	0.009
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
PerSer1	Pearson Correlation	.539(**)	.332(**)	1	.864(**)	.811(**)	.802(**)	0.098	0.016	0.024	0.073	-0.128	-0.170	.280(**)	0.094	0.052	-0.048
	Sig. (2-tailed)	0.000	0.001		0.000	0.000	0.000	0.325	0.870	0.807	0.461	0.196	0.086	0.004	0.347	0.601	0.633
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
PerSer2	Pearson Correlation	.584(**)	.333(**)	.864(**)	1	.790(**)	.801(**)	0.047	0.052	0.054	0.081	-0.138	-0.145	.211(*)	0.108	0.009	-0.026
	Sig. (2-tailed)	0.000	0.001	0.000		0.000	0.000	0.634	0.602	0.591	0.414	0.163	0.145	0.033	0.278	0.925	0.792
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
PerSer3	Pearson Correlation	.559(**)	.378(**)	.811(**)	.790(**)	1	.953(**)	0.103	-0.016	-0.010	0.035	-0.077	-0.122	.279(**)	0.060	-0.011	0.018
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		0.000	0.299	0.869	0.919	0.723	0.441	0.221	0.004	0.546	0.910	0.859
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
PerSer4	Pearson Correlation	.515(**)	.410(**)	.802(**)	.801(**)	.953(**)	1	0.158	0.045	0.018	0.062	-0.094	-0.156	.225(*)	0.027	-0.070	0.055
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000		0.110	0.650	0.860	0.534	0.344	0.116	0.022	0.785	0.481	0.581
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
ResEff1	Pearson Correlation	0.036	-0.043	0.098	0.047	0.103	0.158	1	.582(**)	.589(**)	.602(**)	.206(*)	.205(*)	0.159	-.197(*)	-0.167	.381(**)
	Sig. (2-tailed)	0.716	0.666	0.325	0.634	0.299	0.110		0.000	0.000	0.000	0.037	0.038	0.108	0.046	0.091	0.000
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
ResEff2	Pearson Correlation	0.093	-0.038	0.016	0.052	-0.016	0.045	.582(**)	1	.709(**)	.706(**)	0.175	0.193	-0.077	-.196(*)	-0.171	.443(**)
	Sig. (2-tailed)	0.348	0.704	0.870	0.602	0.869	0.650	0.000		0.000	0.000	0.077	0.051	0.441	0.047	0.084	0.000
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
ResEff3	Pearson Correlation	0.039	-0.088	0.024	0.054	-0.010	0.018	.589(**)	.709(**)	1	.945(**)	0.046	0.067	-0.108	-.205(*)	-0.111	.391(**)
	Sig. (2-tailed)	0.699	0.377	0.807	0.591	0.919	0.860	0.000	0.000		0.000	0.644	0.501	0.279	0.038	0.263	0.000
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
ResEff4	Pearson Correlation	0.038	-0.104	0.073	0.081	0.035	0.062	.602(**)	.706(**)	.945(**)	1	0.057	0.072	-0.047	-.257(**)	-0.140	.424(**)
	Sig. (2-tailed)	0.704	0.296	0.461	0.414	0.723	0.534	0.000	0.000	0.000		0.564	0.470	0.639	0.009	0.160	0.000
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
SelfEff1	Pearson Correlation	-0.163	-.395(**)	-0.128	-0.138	-0.077	-0.094	.206(*)	0.175	0.046	0.057	1	.898(**)	.336(**)	-.328(**)	-.487(**)	.430(**)
	Sig. (2-tailed)	0.101	0.000	0.196	0.163	0.441	0.344	0.037	0.077	0.644	0.564		0.000	0.001	0.001	0.000	0.000
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
SelfEff2	Pearson Correlation	-0.152	-.401(**)	-0.170	-0.145	-0.122	-0.156	.205(*)	0.193	0.067	0.072	.898(**)	1	.311(**)	-.381(**)	-.505(**)	.368(**)
	Sig. (2-tailed)	0.125	0.000	0.086	0.145	0.221	0.116	0.038	0.051	0.501	0.470	0.000		0.001	0.000	0.000	0.000
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
SelfEff3	Pearson Correlation	0.184	-0.066	.280(**)	.211(*)	.279(**)	.225(*)	0.159	-0.077	-0.108	-0.047	.336(**)	.311(**)	1	-0.152	-.222(*)	0.091
	Sig. (2-tailed)	0.063	0.510	0.004	0.033	0.004	0.022	0.108	0.441	0.279	0.639	0.001	0.001		0.125	0.024	0.363
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
ResCost1	Pearson Correlation	0.027	.391(**)	0.094	0.108	0.060	0.027	-.197(*)	-.196(*)	-.205(*)	-.257(**)	-.328(**)	-.381(**)	-0.152	1	.750(**)	-.285(**)
	Sig. (2-tailed)	0.790	0.000	0.347	0.278	0.546	0.785	0.046	0.047	0.038	0.009	0.001	0.000	0.125		0.000	0.007
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
ResCost2	Pearson Correlation	-0.016	.294(**)	0.052	0.009	-0.011	-0.070	-0.167	-0.171	-0.111	-0.140	-.487(**)	-.505(**)	-.222(*)	.750(**)	1	-.305(**)
	Sig. (2-tailed)	0.874	0.003	0.601	0.925	0.910	0.481	0.091	0.084	0.263	0.160	0.000	0.000	0.024	0.000		0.002
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103
PMT	Pearson Correlation	-0.047	-.257(**)	-0.048	-0.026	0.018	0.055	.381(**)	.443(**)	.391(**)	.424(**)	.430(**)	.368(**)	0.091	-.285(**)	-.305(**)	1
	Sig. (2-tailed)	0.634	0.009	0.633	0.792	0.859	0.581	0.000	0.000	0.000	0.000	0.000	0.000	0.363	0.007	0.002	
	N	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103	103

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Regression

Regression is a statistical analysis process by which the independent variables in a regression model are able to make a distinction between pairs of groups (Hair, Anderson, Tatham & Black, 1998). Essentially, it takes correlation a step further and looks at predicting one variable from another (Field, 2005). Simple regression involves testing a prediction with one independent variable at a time against the dependent variable. Multiple regression is just an extension of this – using more than one independent variable at a time to test for prediction against the dependent variable.

Model Summary Table

A model summary table indicates the different models (or scenarios) of independent variable that would best predict the outcome variable (dependent variable). For this study, the statistics that will be assessed from this table are the multiple *R* and the *R* Square.

The multiple *R* is a gauge of how well the model predicts the observed data; large values of *R* represent a large correlation between the predicted and observed values of an outcome (e.g., an *R* of 1 represents a situation in which the model perfectly predicts the observed data) (Field, 2005).

The *R* Square is the amount of variation in the outcome variable that is accounted for by the model; it actually represents the percentage of the variation in the outcome that can be explained by the model (Field, 2005).

ANOVA Table

An ANOVA (analysis of variance) table describes whether each model is a significant fit of the data overall (Field, 2005). For this study, the *F*-test is assessed. A good model should have a large *F*-ratio (greater than 1 at least) and values of less than .05 in the column labelled 'Sig' (Field, 2005).

Coefficients Table

The unique contribution of variables to the regression model is viewed in a coefficients table. Whether each independent variable scale item made a significant contribution to predicting the

dependent variable can be seen in the column 'Sig' – with values less than .05 being significant (Field, 2005). Standardized beta values show the importance of each independent scale ("predictor") item – the bigger the absolute value, the more important it is.

Regression analysis results are most reliable when the independent variables are not multicollinear; this means that two or more independent variables should not have a high level of correlation with each other (Woon, Tan & Low, 2005; Hair et al., 1998). A determinative sign of multicollinearity can be taken from the VIF. VIF values in the range of 1 to 1.8 are designative of nonmulticollearity (Gammie, Jones & Robertson-Miller, 2003).

Analysis

The first series of regression tables presented will use the forced entry regression method to predict if any one of the four components is a good predictor of the dependent variable.

The second series of regression tables will use the Stepwise method of linear regression to predict any possible relationships between one or more of the fifteen scale items and the dependent variable.

Entry Method

Table 5 shows that the multiple *R* of .487 for 'Model 2' (i.e., the *response efficacy* variable) provides the largest predictive value of any of the four components to the PMT dependent variable.

Additionally, the *R* Square for Model 2 is .206 which shows that about 20% of the variation in the outcome can be explained by that particular model.

Table 5: Enter Method - Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.371	0.137	0.083	0.388
2	0.487	0.237	0.206	0.361
3	0.436	0.190	0.166	0.370
4	0.310	0.096	0.078	0.389

Model 1: (Constant), PerSer4, PerVul2, PerVul1, PerSer1, PerSer2, PerSer3
Model 2: (Constant), ResEff4, ResEff1, ResEff2, ResEff3
Model 3: (Constant), SelfEff3, SelfEff2, SelfEff1
Model 4: (Constant), ResCost2, ResCost1

Table 6 helps to support the theme that Model 2 predicts the PMT dependent variable the best out of any other combination of variables. Model 2 had the highest value of the four models in the *F*-test (7.618) and was significant at $p < .001$.

Table 6: Enter Method - ANOVA(b)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.296	6	0.383	2.547	.025(a)
	Residual	14.423	96	0.150		
	Total	16.718	102			
2	Regression	3.966	4	0.991	7.618	.000(a)
	Residual	12.753	98	0.130		
	Total	16.718	102			
3	Regression	3.180	3	1.060	7.750	.000(a)
	Residual	13.539	99	0.137		
	Total	16.718	102			
4	Regression	1.609	2	0.804	5.323	.006(a)
	Residual	15.110	100	0.151		
	Total	16.718	102			

Model 1: (Constant), PerSer4, PerVul2, PerVul1, PerSer1, PerSer2, PerSer3
Model 2: (Constant), ResEff4, ResEff1, ResEff2, ResEff3
Model 3: (Constant), SelfEff3, SelfEff2, SelfEff1
Model 4: (Constant), ResCost2, ResCost1
b. Dependent Variable: PMT

Table 7 however, indicates that none of the four models shows any levels of importance in the standardized beta coefficient values, which means they are actually not very significant in predicting the dependent variable. Moreover, it appears that these components show multicollinearity since all the items have VIF values exceeding 1.8.

Table 7: Enter Method Coefficients(a)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	1.436	0.102		14.024	0.000		
	PerVul1	0.024	0.026	0.120	0.929	0.355	0.537	1.861
	PerVul2	-0.078	0.023	-0.378	-3.384	0.001	0.721	1.387
	PerSer1	-0.035	0.041	-0.175	-0.848	0.399	0.210	4.755
	PerSer2	-0.022	0.041	-0.112	-0.534	0.594	0.206	4.858
	PerSer3	-0.083	0.070	-0.395	-1.183	0.240	0.081	12.413
	PerSer4	0.157	0.070	0.754	2.243	0.027	0.080	12.578
2	(Constant)	0.790	0.086		9.143	0.000		
	ResEff1	0.058	0.047	0.141	1.224	0.224	0.588	1.701
	ResEff2	0.080	0.040	0.260	1.981	0.050	0.450	2.221
	ResEff3	-0.061	0.076	-0.219	-0.801	0.425	0.104	9.651
	ResEff4	0.098	0.075	0.363	1.318	0.190	0.103	9.735
3	(Constant)	0.983	0.078		12.593	0.000		
	SelfEff1	0.156	0.061	0.531	2.564	0.012	0.190	5.251
	SelfEff2	-0.023	0.053	-0.090	-0.437	0.663	0.194	5.153
	SelfEff3	-0.013	0.021	-0.060	-0.628	0.532	0.886	1.128
4	(Constant)	1.620	0.134		12.126	0.000		
	ResCost1	-0.020	0.034	-0.083	-0.576	0.566	0.437	2.288
	ResCost2	-0.061	0.036	-0.243	-1.690	0.094	0.437	2.288

Model 1: (Constant), PerSer4, PerVul2, PerVul1, PerSer1, PerSer2, PerSer3
Model 2: (Constant), ResEff4, ResEff1, ResEff2, ResEff3
Model 3: (Constant), SelfEff3, SelfEff2, SelfEff1
Model 4: (Constant), ResCost2, ResCost1
a. Dependent Variable: PMT

Stepwise Method

In the correlation section, there were certain items within each component that showed small to medium relationships with dependent variable *PMT;* here we want to see if these and/or any of the other items might be used alone or in combination to predict relationships with the dependent variable.

In Table 8, the multiple *R* of .601 for 'Model 3' (i.e., the ResEff2, SelfEff1 and ResEff4 items) provides for the largest correlation between any one (and combination thereof) of the fifteen predicted values and the observed values.

Additionally, the *R* Square for 'Model 3' is .362 which shows that about 36% of the variation in the outcome that can be explained by that particular model.

Table 8: Stepwise Method - Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.443[a]	.196	.188	.365
2	.570[b]	.325	.311	.336
3	.601[c]	.362	.342	.328
4	.588[d]	.345	.332	.331

a. Predictors: (Constant), ResEff2

b. Predictors: (Constant), ResEff2, SelfEff1

c. Predictors: (Constant), ResEff2, SelfEff1, ResEff4

d. Predictors: (Constant), SelfEff1, ResEff4

Table 9 tells a different story for 'Model 3' – the particular variable combination provided the lowest of the four models in the *F*-test (18.695). Table 6 shows that 'Model 4' with an *F* of 26.379 for SelfEff1 and ResEff4 (significant at p <.001) predicts the PMT dependent variable the best out of any other combination of variables.

Table 9: Stepwise Method - ANOVA

ANOVA [e]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3.282	1	3.282	24.667	.000[a]
	Residual	13.437	101	.133		
	Total	16.718	102			
2	Regression	5.429	2	2.714	24.043	.000[b]
	Residual	11.290	100	.113		
	Total	16.718	102			
3	Regression	6.046	3	2.015	18.695	.000[c]
	Residual	10.672	99	.108		
	Total	16.718	102			
4	Regression	5.774	2	2.887	26.379	.000[d]
	Residual	10.944	100	.109		
	Total	16.718	102			

a. Predictors: (Constant), ResEff2

b. Predictors: (Constant), ResEff2, SelfEff1

c. Predictors: (Constant), ResEff2, SelfEff1, ResEff4

d. Predictors: (Constant), SelfEff1, ResEff4

e. Dependent Variable: PMT

In Table 10, the SelfEff1 item within Model 3 does appear to have more of a medium standardized beta coefficient with a value of .383 and a significance result of 0.00; plus it falls into the acceptable range for nonmulticollearity. However, the ResEff2 and ResEff4 items show low importance in their standardized beta coefficient values (.184 and .273 respectively) and ResEff2 is shown to not be significant in predicting the outcome with a result of .115. Moreover, both items are multicollinear since their VIF values exceed 1.8. As such, Model 3 is not the best of these four models for reliably predicting the dependent variable.

The scale items within Models 1, 2 and 4 show scale items with small to medium importance values; they all appear to be significant in predicting the dependent variable and they all have acceptable VIF values. In fact, Model 4 (with the SelfEff1 and ResEff4 items) appears to show the best coefficient data for predicting the dependent: standardized beta coefficient values (.407 and .401 respectively) and low VIF values (1.003).

Table 10: Stepwise Method Coefficients

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	.879	.075		11.789	.000		
	ResEff2	.136	.027	.443	4.967	.000	1.000	1.000
2	(Constant)	.700	.080		8.748	.000		
	ResEff2	.117	.026	.379	4.544	.000	.969	1.032
	SelfEff1	.107	.024	.364	4.361	.000	.969	1.032
3	(Constant)	.635	.083		7.674	.000		
	ResEff2	.057	.036	.184	1.589	.115	.483	2.069
	SelfEff1	.112	.024	.383	4.670	.000	.961	1.041
	ResEff4	.074	.031	.273	2.393	.019	.497	2.012
4	(Constant)	.662	.082		8.102	.000		
	SelfEff1	.119	.024	.407	5.028	.000	.997	1.003
	ResEff4	.109	.022	.401	4.945	.000	.997	1.003

a. Dependent Variable: PMT

Assessing the Coping Stages

Regrettably, because the sample size of collected data was insufficient, the analyses on three-tier subset of coping stages are not able to be evaluated (i.e., correlation and regression analyses output values were disproportionately skewed and inaccurate in most instances).

Discussion and Findings

This section provides a discussion of the results emerging from the statistical data testing and states whether main hypotheses were supported.

Hypothesis One – Is There an Underlying Group of Users?

To answer this test question, this part of the section will look at the findings of the Independent Samples T-Tests.

To begin with, it is important to reiterate the fact that the testing for Hypothesis One was completed entirely separately from the testing for Hypothesis Two. All of the twenty scale items were included in the assessment and testing phases and none were ruled out for this instance.

The Independent Samples T-Tests showed that eight of the twenty independent variable scale items did not support the supposition that there would be two groups in the collected data. Three of these eight scale items were from the *perceived rewards* variable. These three particular items are probably not capturing the construct of perceived rewards appropriately anyway and this is discussed in greater detail further on. Four of the remaining scale items belonged to the *response efficacy* variable and the fifth to the *self efficacy* variable. Although the test results do not support a clear pattern of different respondents within these five scale items, it could imply that the overall means values for each item may be more representative of the item model than the standard deviation initially suggested. This is also discussed in more detail further on.

Twelve of the twenty independent variable items clearly contained considerable differences in the means per item as well as showing significance in the T-Tests. These results indicate that the means of the two groups in those samples are statistically different from each other.

This finding is important because it confirms that there is indeed a sub-group of wireless router users in New Zealand. This information is crucial for security advocacy or security policy-making organizations – security strategies should be developed and focused around those people who are ***not*** concerned about wireless security.

Hypothesis Two –Are There Factors Effecting Behavioral Intention?

To answer this test question, this part of the section will first look at the reliability and validity findings and then focus on the correlation & regression results.

Reliability and Validity Results

It was shown that the scale items within the *perceived vulnerability* and *perceived severity* variables were all shown to be measuring the same component. Merging of the variables was acceptable because although the scale items did not capture the intended dimension of the threat, they were still capturing the fact that respondents recognized an existence of threat.

The *perceived rewards* variable and the *response costs* variables were intended to assess aspects that weaken protection motivation intentions. The removal of the *perceived rewards* items and two of the *response costs* items was implicit as they were probably not measuring their intended variables. The literature suggests that researchers have pragmatically focused on factors that support protection motivation intentions (Pechman et al, 2003). The scale item questions used in the survey instrument were based upon existing PMT research; this could suggest that future PMT research needs to develop the testing of the factors that weaken intentions.

Correlation & Regression Results

Independent Variable to Independent Variable

It was fully expected to see that scale items measuring the same variable correlated well between themselves (e.g., the *perceived vulnerability* items positively related to the *perceived severity* items; and the *response efficacy* items related positively to the *self efficacy* items).

Although it was expected that some scale items (from different appraisal pathways) would correlate well with items outside of their intended variables, it was not necessarily known how this would occur. Some noteworthy examples:

- The SelfEff3 (*self efficacy*) positively relating to all four of the *perceived severity* items. This is an interesting finding as it indicates that as people notice an increase in the degree of risk posed by wireless hacking, the more they feel like they could autonomously enable security features.

- The *perceived vulnerability* items negatively related to the *self efficacy* items. This may indicate that as people feel more vulnerable to threats of wireless hacking, the more they feel that they would need help in setting up security features on their wireless network.
- The PerVul2 (*perceived vulnerability*) item negatively related to the *response costs*. This may indicate that as people feel more susceptible to wireless hacking, the more they feel that enabling security features would require extra efforts of time and money on their part. This correlation makes sense when put into the context of the previously described relationship (i.e., perhaps the time and money is analogous to getting help in network setup).

The *response cost* scale items in the correlation matrix showed that negative relationships existed between the two *response cost* items and the seven items within the *response efficacy* and *self efficacy* items. Although many of these relationships show only small size effects, the overall existence of the negative correlations show the coping appraisal elements of the PMT model (See Figure 8; Coping Appraisal: as *response efficacy* and *self efficacy* increase, *response cost* decreases).

The *perceived rewards* variable was removed because of low alpha scores, so the similar threat appraisal elements were not tested.

Independent Variables to Dependent Variable

First, it is important to take into account that some of the test results for Hypothesis One. That is, weak T-Test results for the *response efficacy* variable and the *self efficacy* variable could imply that the means values are more representative of the item model than the standard deviation initially put forward. This suggests that these two variables would probably provide more reliable test results than the other four variables during regression analysis.

Coming back to the Hypothesis Two assessments – it was shown that nine of the fifteen independent variable scale items had important relationships with recommended (adaptive / "Have Enabled") response of the dependent variable (*PMT*):

- Scale item PerVul2 (*perceived vulnerability*) negatively related to *PMT*; this was not expected as PMT-based research has shown that individuals who exhibit high levels of *perceived vulnerability* also show increased intention to adopt the recommended coping response.
- All four *response efficacy* items positively related to *PMT*; these results were expected as PMT-based research has shown that there are positive correlations between *response efficacy* and the recommended coping response.
- Two of the three *self efficacy* items positively related to *PMT*; these results were expected as PMT-based research shows there are significant positive correlations with *self efficacy* on adopting the recommended coping response.
- Both of the *response cost* items negatively related to *PMT*; these results were expected as PMT-based research provides that there is a significant link between *response cost* and the recommended coping response.

Overall, the regression results help to justify the correlations described previously regarding how the *response efficacy* and *self efficacy* correlated well overall with the PMT dependent variable.

- The Entry Method has shown that the *response efficacy* variable was the closest to showing legitimate statistics in predicting the recommended coping response of the dependent variable. Although it did not pass the coefficient tests, it is notable that four scale items in the *response efficacy* variable also showed important relationships in the correlation analysis.
- The Stepwise Method has shown that three of the fifteen scale items (i.e., ResEff2, ResEff4 and SelfEff1 – from models 2 and 4) were good predictors of the recommended coping response of the dependent variable (i.e., *PMT*) This is also noteworthy because these items were also shown in the correlation analysis to be three of the nine independent variable scale items which showed important relationships with the dependent variable (i.e., PerVul2, ResEff1, ResEff2, ResEff3, ResEff4, SelfEff1, SelfEff2, ResCost1, ResCost2).

The PMT Assessment – Summation of the Six Postulations in Hypothesis Two

H1: ***Perceived vulnerability*** *is significant in determining if an individual adopts the recommended behavior of enabling security measures on a home wireless network.*

The findings did not support this hypothesis that *perceived vulnerability* would be a significant predictor of behavior. Indeed, one of the scale items was actually negatively correlated to the dependent variable, and there were no indications of prediction in the regression models. Research has ascribed the lack of a positive relationship to considerable differences in which a person perceives dissimilar threats (Plotnikoff & Higginbotham, 2002). This could be the case here as well. That is, media reports of security breaches are common but often times those reports do not specifically highlight if the breach arose from the use of undefended wireless networks (Woon, Tan & Low, 2005).

H2: ***Perceived severity*** *is significant in determining if an individual adopts the recommended behavior of enabling security measures on a home wireless network.*

Research suggests that it is often very difficult to obtain variability in the data for perceived severity (Harrison, Mullen & Green, 1992; Janz & Becker, 1984). Accordingly, the scale items showed no significant correlations and there were no indications of prediction in the regression models for this study either. Surprisingly enough, although these findings did not support the hypothesis that *perceived severity* would be a significant predictor of behavior, this is actually consistent with findings coming out of the health literature regarding protection motivation theory (Maddux and Rogers 1983; Milne, Sheeran & Orbell, 2000) for *perceived severity*.

H3: ***Perceived rewards*** *are significant in determining if an individual adopts the recommended behavior of enabling security measures on a home wireless network.*

It was revealed in reliability and validity testing that the scale item questions in the respondent survey instrument were most likely improperly constructed. This was evaluated from data gathered for the questions which suggested that the scale items were probably measuring

different components (that may in fact not have even been part of the PMT model). Abraham et al (1994) also had difficulties in attempting to operationalize *perceived rewards*. It has been this difficulty factor in operationalizing *perceived rewards* which may be the reason why it appears to have been neglected in most PMT research (Milne, Sheeran & Orbell, 2000). Therefore, the variable data was left out entirely during the relationship testing phase of this study and the hypothesis was not assessed.

H4: ***Response efficacy*** *is significant in determining if an individual adopts the recommended behavior of enabling security measures on a home wireless network.*

The findings in this study support this hypothesis that *response efficacy* is a significant predictor of behavior. This conclusion keeps in line with several previous health research studies regarding protection motivation theory (Maddux and Stanley 1986; Wurtele 1988).

For this research study, this could mean that in order to get users to secure wireless networks, they must be convinced that enabling security features will deter hacker attacks. The message should involve easy-to-understand and rational explanations of why people should make the effort to adopt security measures **and** should probably come from recognizable, trusted sources (e.g., New Zealand government agencies – SSC; hardware retailers, ISPs or hardware manufacturers).

H5: ***Self efficacy*** *is significant in determining if an individual adopts the recommended behavior of enabling security measures on a home wireless network.*

The findings in this study support this hypothesis that *self efficacy* is a significant predictor of behavior. This conclusion can also be supported by the results of several previous health research studies regarding protection motivation theory (Fruin, Pratt & Owen, 1991; Maddux and Rogers 1983; Maddux and Stanley 1986).

For this research study this could mean that in order to get users to secure networks they may need to feel that they could actually enable security features by themselves and not need some

form of human assistance to help them do it. This could be accomplished through education and training programs, however, since these are home users of wireless routers and networks, other potential solutions may involve:

- Retailers delivering customized installation materials at the point of sale of the technical hardware; or,
- Hardware manufacturers, ISPs and retailers referring users to websites which offer simple, customizable, step-by-step installation procedures.

(Woon, Tan & Low, 2005)

H6: ***Response cost*** *is significant in determining if an individual adopts the recommended behavior of enabling security measures on a home wireless network*

Research states that *response cost* should be a significant predictor of behavior (Neuwirth, Dunwoody & Griffin, 2000; Helmes, 2002). The findings emerging from this study are too inconclusive to support this hypothesis though. There were several indicators found within the correlation matrix to support the statement, but there was not strong evidence in the prediction (regression) tests.

This summation shows that two out of the six proposed (Hypothesis Two) postulations were positively supported. Just as in previous health research studies regarding protection motivation theory, the coping-appraisal component of the model was found to have greater predictive validity than was the threat-appraisal component (Cox, Koster & Russell, 2004; Wurtele 1988; Wurtele and Maddux 1987; Milne, Sheeran & Orbell, 2000).

Limitations, Implications and Future Research

Sample Size

The sample size of 103 respondents is in all probability not a reliable sample of the actual total number of home users of wireless routers in New Zealand.

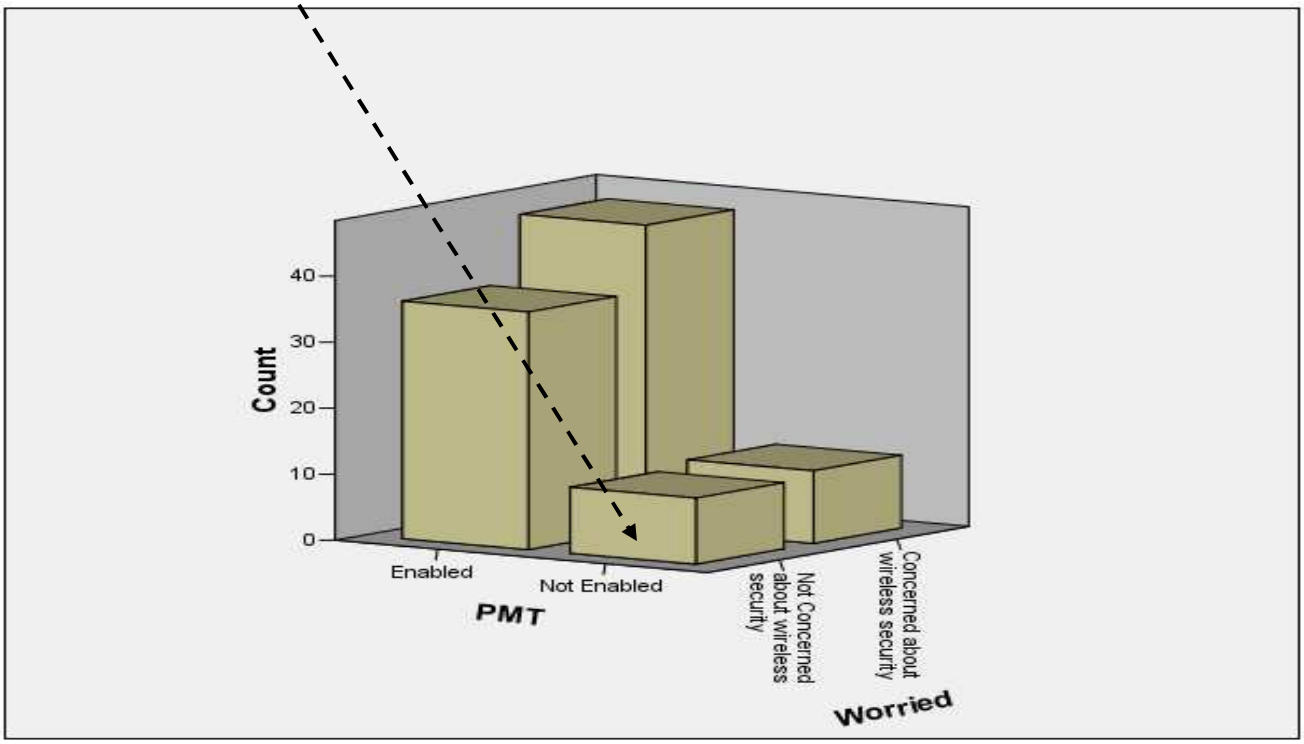
The values in the correlation matrix (and many of the values used in the regression analysis) are based upon the mean of the scale items and the mean scores for many of these items are not good fits for the population because the sample size of respondents is too low. As such, a word of warning must be provided that the correlation and regression analyses data and subsequent explanations described below may not be entirely accurate or reliable. These analyses and explanations would need to be validated by enlarging the sample size in order to deliver more accurate and reliable results.

To accomplish this, efforts would need to be focused on making certain more representative and appropriate numbers of samples are obtained for the study. And if the TTM elements are to be assessed, additional attention should be placed in ensuring that the composition of the samples in each subgroup of the coping stage (i.e., non-intenders, intenders, actors) is uniformly distributed.

Breakdown of the Two Underlying Groups

The first main research question in this report is largely successful in identifying that besides those that enable or do not enable wireless security on their home networks, there is a sub-group of distinct users in New Zealand that are worried about security and those that are not.

A process was performed on the current sample set to recode all of the scale items of the independent variables and that was compared against the dependent variable. The chart below helps to illustrate that further research could examine these sub-groups and more thoroughly assess the characteristics that differentiate those persons who are both unconcerned about security and who have not enabled security.



Conclusion

This report replicated and expanded upon research found in Woon, Tan and Low (2005) in order to ascertain characteristics of home wireless network users in New Zealand.

The first research area focused on groups of users – that is, aside from the people who activate and those who do not, are there also people who are worried about wireless security and those who are not? The second objective of this report was to replicate the overall theme of the research found within Woon, Tan and Low (2005) – to determine the factors that influence behavioral intention.

In regards to the first main research question, this report analyzed and assessed patterns of responses to independent variable scale items in order to determine whether there is indeed an underlying group of people who are worried about security. In regard to the second main research question, this report focused exclusively on measuring the concept of behavioral intention. Six testable ideas (*independent* variables) were developed to evaluate and determine the intentions of wireless network users (the *dependent* variable). The data collected from the thirty-three item online questionnaire was then statistically tested for the two main hypotheses.

The statistical testing provided proof to support the first main research hypothesis: besides the enablers, there is indeed a sub-group of "worried" wireless router users in New Zealand. This information is crucial for security advocacy or security policy-making organizations – security strategies should be developed and focused upon those people who are ***not*** concerned about wireless security.

The statistical testing for the second main research hypothesis revealed both expected and unexpected results. First, from the preliminary correlation testing, three unexpected findings emerged:

- The more people notice an increase in the degree of risk posed by wireless hacking, the more they feel like they could autonomously enable security features.

- The more people feel vulnerable to threats of wireless hacking, the more they feel that they would need help in setting up security features on their wireless network.
- The more people feel susceptible to wireless hacking, the more they feel that enabling security features would require extra efforts of time and money on their part.

From the Hypothesis Two postulation summations:

- The independent variable assessing the *perceived rewards* hypothesis had to be completely removed due to the fact that the scale items utilized to measure it did not function as intended, even though they were based upon existing PMT research. This leads to the assumption that future PMT research needs to develop the testing of the theoretical factors that weaken intentions.
- The independent variable assessing the *perceived severity* hypothesis could not be supported by the data, however, this result is actually consistent with other PMT-based research which has not found this variable to be a significant predictor of behavior intention.
- The independent variable assessing the *response efficacy* hypothesis was supported. This may imply that in order to get users to secure wireless networks, they must be convinced that enabling security features will deter hacker attacks. The message should involve easy-to-understand and rational explanations of why people should make the effort to adopt security measures **and** should probably come from recognizable, trusted sources (e.g., New Zealand government agencies – SSC; hardware retailers, ISPs or hardware manufacturers).
- The independent variable assessing the *self efficacy* hypothesis was supported. This may imply that in order to get users to secure networks they may need to feel that they could actually enable security features by themselves without some form of human assistance to help them. This could be accomplished through education and training programs, however since these are home users of wireless routers and networks, other potential solutions may involve:

- Retailers delivering customized installation materials at the point of sale of the technical hardware; or,
- Hardware manufacturers, ISPs and retailers referring users to websites which offer simple, customizable, step-by-step installation procedures.

Although the results and implications described above seem plausible, it must be reiterated that the sample size of 103 respondents is in all probability not a reliable sample of the actual total number of home users of wireless routers in New Zealand. These analyses and explanations would need to be validated by enlarging the sample size in order to deliver more accurate and reliable results which could then be used by public officials, academics or area businesses to develop policies, procedures or other educational mechanisms to address and reduce the risks posed to the users of unprotected wireless devices.

Bibliography

Abraham, S.C.S., Sheeran, P., Abrams, D. & Spears, R. (1994). Exploring teenagers' adaptive and maladaptive thinking in relation to the threat of HIV infection. *Psychology and Health*, *9*(4), 253-272.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology, 32*(4), 665-683.

Arbaugh, W.A., Shankar, N., Wang, J. & Zhang, K. (2002). Your 802.11 Network Has No Clothes. *IEEE Wireless Communications Magazine, 9*(6), December 2002, 44-51.

Bandura, A. (1977). Self Efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, *84*(2), 191-215.

Bandura, A., Adams, N., Hardy, A. & Howells, G. (1980). Tests of the Generality of Self Efficacy Theory. *Cognitive Therapy and Research*, *4*(1), 39-66.

Bartlett, J.E., Kotrlik, J.W. & Higgins, C.C. (2001). Organizational Research: Determining Appropriate Sample Size in Survey Research. *Information Technology, Learning, and Performance Journal, 19*(1), 43-50.

Bland, V. (2004). Working anytime and anywhere. *New Zealand Herald website,* released January 21, 2004. Retrieved June 6, 2008, from: http://www.nzherald.co.nz/section/11/print.cfm?c_id=11&objectid=3544662&pnum=0

Block, L.G. & Keller, P.A. (1998). Beyond protection motivation: An integrative theory of health appeals. *Journal of Applied Social Psychology, 28*(17), 1584–1608.

Bryce, S.J. (2004). *Factors Influencing the Adoption of Wireless Networks in New Zealand Businesses.* Unpublished honours dissertation, University of Otago, Dunedin, New Zealand.

Cameron, J. & Pierce, W. (2002). *Rewards and intrinsic motivation*. Westport, CT: Bergin & Garvey.

Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). New York: John Wiley & Sons.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2nd ed.). New York: Academic Press.

Cohen, J. (1992). A Power Primer. *Psychological Bulletin*, *112*(1), 155-159.

Comrey, A.L. (1973). *A First Course in Factor Analysis*. New York: Academic Press.

Condiotte, M.M. & Lichtenstein, E. (1981). Self Efficacy and Relapse in Smoking Cessation Programs. *Journal of Consulting and Clinical Psychology*, *49*(5), 648–658.

Construct Validity. (2008). *Construct Validity*. The Web Center for Social Research Methods: The Research Methods Knowledge Base. Retrieved June 15, 2008, from: http://www.socialresearchmethods.net/kb/convdisc.php

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

Cox, D.N., Koster, A. & Russell, C.G. (2004). Predicting Intentions to Consume Functional Foods and Supplements to Offset Memory Loss Using an Adaptation of Protection Motivation Theory. *Appetite*, *43*(1), 55-64.

Cronbach L.J. (1951). Coefficient Alpha and the Internal Structure of Tests. *Psychometrika, 16*(3), 297- 334.

DiClemente, C.C., Prochaska, J.O., Fairhurst, S.K., Velicer, W.F., Velasquez, M.M. & Rossi, J.S. (1991). The process of smoking cessation: An analysis of precontemplation, contemplation, and preparation stages of change. *Journal of Consulting and Clinical Psychology, 59*(2), 295-304.

Field, A. (2005). *Discovering Statistics Using SPSS*. London: Sage Publications.

Floyd, D.L., Prentice-Dunn, S. & Rogers, R.W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Psychology, 30*(2), 407-429.

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

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

Griffin, P. (2005). When technology lets you work from home. *New Zealand Herald website*, released March 21, 2005. Retrieved June 6, 2008, from: http://www.nzherald.co.nz/feature/print.cfm?c_id=1500889&objectid=10116279&pnum=0

Grimely, D.M., Williams, C.D., Miree, L.L. & Baichoo, S. (2000). Stages of readiness for changing multiple risk behaviors among incarcerated male adolescents. *American Journal of Health Behavior, 24*(5), 361-369.

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

Harrison, J. A., Mullen, P. D. & Green, L. W. (1992). A meta-analysis of studies of the health belief model with adults. *Health Education Research, 7*(1), 107-116.

Helmes, A.W. (2002). Application of the Protection Motivation Theory to Genetic Testing for Breast Cancer Risk. *Preventive Medicine*, *35*(5), 453-462.

Ho, R. (1998). The Intention to Give Up Smoking: Disease Versus Social Dimensions. *Journal of Social Psychology, 138*(3), 368-380.

Horwath, C.C. (1999). Applying the transtheoretical model to eating behavior change: Challenges and opportunities. *Nutrition Research Reviews*, *12*(2), 281–317.

Hutcheson, G. & Sofroniou, N. (1999). *The Multivariate Social Scientist*. London: Sage Publication.

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

Janz, N. & Becker, M. H. (1984). The health belief model: A decade later. *Health Education Quarterly*, *11*(1), 1-47.

Maddux, J.E. & Rogers, R.W. (1983). Protection Motivation Theory and Self Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology, 19*(5), 469-479.

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

Martin, I.H., Bender, H. & Raish, C. (2007). What Motivates Individuals to Protect Themselves from Risks: The Case of Wildland Fires. *Risk Analysis, 27*(4), 887-900.

McDowell, M., Householder, A. & Lytle, M. (2005). *National Cyber Alert System – Cyber Security Tip ST05-003: Securing Wireless Networks*. United States Computer Emergency Readiness Team. Retrieved June 10, 2007, from: http://www.uscert.gov/cas/tips/ST05-003.html.

McMillan, R. (2008). Survey: 12% of consumers 'borrow' free Wi-Fi. *IDG News Service*, released April 16, 2008. Retrieved June 6, 2008, from: http://www.networkworld.com/news/2008/041608-survey-12-percent-of-consumers.html

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

Mimoso, M. S. (2003). *Gartner: War Drive Illustrates Wireless Problem*. SearchSecurity.com, released June 4, 2003. Retrieved June 6, 2008 from: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci904547,00.html).

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

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

OECD. (2003). *Development of Wireless Local Area Networks in OECD Countries*. (Report: DSTI/ICCP/TISP(2002)10/FINAL). Organisation for Economic Co-operation and Development (OECD) website. Retrieved June 5, 2008, from: http://www.oecd.org/dataoecd/44/42/2506976.pdf

Pahnila, S., Siponen, M. & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. In the Proceedings of the *40th Hawaii International Conference on System Sciences* (HICSS '07), *January 3-6, 2007* (pp. 1-10). Waikoloa, HI. Retrieved February 28, 2008, from: http://csdl2.computer.org/comp/proceedings/hicss/2007/2755/00/27550156b.pdf

Pearson, K. (1896). Mathematical Contributions to the Theory of Evolution: III. Regression, Heredity, and Panmixia. *Philosophical Transactions of the Royal Society of London,* Ser. A, 187, 253-318.

Pechmann, C., Zhao, G., Goldberg, M.E. & Reibling, E.T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing, 67*(2), 1–18.

Plotnikoff, R.C. & Higginbotham, N. (2002). 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), 87-98.

Poulsen, K. (2001). *War Driving by the Bay*. SecurityFocus website, released April 12, 2001. Retrieved June 6, 2008, from: http://www.securityfocus.com/news/192

Prochaska, J.O., Norcross, J.C. & DiClemente, C.C. (1994). *Changing for Good*. New York: William Morrow.

Richardson, R. (2007). *2007 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute. Retrieved June 6, 2008, from: http://www.gocsi.com/forms/csi_survey.jhtml

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

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

Rogers, R.W. & Prentice-Dunn, S. (1997). Protection motivation theory. In D. Gochman (Ed.). *Handbook of health behavior research I: Personal and Social Determinants*. New York: Plenum Press.

Royster, G. (2005). Wireless Security Hodgepodge. *Infosec Writers website*. Retrieved June 6, 2008, from: http://www.infosecwriters.com/text_resources/pdf/Wireless_Security_Hodgepodge.pdf

Schwarzer, R. (2008). Modeling health behavior change: How to predict and modify the adoption and maintenance of health behaviors. *Applied Psychology: An International Review, 57*(1), 1-29.

SIGS. (2002). *New Zealand Government Security: Security in the Government Sector* (June 26, 2002). Retrieved from March 15, 2008, from: http://www.security.govt.nz/sigs/sigs.pdf.

Srikanth, S. (2004). Tutorial 4(T4): IEEE 802.11 Wireless Local Area Networks. In the Proceedings of the *1st International Symposium on Wireless Communication Systems. September 20-22, 2004* (pp.1-4). MAURITIUS. Retrieved June 6, 2008, from: http://www.ieeevtc.org/iswcs04/tut4.html

Stanton, B., Guo, J., Cottrell, L., Galbraith, J., Li, X., Gibson, C., Pack, R., Cole, M., Marshall, S. & Harris, C. (2005). The complex business of adapting effective interventions to new populations: An urban to rural transfer. *Journal of Adolescent Health, 37*(2), 163.e17–163.e26.

Stoneburner, G., Goguen, A. & Feringa, A. (2002). *Special Publication 800-30: Risk Management Guides for Information Technology Systems*. National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce (July 2002). Retrieved March 14, 2008, from: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Sustainability NZ. (2008). *Teleworking*. New Zealand Ministry of the Environment website: Sustainability NZ. Retrieved June 5, 2008, from: http://www.sustainability.govt.nz/content/working-away-office-teleworking

T-Test. (2008). *The T Test*. The Web Center for Social Research Methods: The Research Methods Knowledge Base. Retrieved June 21, 2008, from: http://www.socialresearchmethods.net/kb/stat_t.php

Tanner, J.F. Jr., Day, E. & Crask, M.R. (1989). Protection Motivation Theory: An Extension of Fear Appeals Theory in Communication. *Journal of Business Research, 19*(4), 267-276.

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

Velicer, W.F. & Prochaska, J.O. (2008). Stage and Non-stage Theories of Behavior and Behavior Change: A Comment on Schwarzer. *Applied Psychology: An International Review, 58*(1), 75–83.

Weinstein, N.D., Rothman, A.J. & Sutton, S.T. (1998). Stage theories of health behavior: Conceptual and methodological issues. *Health Psychology, 17*(3), 290–299.

Welch, D. (2007). *Two-thirds of New Zealand Homes Online*. Media Release April 27, 2007, Statistics New Zealand website. Retrieved on June 5, 2008, from: http://www.stats.govt.nz/products-and-services/hot-off-the-press/household-use-of-information-and-communication-technologies-survey-2006/household-use-ict-2006-hotp.htm

Wireless Security. (2006). *Using Wireless Technology Securely*. United States Computer Emergency Readiness Team (US-CERT). Retrieved March 15, 2008, from: http://www.us-cert.gov/reading_room/Wireless-Security.pdf.

Woon, I.M.Y., Tan, G.W. & Low, R.T. (2005). A Protection Motivation Theory Approach to Home Wireless Security. In the Proceedings of the *Twenty-Sixth International Conference on Information Systems, December 11-14, 2005* (pp. 367-380). Las Vegas, NV. Retrieved May 15, 2007, from: http://aisel.aisnet.org/password.asp?Vpath=ICIS/2005&PDFpath=SA03.pdf.

Wurtele, S.K. (1988). Increasing Women's Calcium Intake: The Role of Health Beliefs, Intentions, and Health Value. *Journal of Applied Social Psychology, 18*(8), 627-639.

Wurtele, S.K. & Maddux, J.E. (1987). Relative Contributions of Protection Motivation Theory Components in Predicting Exercise Intentions and Behavior. *Health Psychology, 6*(5), 453-466.

Appendix

The Survey Instrument

Introduction and Informed Consent:

Victoria University of Wellington, New Zealand
Te Whare Wānanga o te Ūpoko o te Ika a Māui Aotearoa
School of Information Management

A survey of wireless network security

Informed Consent Information:

This is a research project that will assess the factors that differentiate between users who secure their home wireless networks and those who do not. The study is being conducted by Dennis DiGiusto as part of the project requirements for the Masters of Information Management degree being undertaken at Victoria University of Wellington and has been approved by the University Human Ethics (HEC) Committee.

If you agree to participate in this study, you will fill out a web-based survey questionnaire which will ask questions related to your general knowledge of your wireless router set-up and your opinions on wireless hacking and wireless security. The survey will take about 6-10 minutes to complete. In terms of confidentiality, the research will be conducted on a strictly anonymous basis. (The survey does not ask for nor does it collect your personal identity; as such, all responses to the survey will be collected and recorded such that you remain anonymous). Any respondent can email the Researcher listed below to obtain a copy of the final report.

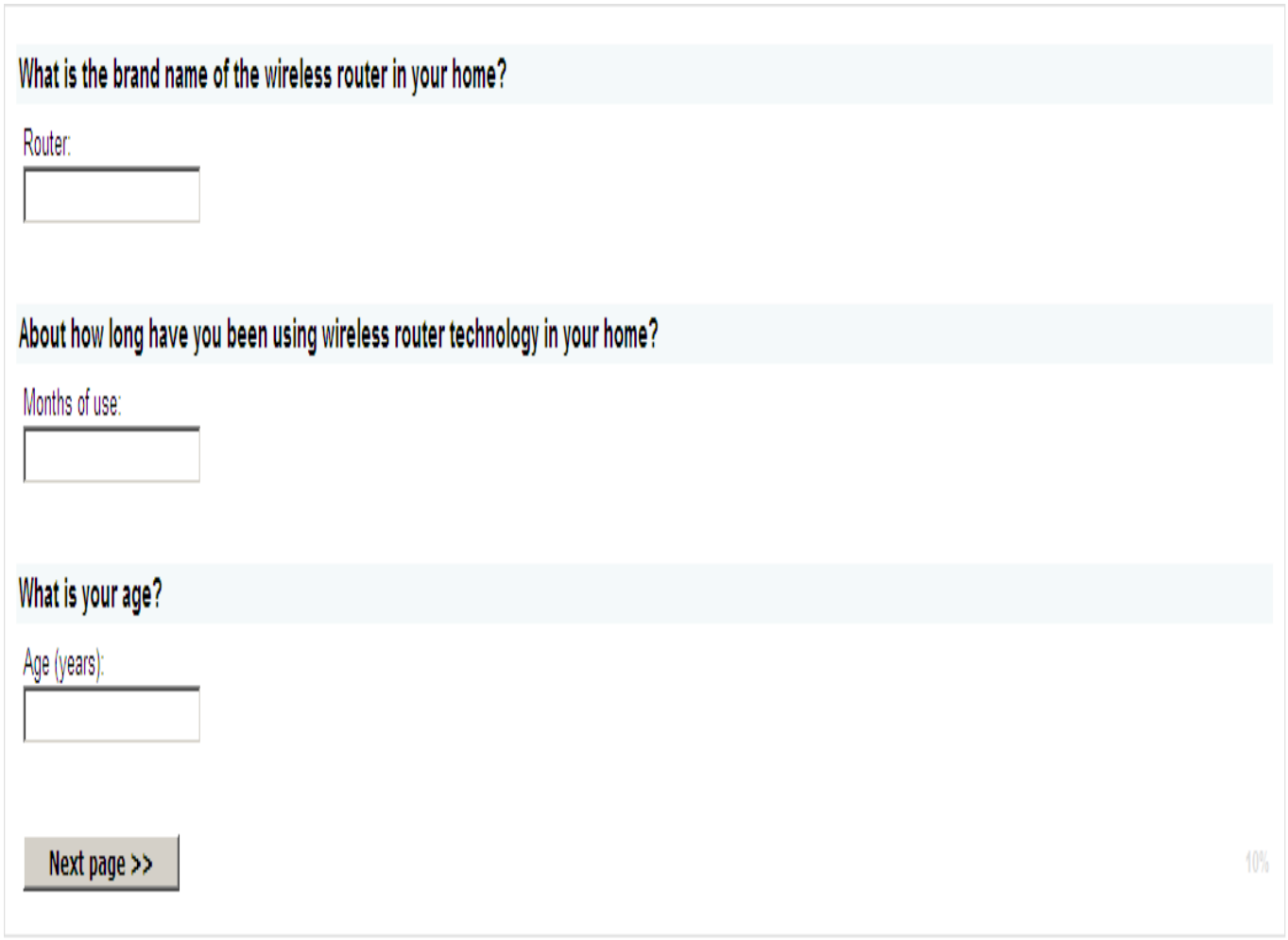
Researcher: Dennis DiGiusto, MIM Candidate, School of Information Management, Victoria University of Wellington, digiusdenn@student.vuw.ac.nz
Supervisor: Dr. David Mason, Victoria University of Wellington, 04-463-7435, david.mason@vuw.ac.nz

By clicking the 'Next Page' button you are deemed to have given your consent to participate.

Next page >>

0%

Page 2, Demographics:



Page 3, *Perceived Vulnerability*:

On a scale of 1 to 7, where would you place yourself in terms of being exposed to wireless hacking?

(1 = Strongly Agree, 7 = Strongly Disagree)

I could be subjected to a malicious wireless hacking attempt*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

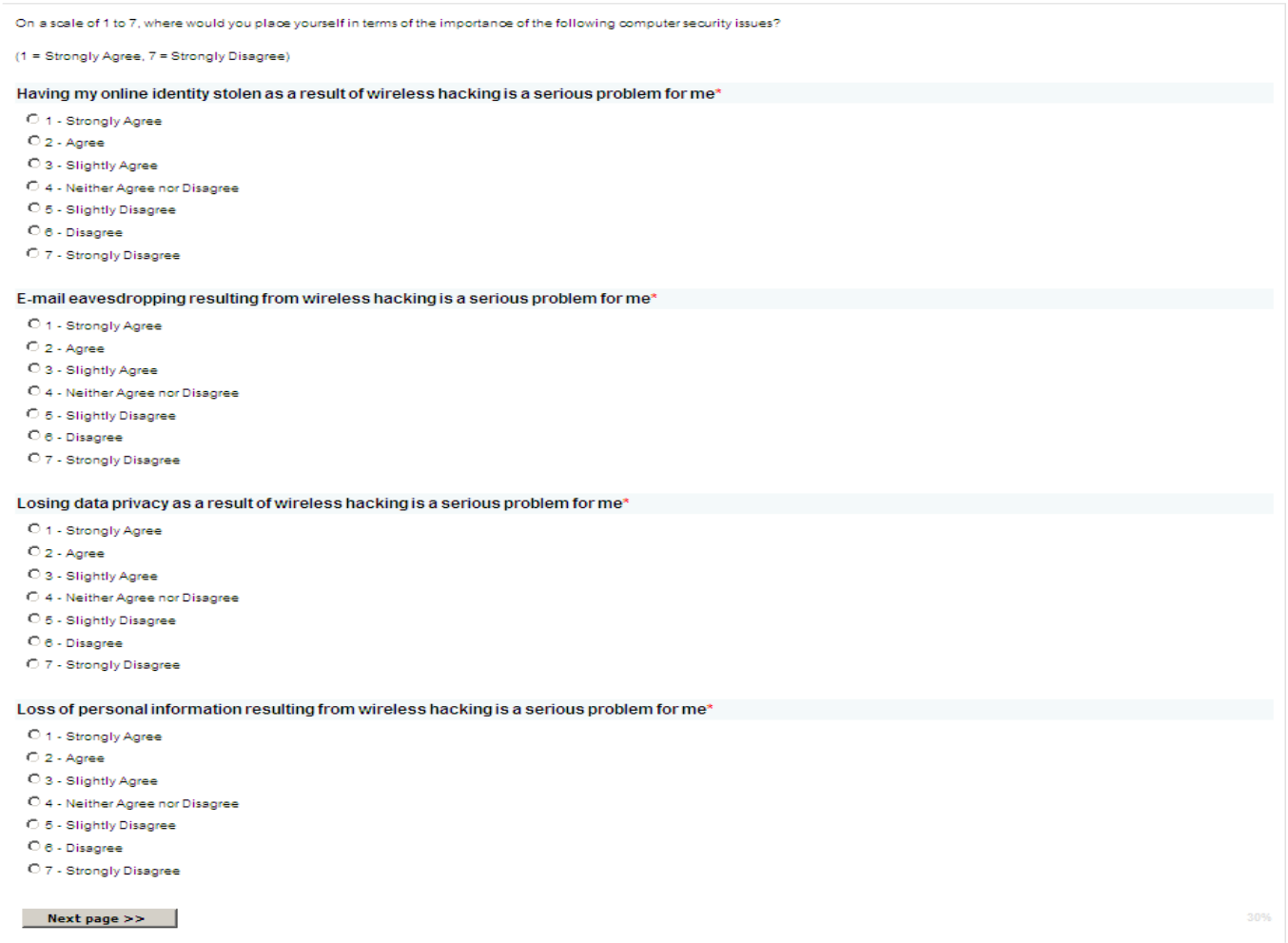
I feel that I could be vulnerable to wireless hacking*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Next page >>

20%

Page 4, *Perceived Severity*:



On a scale of 1 to 7, where would you place yourself in terms of the importance of the following computer security issues?

(1 = Strongly Agree, 7 = Strongly Disagree)

Having my online identity stolen as a result of wireless hacking is a serious problem for me*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

E-mail eavesdropping resulting from wireless hacking is a serious problem for me*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Losing data privacy as a result of wireless hacking is a serious problem for me*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Loss of personal information resulting from wireless hacking is a serious problem for me*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Next page >>

30%

Page 5, *Response Efficacy*:

On a scale of 1 to 7, where would you place yourself in terms of the importance of the following computer security issues?

(1 = Strongly Agree, 7 = Strongly Disagree)

Enabling security measures on my home wireless network will prevent hackers from stealing network bandwidth*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Enabling the security measures on a home wireless network is an effective way of deterring hacker attacks*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Enabling security measures on my home wireless network will prevent hackers from gaining important personal or financial information*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Enabling security measures on my home wireless network will prevent hackers from stealing my identity*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Next page >>

40%

Page 6, *Self Efficacy*:

On a scale of 1 to 7, where would you place yourself in terms of the following computer security issues?

(1 = Strongly Agree, 7 = Strongly Disagree)

It would be easy for me to enable security features on the home wireless network by myself*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

I could enable wireless security measures even if there was no-one around instructing me as I go along*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

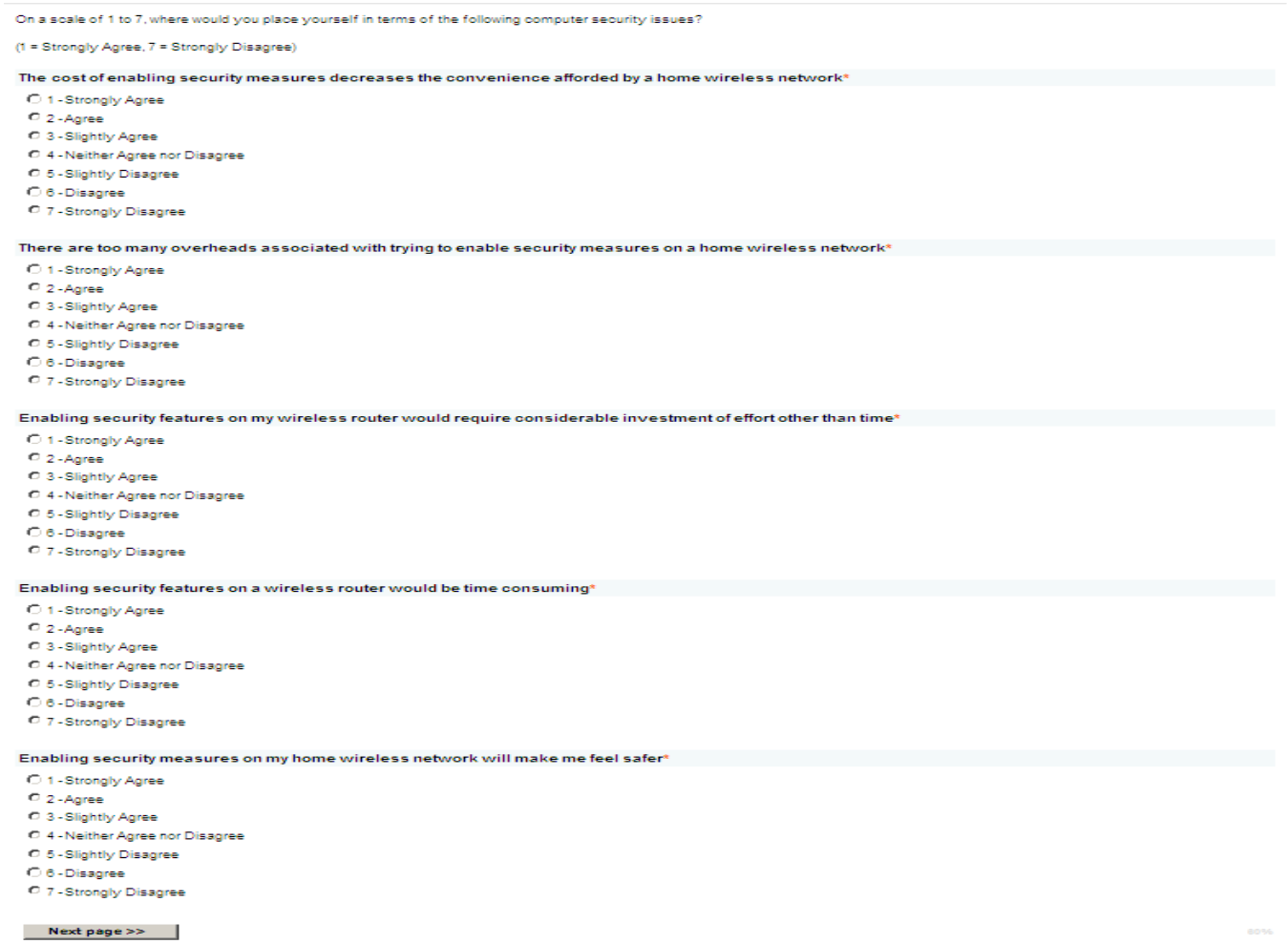
I could enable wireless security measures if I only had manuals for reference*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Next page >>

50%

Page 7, *Response Cost* items & one *Perceived Rewards* item:



On a scale of 1 to 7, where would you place yourself in terms of the following computer security issues?

(1 = Strongly Agree, 7 = Strongly Disagree)

The cost of enabling security measures decreases the convenience afforded by a home wireless network*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

There are too many overheads associated with trying to enable security measures on a home wireless network*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Enabling security features on my wireless router would require considerable investment of effort other than time*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Enabling security features on a wireless router would be time consuming*

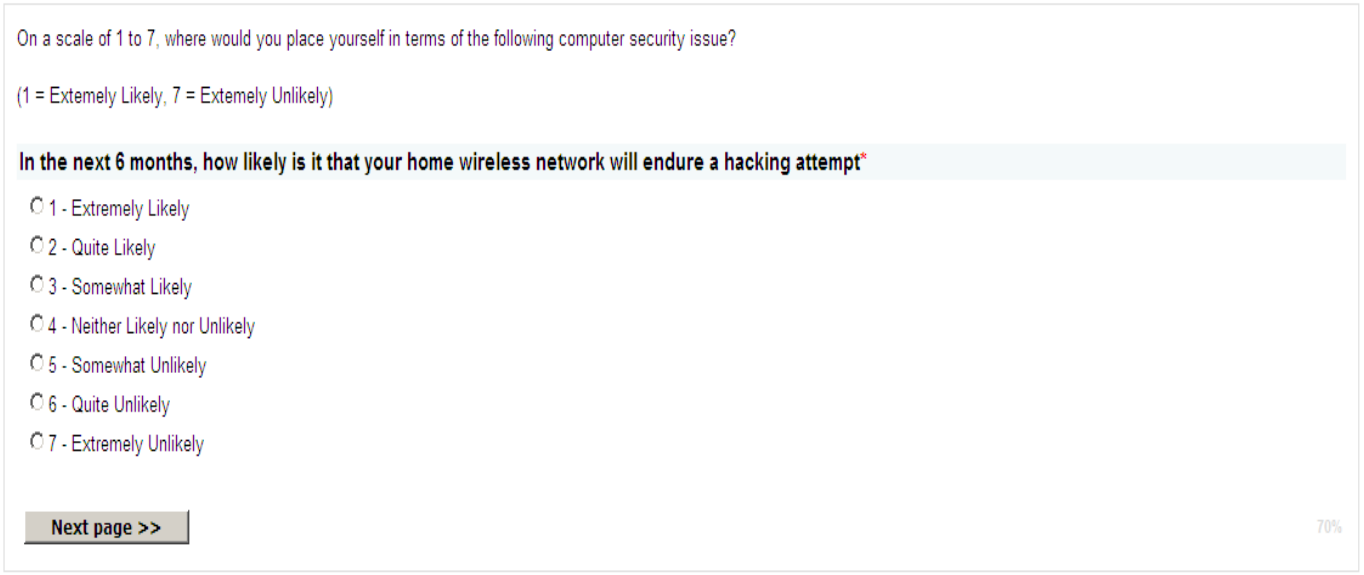
- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Enabling security measures on my home wireless network will make me feel safer*

- 1 - Strongly Agree
- 2 - Agree
- 3 - Slightly Agree
- 4 - Neither Agree nor Disagree
- 5 - Slightly Disagree
- 6 - Disagree
- 7 - Strongly Disagree

Next page >>

Page 8, second *Perceived Rewards* item:


On a scale of 1 to 7, where would you place yourself in terms of the following computer security issue?

(1 = Extemely Likely, 7 = Extemely Unlikely)

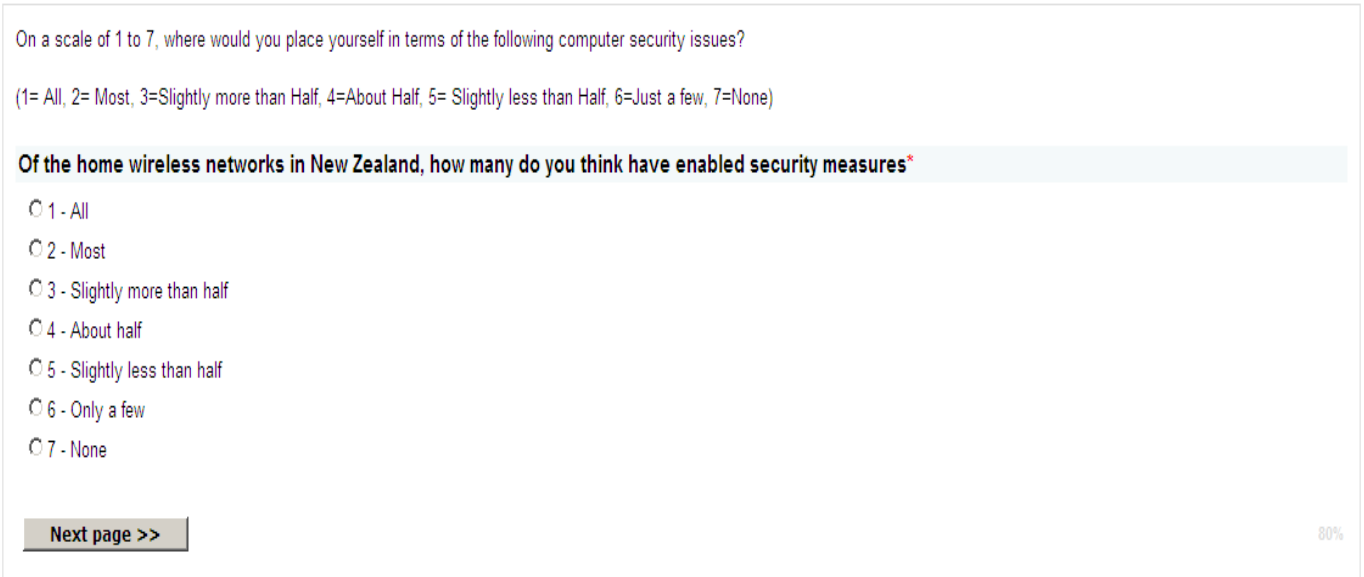
In the next 6 months, how likely is it that your home wireless network will endure a hacking attempt*

- 1 - Extremely Likely
- 2 - Quite Likely
- 3 - Somewhat Likely
- 4 - Neither Likely nor Unlikely
- 5 - Somewhat Unlikely
- 6 - Quite Unlikely
- 7 - Extremely Unlikely

Next page >>

70%

Page 9, third *Perceived Rewards* item:


On a scale of 1 to 7, where would you place yourself in terms of the following computer security issues?

(1= All, 2= Most, 3=Slightly more than Half, 4=About Half, 5= Slightly less than Half, 6=Just a few, 7=None)

Of the home wireless networks in New Zealand, how many do you think have enabled security measures*

- 1 - All
- 2 - Most
- 3 - Slightly more than half
- 4 - About half
- 5 - Slightly less than half
- 6 - Only a few
- 7 - None

Next page >>

80%

Page 10, Coping (decision) Stage items:

The following statements describe various safe computing activities; where would you place yourself in terms of completing these actions? *

	-Already done-	-Will do in next month-	-Will do in next 6-12 months-	-Will do next year-	-Will not do-
Assign user account(s) and password(s) on your home computer(s)	○	○	○	○	○
Install Anti-Virus protection software on your home computer(s)	○	○	○	○	○
Install a Firewall (software and/or hardware) on your home computer(s)	○	○	○	○	○
Install applicable updates for your internet browser(s)	○	○	○	○	○
Password-protect files that contain sensitive personal data, such as financial account information	○	○	○	○	○
Adjust the "junk mail" settings on your email application	○	○	○	○	○
Enable the security feature(s) on your wireless router	○	○	○	○	○
Adjust the "administrator" settings on your wireless router	○	○	○	○	○
Update the "name" (or SSID) of your wireless router	○	○	○	○	○
Update the encryption settings on your wireless router	○	○	○	○	○

Submit form

90%