Assessing Home Internet Users' Demand for Security: Will They Pay ISPs?

Dallas Wood and Brent Rowe

RTI International

Abstract

One strategy for improving cyber security would be for Internet service providers (ISPs) to take a more active role in curtailing criminal behavior over the Internet. However, few ISPs today are offering robust security to their customers. They largely contend that home Internet users are unwilling to pay for improvements in cyber security. Yet no prior studies have attempted to quantify home Internet customers' willingness to pay the monetary and nonmonetary costs of ISP security initiatives. Our research study took the first step in filling this gap in the literature. Specifically, we used choice-based conjoint analysis to examine the preferences of U.S. broadband Internet customers. Our findings support the notion that consumers are willing to accept price increases, ISP-required security training, and suspensions of their Internet service when malware is detected on their computer in exchange for reductions in the risk of their computer slowing down or crashing, the risk of their identity being stolen, or the risk that others will be affected by their insecurity.

1. Introduction

Cyber attacks resulting from the current insufficient state of Internet security have led to large financial losses for businesses, governments, and individuals. Home Internet users are a large factor in this problem because they typically do not maintain adequate security measures on their computers, which leaves them vulnerable to becoming part of a botnet, spreading viruses, or propagating other threats to cyber security.

Past research suggests that Internet service providers (ISPs) have the potential to improve the security of home users by identifying and quarantining customers that have malware on their machines and by providing users with security software and educating them on the importance of cyber security. However, ISPs largely contend that home Internet users are unwilling to pay for improvements in cyber security. To date, no study has attempted to assess home user demand for ISP-based security packages.

In this paper, we address three research questions related to these issues. First, we quantify U.S. broadband users' preferences using choice-based conjoint analysis. We hypothesize that broadband Internet users have clear preferences over several features of ISP security packages, favoring packages that impose fewer costs and provide greater reductions in cyber security risks. Second, we use the conjoint analysis results to explore how much broadband users are willing to pay for changes in individual ISP security package features (holding all other features constant). We hypothesize that the mean broadband Internet user is willing to pay positive sums to improve their own security and the security of others and willing to accept non-monetary costs associated with ISP security packages in exchange for modest reductions in their monthly internet bill. Lastly, we explore how much broadband users would be willing to pay for hypothetical security packages that combine multiple benefits and non-monetary costs. We hypothesize that the mean broadband user is willing to pay positive sums for ISP security packages, even when those packages only benefit others.

2. ISP-Based Security Solutions and Home User Demand for Security

Recent studies and security experts have suggested that ISPs are in a good position to cost-effectively prevent certain types of malicious cyber behavior, such as the operation of botnets on home users' computers. The most important reason that ISPs are assumed to be potential critical control points is that ISPs provide home users with access to the Internet. This allows them to observe traffic flowing into and out of their networks, placing them in a position to identify traffic spikes that could be associated with excessive malicious traffic (e.g., caused by worms or spam bots).

Once an ISP identifies signs of infection or misbehavior, they can pursue a number of security solutions. In general, these ISP-based security solutions can be grouped into two main categories:

1. **Internal solutions**: These solutions are implemented inside the ISP and involve filtering traffic so that suspicious activity is addressed with or without the user's consent (e.g., responding to traffic spikes or other signs of infection by cutting off the infected user's Internet access until their machine has been repaired).

2. **External solutions**: These solutions help Internet subscribers improve their own security, either by providing them with security advice (e.g., how to set up a firewall) or with free security products (e.g., antivirus software). Fundamentally, these solutions rely on voluntary user action to improve security (and are therefore "external" to the ISP).

However, existing information suggests that neither of these types of solutions are being pursued to their full extent. In terms of internal security solutions, most ISPs do not take an active role. According to the 2009 Worldwide Infrastructure Security report, only 28% of the ISPs surveyed said that they use automated techniques for quarantining infected or malicious subscribers (Arbor Networks, 2010). In

terms of external solutions, many ISPs (such as Comcast and AOL) provide antivirus software to their home Internet customers for free (Rowe et al., 2011). However, no data exist that enable us to determine how effective these solutions, which require voluntary action on the part of home users, have been in improving overall cyber security. One ISP interviewed for this study[1] indicated that only 50% of their customers have downloaded a security software package that is free with their subscription.

A number of policy solutions have been proposed to provide ISPs with a financial incentive to take a greater role in promoting cyber security (Lichtman & Posner, 2004; Moore, 2010; Clayton, 2010). One prevalent strategy discussed throughout the cyber security literature is to make ISPs liable for the damages caused by their subscribers when they are infected with malware (Lichtman & Posner, 2004). However, various researchers have raised some concern with imposing liability on ISPs (Anderson et al., 2008; Moore, 2010). For example, in a commissioned report for the European Network and Information Security Agency, the authors cite several stumbling blocks with this approach, such as the potentially high transaction cost of lawsuits and the difficulty of valuing the monetary losses associated with individual events (Anderson et al., 2008). Instead, they recommended that ISPs be charged a fixed penalty if they do not quarantine infected individuals in a timely manner once they have been notified of their activities.

In either case, imposing financial costs on ISPs for ignoring malware present on their subscribers' computers would certainly provide an incentive for them to pursue more "internal solutions" such as quarantining infected or malicious subscribers (which could lead to higher monthly Internet fees). However, it is likely that such costs will also lead ISPs to pursue more "external solutions" that require them to play an active role in securing their subscribers' computers. For example, Lichtman and Posner (2004) note that "ISPs have a direct contractual relationship with their subscribers and so surely a liable ISP will require each of its subscribers to adopt rudimentary precautions…[b]etter still, these contract terms can be enforced by technology, which is to say that an ISP can block any subscriber whose virus definitions are horribly out of date or whose firewall is malfunctioning" (p. 27).

Based on this discussion, it seems that ISP-based security solutions have the potential to impose at least three types of monetary and nonmonetary costs on broadband Internet users:

- increases in the cost of Internet access,
- time spent complying with ISP security requirements, and
- limits placed on their Internet access.

However, broadband Internet users would not have to incur these costs without reason. They would receive protection from malware and other threats to their security if these ISP strategies were pursued. Specific benefits would include the following:

- Improved computer performance: By removing malware that uses the scarce computing resources of a user's computer, they may perceive an increase in the performance of their machine.
- Reduced risk of identity theft: By removing malware from a user's computer and blocking spam from their e-mail accounts, ISP strategies can reduce the risk of a person's identity getting stolen.
- Reduced risk to other individuals and business from a user's insecurity: By helping to mitigate the presence of botnets, ISP-based security strategies can help reduce the risk that businesses or other individuals would incur the costs imposed by them.

To fully understand the consequences of pursuing ISP security strategies, we must understand how willing U.S. broadband users are to accept the cost of these strategies in exchange for the benefits they provide. Although the cost of implementing these ISP-based solutions has been discussed in the

---

[1] Participation by this ISP required that their name be kept confidential.

literature (Clayton, 2010), no study has attempted to quantify how willing ISP customers will be to accept these packages once implemented. Several studies have tried to estimate demand for cyber security services in general. For example, a 2004 study of consumers in the United Kingdom found that 58% would be willing to pay $3 or more per month for greater protection. In the same study, 66% of consumers said that they would switch ISPs to one that offered "clean" Internet service (StreamShield Networks, 2004). In a more recent study, Gallaher and colleagues (2006) interviewed a small sample of home Internet users and found that more than 50% spend more than $20 per year on security products or subscription services. More than half also indicated a WTP their ISP 10% more for additional security. However, none of these studies used rigorous demand-assessment techniques to quantify users' WTP for security services. All of these past studies used simple opinion surveys that did not allow users to express their demand in terms of various cost trade-offs and specific security service components. The present study aims to take the first step in filling this gap in the literature by using sophisticated methods for quantitative demand assessment, which are described in the following section.

3. Methods for Quantifying Home Broadband Users Demand for Improvements in Cyber Security

The primary purpose of this study is to assess the demand of home broadband Internet users for improvements in cyber security. In order to answer this question, we must first conceptualize how the various costs and benefits of these ISP strategies contribute to an individual broadband user's utility. Based on the discussion in the previous section, we can identify three costs to home users:

- increases in the cost of Internet access,
- time spent complying with ISP security requirements, and
- limits placed on their Internet access.

We can also identify three types of benefits users would receive in exchange for accepting these costs:

- improved computer performance,
- reduced risk of identity theft, and
- reduced risk to other individuals and business from a user's insecurity

Although other costs and benefits could be considered in relation to ISP security strategies, we believe that these are the ones that would most concern broadband users. Therefore, we can conceptualize the broadband user utility as a function that takes the form of

$$U = f(F, T, A, P, I, O)$$

where F is the additional fee ISPs charge broadband users for pursuing the security strategy, T is time users must spend complying with ISP security strategies, A is a measure of the user's ability to access the Internet (which can be impeded by some ISP security strategies), P is a measure of the performance of the user's computer (which can be reduced by the presence of malware on their machine), I is a measure of the risk of identity theft (which can be reduced by ISP security strategies), and O is a measure of the losses incurred by others because of an individual broadband user's lack of security. We hypothesize that increases in the cost of Internet access decrease personal utility ($\partial U/\partial F < 0$), increases in the time it takes to comply with ISP security requirements decrease personal utility ($\partial U/\partial T < 0$), improvements in a user's access to the Internet increase utility ($\partial U/\partial A > 0$), improvements in the performance of a user's computer increase utility ($\partial U/\partial P > 0$), increases in the risk of identity theft reduce utility ($\partial U/\partial I < 0$), and increases in losses incurred by others reduce an individual user's utility

($\partial U/\partial O < 0$).

We operationalize this conceptual model using choice-based conjoint analysis. Choice-based conjoint analysis is a stated-preference survey method in which survey respondents are asked to choose between hypothetical products or policies. Conjoint analysis has been extensively used by market researchers for the past 30 years to evaluate the market potential of new products and to create pricing strategies (Orme, 2010). In recent years, conjoint analysis has also been increasingly used to value the net benefits of government health and environmental policies (Hensher, Rose, & Greene, 2005), as well as types of security policies (Smith & Mansfield, 2006; Robinson et al., 2010). Evidence supporting the reliability of conjoint analysis for making credible estimates of purchasing decisions has also been obtained through field experiments (List, Sinha, & Taylor, 2006).

For the purposes of this study, we created conjoint choice tasks that required survey respondents to choose between ISP security packages that were differentiated by the costs they would impose on the respondent and the security benefits they would provide. In the following sections, we describe how the survey was developed, how it was administered, and the statistical methods used to evaluate the survey data collected.

3.1 Survey Development and Design

Data for this study were collected through a survey instrument, the primary component of which was a set of seven forced-choice questions that included a no-choice alternative (an opt-on) follow-up question (see Figure 1 for an example). Each question described two hypothetical security packages that an ISP might offer broadband customers. After the respondent selected which of the two hypothetical packages they most preferred, they were asked if they would actually support their own ISP pursuing the package they selected. For the purposes of this study, we consider this choice task as being composed of three alternatives: Option A (if a person selected Option A and indicated that he would support his ISP pursuing that option), Option B (if a person selected Option B and indicated that he would support his ISP pursuing that option), and a third no-choice alternative (if a person selected either Option A or B and indicated that he would not support his ISP pursuing that option).

Each hypothetical ISP security package was presented as being composed of the six costs and benefits (known as package "features" or "attributes") we used to conceptualize broadband user utility. However, in order to make the description of these attributes tractable in an experimental setting, we had to establish a set of finite descriptors known as "levels" to describe each attribute in a way the average broadband user would understand. We attempted to create levels for each of the six attributes so that they would include the set of plausible extremes. For example, the levels chosen for the attribute for limiting access to the Internet range from the ISP never having the ability to limit one of its customers' access to the ISP being able to totally disconnect a customer from the Internet if her computer appears to be infected by malware.

However, choosing the levels for the cyber security outcomes (benefits) attributes proved to be more difficult. We considered using quantitative measures of the how much various threats could be reduced (for example, saying the risk of identity theft would be reduced by 50%) but were concerned that (1) respondents would find these questions difficult to comprehend and (2) respondents would be answering questions from different baselines as to what the current risks were. Therefore, three qualitative levels were chosen for each attribute to indicate whether the package in question greatly reduced a given threat, somewhat reduced it, or did not reduce it at all. A summary of the attributes and levels used in the final survey instrument are presented in Table 1.

	Option A	Option B
ISP Strategies to Improve Security		
Adding a fee to your bill to provide security services to Internet subscribers	$4 per month	$7 per month
Requiring you and other Internet subscribers to comply with security requirements and training	0 hours per month	0 hours per month
Limiting Internet access for you or other subscribers who show signs of malicious or illegal activity	ISP can never limit your access to the Internet	ISP can never limit your access to the Internet
Cyber Security Outcomes		
Reduced risk of your computer slowing down or crashing	Greatly Reduced	Greatly Reduced
Reduced risk of your identity being stolen	Not Reduced	Not Reduced
Reduced risk to other individuals and business from your insecurity	Not Reduced	Greatly Reduced
If these were the only options available, which would you choose?	☐	☐

Suppose your ISP was going to pursue the strategies for improving security that are included in your preferred option and that these strategies resulted in the outcomes described in the table above. Would you support your ISP pursuing these strategies?

☐ Yes, I would support my ISP pursuing these strategies
☐ No, I would not support my ISP pursuing these strategies

Figure 1: Example Choice Question

Given the six attributes and three levels described above, 729 (3 x 3 x 3 x 3 x 3 x 3) possible hypothetical packages could be created. However, one of the primary benefits of conjoint analysis is that only a small fraction of these potential packages have to be evaluated by actual respondents if each attribute being considered is assumed to add linearly to a person's utility. When this assumption is made and a proper subsample of the 729 hypothetical package profiles is chosen (this subsample is referred to as the "experimental design"), then statistical analysis can be used to predict how respondents would answer the remaining hypothetical choice tasks (Orme, 2010). A "proper subsample," or statistically efficient experimental design, is one that possesses several properties (Zwerina, Huber, &Kuhfield, 1996; Kanninen, 2002), such as the following:

- *Level balance*: The levels of an attribute occur with equal frequency.
- *Orthogonality*: The occurrences of any two levels of different attributes are uncorrelated.
- *Minimal overlap*: Cases where attribute levels do not vary within a choice set should be minimized.
- *Utility imbalance*: The probabilities of choosing alternatives within a choice set should be as efficient as possible. For example, for two alternatives the probabilities should be approximately 0.75 and 0.25 (Kanninen, 2002).

Table 1: Attributes and Levels for Choice Experiment Design

Attributes	Levels
Fee	$4 per month $7 per month $12 per month
Require Internet users to follow certain security policies and be trained regularly	0.5 hours per month 1 hour per month 3 hours per month
Limit Internet access of customers whose computers show signs of being hacked	- ISP can never limit a user's access to the Internet - ISP can restrict a user's usage to certain functions or Web sites if the ISP suspects the user has been hacked - ISP can cut off a user's connection to the Internet entirely if the ISP suspects the user has been hacked
Reduced risk of a user's computer slowing down or crashing	- Not reduced - Somewhat reduced - Greatly reduced
Reduced risk of a user's identity being stolen	- Not reduced - Somewhat reduced - Greatly reduced
Reduced risk to other individuals and businesses from a user's insecurity	- Not reduced - Somewhat reduced - Greatly reduced

Unfortunately, it is often impossible to achieve both level balance and orthogonality in small designs. However, Kuhfeld, Tobias, and Garratt (1994) show that it is possible to produce relatively efficient designs that are neither balanced nor orthogonal. Such efficient designs can be produced using an iterative computer algorithm. The experimental design for our stated preference questions was created using Sawtooth Choice-Based Conjoint Software (Sawtooth, 2010).

3.2 Survey Fielding and Sample Characteristics

After the survey instrument was completed, it was programmed for Web administration by comScore, Inc, which maintains a large opt-in consumer panel that to be representative of the online population and projectable to the total U.S. population. These panelists are recruited across thousands of sites not used by other panel suppliers, and they do not have to be willing to answer surveys to be accepted to the panel. Once the survey was programmed, it was administered from November 2010 to December 2010 to members of the comScore panel that had broadband Internet access, exceeded 18 years of age, and resided inside the United States. We decided to include only broadband users in our sample because they are the users that would be most affected by ISP security packages.

To determine the proper sample size for this survey, we used the technique recommended by Orme as a starting point. This method relies on the number of total questions per respondent (t), the maximum number of attribute levels (c), the number of alternatives in the trade-offs (a), and the number of respondents (n). In this study, $c = 3$ (all attributes possess only three levels), $a = 2$ (alternatives of A or B), and $t = 7$ main questions. Specifically, Orme recommends that ($nta/c \geq 500$), for a minimum sample

size of at least n = 107 for each version of our survey. To improve the statistical power and reliability of our analyses, we sampled a significantly greater number n = 3,635.

Descriptive statistics of the sample we collected are provided in Table 2. The sample was approximately evenly split between males and females. Approximately half of the sample was under 40 years of age. The vast majority of survey respondents (~70%) were college educated. The majority of respondents (57%) had household incomes exceeding $50,000. The vast majority of the sample was white (81%). The majority of respondents pay more than $40 per month for broadband access (54%). Specifically, the mean monthly broadband bill was estimated to be $46.

Table 2: Sample Characteristics (N = 3,635)

	2010 Survey (N = 3,635)	**Pew 2010 Survey (N=1,413)**
Gender		
Male	49%	45%
Female	51%	55%
Age		
18–24 years	11%	12%
25–34 years	31%	15%
35–44 years	15%	16%
45–54 years	26%	22%
55–64 years	12%	21%
65 years or older	5%	12%
Don't know/refused	0%	2%
Education		
High school diploma or less	21%	27%
Some college	30%	30%
College graduate	49%	43%
Don't know/refused	0%	0%
Annual Household Income		
< $50,000	44%	33%
$50,000–$99,000	36%	32%
$100,000+	21%	20%
Don't know/refused	0%	15%
Race		
White	81%	80%
Nonwhite	19%	20%
Monthly Broadband Bill		
< $20	8%	2%
$20–$39	38%	33%
$40+	54%	36%
Don't know/refused	0%	29%

To determine how well this sample compares with the U.S. broadband population, we compared it with a sample collected by the Pew Research Center in May 2010 and used in its 2010 Home Broadband Adoption study (Smith, 2010). This sample was intended to be representative of the U.S. adult population as a whole, not just broadband users. A combination of landline and cellular random digit dial (RDD) samples was used to represent all adults in the continental United States who have access to either a landline or cellular telephone. Of this sample, 86% was composed of broadband users. The demographic characteristics of these broadband users are compared with the characteristics of those in our sample. As we can see, the demographic characteristics are relatively similar across both samples. However, it is important to note that our sample does appear to be slightly younger and slightly more educated than the broadband users included in the Pew sample.

3.3 Statistical Analysis of Survey Data Collected

The first research question of this paper is to quantify U.S. broadband user preferences. However, the data collected through the survey described above do not allow us to quantify broadband user preferences directly, as we only observe the choices they make between hypothetical ISP security options. Instead, we can only quantify these preferences if we make a series of assumptions regarding the average broadband user's utility function. Specifically, we estimate broadband user preference parameters using a Random Utility Maximization (RUM) model.

The RUM model assumes that utility is defined as a function of the six attributes used to define a hypothetical ISP security package option and some random component. More formally, we define the utility a person receives from ISP security option j on choice task t by

$$u_{jt} = v_{jt}(\mathbf{X}_{jt}) + \varepsilon_{jt}, \qquad j = 0, 1, 2, \quad t = 1,\ldots,7, \tag{2.1}$$

where v_j is the deterministic (observable) component of utility that depends on the attribute levels that compose security option j in choice task t (represented as the vector $\mathbf{X}_{jt}$) and ε_j is a random error that represents the component of utility that is unobservable to the researcher.

We follow convention and assume that the deterministic portion of the utility function (v_j) follows a linear specification for utility such that preferences for the three alternatives on a given choice occasion are given by

$$U_{isp\_package} = \beta_{fee}*\boldsymbol{fee^i} + \beta_{time}*\boldsymbol{time^i} + (\beta_{never\_limit\_access}) + \beta_{restrict\_access\_if\_user\_hacked}) +$$
$$\beta_{can\_cutoff\_acces\_if\_user\_hacked})* \boldsymbol{x^i_{isp\_access}} + (\beta_{not\_reduced} + \beta_{somewhat\_reduced} + \beta_{greatly\_reduced})$$
$$\boldsymbol{x^i_{comp\_crash}} + (\beta_{not\_reduced} + \beta_{somewhat\_reduced} + \beta_{greatly\_reduced}) \boldsymbol{x^i_{ident\_theft}} + (\beta_{not\_reduced} +$$
$$\beta_{somewhat\_reduced} + \beta_{greatly\_reduced}) \boldsymbol{x^i_{risk\_to\_others}} + \varepsilon^i_{isp\_package} \tag{2.2}$$

$$U_{neither\_package} = \beta_0 * D_{neither\_package}{}^i + \varepsilon^i_{neither\_package}$$

where $\boldsymbol{fee^i}$ is the price of alternative i, $\boldsymbol{time^i}$ is the time associated with complying with ISP security requirements in alternative i, $\boldsymbol{x^i_{isp\_access}}$ is a vector of three indicator variables for different levels of the "limits placed on Internet access" attribute, $\boldsymbol{x^i_{comp\_crash}}$ is a vector of three indicator variables for different levels of "improved computer performance" attribute, $\boldsymbol{x^i_{ident\_theft}}$ is a vector of three indicator variables for the "reduced risk of identity theft" attribute, $\boldsymbol{x^i_{risk\_to\_others}}$ is a vector of three indicator variables for the "reduced risk to other individuals and businesses from your insecurity" attribute, and $D_{neither\_vaccine}{}^i$ is an indicator variable equal to 1 if alternative i is "neither package."

The RUM model presented above was estimated using a mixed-logit model in Stata 11.[2] In this

---

[2] Mixed logit was chosen over simpler methods of estimation, like conditional logit, because it treats variation

estimation, variables fee and time were entered as continuous variables in the regression, while indicator variables for the other 4 attributes were entered as effects coded variables. A primary advantage of this approach is that it allows us to interpret the β parameters as relative importance weights. Specifically, $(-\beta_{fee})$ represents the marginal utility of income and $(-\beta_{time})$ represents the marginal utility of time. The remaining β parameters can be interpreted as relative importance weights (also known as part-worth utilities), where larger values of β indicate greater utility.

After the RUM model has been estimated, the β parameters can be used to make the calculations required to address the remaining two research questions of this paper. First, they are used to estimate how much the average broadband user is willing to pay for changes in the levels of a particular ISP security package attribute (also known as a marginal WTP). A marginal WTP can be estimated by dividing the difference between the part-worth utilities of the two attribute levels in question by the marginal utility of income. For example, the mean marginal WTP to move from a package where the ISP can totally cut off a person's Internet access if her computer is infected with malware to a package where the ISP can never cut off a person's Internet access.

For example, the mean marginal WTP to move from a package where the U.S. government had unlimited access to one's personal information to a package where the government had no access equals the difference between the part-worth utilities for these two levels divided by the marginal utility of money: $[\beta_{never\_limit\_access} - \beta_{can\_cutoff\_acces\_if\_user\_hacked}]/(-\beta_{fee})$.[3] Standard errors and confidence intervals for these estimated marginal WTP measures were estimated using a Krinsky-Robb bootstrapping procedure with 10,000 iterations (Krinsky & Robb, 1986; Krinsky & Robb, 1990).

Second, the estimated RUM model results are used to estimate the maximum amount the mean broadband user would be willing to pay for a hypothetical security package offered by ISPs relative to having no package. For the purposes of this study, we consider two hypothetical security packages. First, we consider the package that would be most preferred by home broadband users. This package would include 0 hours each month complying with ISP security requirements, the ISP can never limit the user's Internet access, the risk of the computer slowing down is greatly reduced, the risk of identity theft is greatly reduced, and the risk to other individuals from user insecurity is greatly reduced. Although this package would likely be unfeasible from the perspective of the ISP, the WTP estimated for this package would represent the most broadband users would ever pay for ISP-based security solutions.

The second hypothetical package we consider in this study is one that is similar to the type of ISP-based security solutions discussed above. Specifically, this package would "quarantine" users that were identified as having malware on their machines and require them to spend time removing this malware from their machine. This package would certainly benefit individuals besides the user herself because such a package would go toward preventing the spread of botnets and other cyber security threats. However, it is readily apparent how much benefit the broadband user herself would receive from this package. Therefore, to achieve a conservative WTP, we assume she receives no direct benefit. In terms of the attribute levels used in the choice experiments, this package would be described as including 3 hours of time each month complying with ISP security requirements, the ISP can entirely cut off the user's Internet access if the ISP suspects the user has been hacked, the risk of the computer slowing down is not reduced, the risk of identity theft is not reduced, and the risk to other individuals from user insecurity is greatly reduced.

The maximum amount broadband users would be WTP for this package can be calculated by estimating the difference between the total utility a given security package yields and the total utility a no-package alternative yields, which is done using what is known as the "log-sum" formula (derived in

---

in respondent preferences as a statistical property, which greatly improves the fit of the model. For this reason, mixed-logit has become the best-practice method for conjoint analysis modeling.

[3] The intuition behind this calculation is that the difference between the part-worth utilities of the two levels under consideration provides one with the number of "utils" gained from making the package change. These "utils" are converted to monetary units by dividing by the marginal utility of income $(-\beta_{fee})$.

Train, 2003). For example, say we wanted to estimate the maximum WTP (relative to the no-package alternative) for the most preferred ISP security package. This would be estimated as follows:[4]

$$\text{Max Mean WTP} = (-1/\beta_{\text{fee}}) * [\ln(\exp(\beta_{\text{time}}*0 + \beta_{\text{never\_limit\_access}} + \beta_{\text{crash risk greatly reduced}} + \beta_{\text{id theft risk greatly}}$$
$$_{\text{reduced}} + \beta_{\text{risk to others greatly reduced}}) + \exp(\beta_0 - \beta_{\text{fee}}*\$7.15 - \beta_{\text{time}}*1.40)) -$$
$$\ln(\exp(\beta_0 - \beta_{\text{fee}}*\$7.15 - \beta_{\text{time}}*1.40))] \qquad (2.3)$$

Here again, standard errors and confidence intervals for these estimated marginal WTP measures were estimated using a bootstrapping procedure with 10,000 iterations.

4. Estimation Results

4.1 Quantified U.S. Broadband User Preferences

For the first research question, Table 3 presents results from our mixed logit model, which quantifies preferences for U.S. broadband users. Based on the size and sign of model coefficients, we can see that user preferences coincide well with the hypotheses stated in constructing our conceptual model. Specifically, increases in the cost of Internet access decrease personal utility, increases in the time it takes to comply with ISP security requirements decrease personal utility, improvements in a user's access to the Internet increase utility, improvements in the performance of a user's computer increase utility, improvements in computer performance increase utility, and increases in losses incurred by others reduce an individual user's utility.

We can also see from these results that the cyber security outcome (or benefit) that matters most to broadband users is reduction in the risk of identity theft. This is demonstrated by the fact that the part-worth utility associated with great reductions in the risk of identity theft (0.43) is larger than the part-worth utility associated with great reductions in the risk of the computer slowing down or crashing (0.32) or risk to others (0.21).

4.2 Marginal Willingness to Pay for Changes in ISP Security Package Features

For the second research question, we calculate the mean marginal WTP estimates for changes in each ISP security package feature from their least to their most favored level. Table 4 reports these mean marginal WTP estimates as well as 95% confidence intervals. As hypothesized, the mean U.S. broadband user is willing to pay positive sums for improvements in their security as well as the security of others (as the confidence intervals indicate, all values are statistically different from zero at the 5% significant level). Specifically, respondents were willing to pay $6.51 per month to greatly reduce the risk of identity theft (other things being equal). If ISPs could achieve and charge for such an improvement, this would represent a 14% increase in ISP revenue over the current mean monthly broadband bill. In terms of improvements in other cyber security outcomes, respondents were willing to pay $4.40 per month to greatly reduce the risk of their computer crashing and $2.94 per month to greatly reduce the risks of cyber security threats to others that may result from their personal insecurity. This third result conflicts with past views (e.g., Anderson, 2001; Varian, 2000) that doubted whether Internet users would be willing to pay to improve the security of others.

In terms of nonmonetary costs associated with ISP security packages, the mean broadband user is willing to accept these costs in exchange for cash payments (such as reductions in their monthly internet bill). For example, the mean WTP to avoid 1 hour spent complying with ISP security requirements was only $0.73 per month. Alternatively, this means respondents would only have to be paid $0.73 per month

---

[4] Please note that the $7.15 and 1.40 hours are the mean dollars and time shown to respondents in the hypothetical choice tasks. The subtraction of $\beta_{\text{fee}}*\$7.15$ and $\beta_{\text{time}}*1.40$ from the alternative-specific constant, β_0, is necessary because we used continuous fee and time terms and effects-coding for the other parameters.

Table 3: Preference Parameter Estimates (coefficients from mixed logit model)

	Estimated Mean Coefficient	Standard Error of the Mean	Estimated Standard Deviation	Standard Error of the Standard Deviation
Add a fee to provide security services to Internet subscribers	−0.14**	0.00	NA	NA
Require Internet users to follow certain security packages and be trained regularly	−0.10**	0.01	NA	NA
Limit Internet access for customers whose computers show signs of being "hacked"				
Never limit access	0.31**	0.02	0.51	0.03
Only restrict access	−0.01**	0.02	0.00	0.05
Entirely cut off access	−0.30**	0.02	NA	NA
Reduced risk of the user's computer slowing down or crashing				
Not reduced	−0.30**	0.02	0.26	0.05
Somewhat reduced	−0.02**	0.02	−0.09	0.08
Greatly reduced	0.32**	0.02	NA	NA
Reduced risk of the user's identity being stolen				
Not reduced	−0.49**	0.02	−25.23	0.00
Somewhat reduced	0.06**	0.02	0.92	0.36
Greatly reduced	0.43**	0.02	NA	NA
Reduced risk to other individuals and businesses from the user's insecurity				
Not reduced	−0.21**	0.02	−0.10	0.08
Somewhat reduced	0.00**	0.02	−0.01	0.04
Greatly reduced	0.21**	0.02	NA	NA
No choice alternative (adjusted)	−0.46**	0.07	1.17	0.42

Note: (1) Effects-coded variables were used for all attributes except fee and time spent complying with security requirements. (2) Standard errors on omitted coefficients were estimated by Krinsky-Robb parametric bootstraps. (3) *** denotes $p < 0.01$, **$p < 0.05$, *$p < 0.10$.

to be indifferent to these requirements (all else being held constant). Such a payment would represent a 1.6% decrease in the mean monthly broadband bill of respondents participating in the survey ($46 per month).

By contrast, U.S. broadband users were much more reluctant to accept limitations on their Internet access. Specifically, we estimate the mean WTP to shift from allowing ISPs to entirely cut off one's Internet access to never being allowed to restrict one's access would be $4.32 per month. Or, conversely,

Table 4: Mean Willingness to Pay for Improvements in ISP Security Package Features

	Estimated WTP ($/month)	95% Confidence Interval
Time Spent Complying with ISP Security Requirements: WTP to avoid 1 hour of time complying with security requirements	0.73	[0.57 to 0.92]
Limiting Internet Access: WTP to move from ISP being able to entirely restrict access to not restrict access at all	4.32	[3.72 to 4.92]
Risk of Computer Slowing Down or Crashing: WTP to move from not reduced to greatly reduced	4.40	[3.83 to 4.97]
Risk of Identity Theft: WTP to go from not reduced to greatly reduced	6.51	[5.86 to 7.16]
Risk to Other Individuals and Businesses: WTP to go from not reduced to greatly reduced	2.94	[2.44 to 3.45]

Note: 95% confidence interval was estimated using Krinsky-Robb parametric bootstrapping technique.

respondents have to be paid $4.32 per month to be indifferent to a shift in the other direction (all else being held constant). This would represent a 9% reduction in the mean monthly broadband bill.

4.3 Maximum Willingness to Pay for Hypothetical ISP Security Packages

For the third research question, we estimate the maximum amount the mean broadband user is willing to pay for two hypothetical ISP security packages—the first is the package most preferred by broadband users and the second is the package where respondents would be subject to "quarantine." Table 5 summarizes the results of our analysis.

The mean WTP for the most preferred ISP security package was $7.24. This estimate represents the most an average broadband user would ever pay for an ISP security package that offers all the benefits considered in our experiment. We estimated a 95% confidence interval for this WTP using by Krinsky-Robb parametric bootstraps and found the lower confidence limit to be $6.51 per month and the upper confidence limit to be $7.97 per month.

The mean WTP for the quarantine package is $1.34 with a 95% confidence interval from $1.14 to $1.54. Although this WTP estimate is 81% less than our estimate for the mean WTP for the most preferred ISP security package, it is based on very conservative assumptions and is still significantly different from zero. This suggests that the average broadband Internet user would indeed be willing to pay for a package that quarantined users infected with malware from the Internet until they had removed the harmful software from their machine. Again, this result conflicts with past views on this topic (e.g., Anderson, 2001; Varian, 2000). However, the relatively small amount users are willing to pay for this package ($1.34 or potentially a 2.9% increase in mean revenue per person) may not be enough to cover the cost of implementing such a program.

Table 5: Willingness to Pay for Hypothetical ISP Security Package

	Estimated WTP ($/month)	95% Confidence Interval
Most Preferred Package: 0 hours each month complying with ISP security requirements, ISP can never limit the user's Internet access, risk of computer slowing down is greatly reduced, risk of identity theft is greatly reduced, and risk to other individuals from user insecurity is greatly reduced.	7.24	[6.51 to 7.97]
Quarantine Package: 3 hours of time each month complying with ISP security requirements, ISP can entirely cut off the user's Internet access if the ISP suspects the user has been hacked, risk of computer slowing down is not reduced, risk of identity theft is not reduced, and risk to other individuals from user insecurity is greatly reduced.	1.34	[1.14 to 1.54]

Note: The 95% confidence interval was estimated using Krinsky-Robb parametric bootstrapping technique.

4.4 Future Research Question: The Impact of Information Treatments on Willingness to Pay for Hypothetical ISP Security Packages

In this paper, we have found evidence that suggests that the mean broadband user is WTP for ISP security packages that protect themselves and others from cyber security threats. However, the majority of broadband users are typically ill informed regarding the threat malware or botnets may pose. This fact raises the question of whether broadband users would be willing to pay more if they were better informed of the dangers associated with cyber security threats.

To investigate this question, we showed each survey respondent an information treatment (which in reality could be a marketing message from their ISP or an educational message from a government entity) early in the survey to affect the cyber security perceptions and choices of survey respondents. Specifically, we created seven information treatments designed to influence (1) broadband users' perceptions of cyber security threats and (2) the amount broadband users are willing to pay for ISP security packages. Table 2 provides brief descriptions of the information treatments used. In future research we intend to explore whether these information treatments influenced survey respondents' perceptions of cybersecurity threats or ISPs and whether they increased the amount they were willing to pay for hypothetical ISP security packages.

5. Conclusions

The purpose of this paper was to explore three research questions. First we sought to quantify U.S. broadband users' preferences. We found that broadband Internet users have clear preferences over several features of ISP security packages and, not surprisingly, favor packages that impose fewer costs and provide greater reductions in cyber security risks. In particular, the cyber security risk that broadband users appear to be most worried about is the risk of identity theft.

Second, we explored how much U.S. broadband users are willing to pay for changes in individual features of ISP security packages. The results of our analysis suggest that U.S. broadband users are indeed willing to pay positive and statistically significant sums to ISPs to achieve improvements in their own security as well as the security of others. Specifically, we found that home Internet users were

Table 6: Information Treatments

Information Treatment	Description of Information Treatment
1	A "**fear**" message directed at describing the consequences a respondent's insecurity has on *themselves*
2	A "**fear**" message directed at describing the consequences a respondent's insecurity has on *others*
3	A "**trust**" message directed at encouraging the respondent to trust their ISP in assisting with *securing their personal computer*
4	A "**trust**" message directed at encouraging the respondent to trust the ISP to monitor their Internet traffic in order *to thwart potential threats to others like botnets*
5	A combination of treatments 1 and 3
6	A combination of treatments 1 and 4
7	A combination of treatments 2 and 4

willing to pay up to $6.51 per month to greatly reduce the risk of identity theft, $4.40 per month to greatly reduce the risk of their computer crashing, and $2.94 per month to reduce the risks other individuals and businesses might face as a result of their personal insecurity.

In addition, we find that when ignoring the benefits that ISP security packages can yield, U.S. broadband users are also willing to accept the nonmonetary costs associated with these packages in exchange for only modest reductions in the monthly cost of Internet access. Specifically, respondents would have to be paid only $0.73 per month to accept an ISP security package that required them to spend 1 hour complying with ISP-determined security standards. Given that the mean monthly broadband bill for the sample was $46 per month, this compensation would correspond to 1.6% decrease in monthly ISP per-person revenue. Similarly, in order for home Internet users to accept a move from ISPs never being able to interrupt an individual's Internet access to allowing ISPs to entirely cut off one's Internet access if users are determined to be suffering from a security problem that may harm others, they would have to receive at least $4.32 per month in compensation. This dollar amount would correspond to a 9% reduction in the mean monthly broadband bill.

However, in the real world, broadband users would be asked to weigh the costs and benefits of a particular ISP security package simultaneously. Therefore, we estimated the maximum WTP for several hypothetical ISP security packages. We found that the most an average broadband user will pay for an ISP security package is approximately $7.24 per month, which would represent a 16% increase in the current average monthly broadband bill in the U.S. Furthermore, we found that, on average, broadband users were willing to pay for ISP security packages that primarily improved the security of other individuals. Specifically, the mean WTP for a package that required all individuals to spend 3 hours complying with ISP security requirements each month, enabled ISPs to entirely cut-off the internet access of users with machines infected with malware, and only reduced the risk to others from the user's own insecurity was $1.34.

In total, our research suggests that U.S. broadband users are willing to accept both monetary and non-monetary costs to improve their security and the security of others. This result conflicts with past

views that doubted whether Internet users would be willing to pay to improve the security of others. From the perspective of ISPs, our results also suggest that they may be able to increase revenue by offering more robust security solutions. However, it is not clear whether the amounts that broadband users are willing to pay are enough to cover the costs of various ISP security packages. It is also left to future research to determine whether marketing or educational awareness campaigns could be used to persuade broadband users to spend more on ISP security packages by making them more informed of the danger cyber security threats present and the potential effectiveness of ISP services.

6. References

Anderson, R. (2001). Why Information security is hard: An economic perspective. *Proceedings of the 17th Annual Computer Security Applications Conference.*

Anderson, R., Bohme, R., Clayton, R., & Moore, T. (2008). Analyzing barriers and incentives for network and information security in the internal market for e-communication. Retrieved June 1, 2011, from http://www.enisa.europa.eu/act/sr/reports/econ-sec.

Arbor Networks. (2010). 2009 Worldwide infrastructure security report. Retrieved February 21, 2010, from http://www.arbornetworks.com/report.

Clayton, R. (2010). Might governments clean-up malware? Retrieved http://weis2010.econinfosec.org/papers/session4/weis2010_clayton.pdf.

Gallaher, M., Rowe, B., Rogozhin, A., & Link, A. (2006). *Economic analysis of cyber security and private sector investment decisions.* Report prepared for the U.S. Department of Homeland Security. Research Triangle Park, NC: RTI International.

Hensher, D. A., Rose, J. M., & Green, W. H. (2005). *Applied choice analysis: A primer*. Cambridge, UK: Cambridge University Press.

Kanninen, B. (2002). Optimal design for multinomial choice experiments. *Journal of Marketing Research, 39*, 214–227.

Krinsky, I., & Robb, A. (1986). On approximating the statistical properties of elasticities. *Review of Economics and Statistics, 68*, 715–719.

Krinsky, I., & Robb, A. (1990). On approximating the statistical properties of elasticities: a correction. *Review of Economics and Statistics, 72,* 189-90.

Kuhfeld, W. F., Tobias, R. D., & Garratt, M. (1994). Efficient experimental design with marketing research applications. *Journal of Marketing Research, 31*, 545–557.

List, J., Sinha, P., & Taylor, M. (2006). Using choice experiments to value non-market goods and services: Evidence from field experiments. *Advances in Economic Analysis & Policy, 6*(2), 1–37.

Lichtman, D., & Posner, E. (2004). *Holding Internet service providers accountable.* University of Chicago John M. Olin Law and Economist Working Paper No. 217. Retrieved June 1, 2011, from http://www.law.uchicago.edu/files/files/217-dgl-eap-isp.pdf.

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection, 3*(3-4), 103–117.

Orme, B. (2010). *Getting started with conjoint analysis*. Madison, WI: Research Publishers, LLC.

Robinson, N., Potoglou, D., Kim, C., Burge, P., & Warnes, R. (2010). Security at what cost? In *Critical infrastructure protection IV: IFIP advances in information and communication technology, 342*, 3–15.

Rowe, B., Wood, D., Reeves, D., & Braun, F. (2011). *Economic analysis of ISP provided cyber security solutions*. Retrieved June 3, 2011, from https://www.ihssnc.org/portals/0/Rowe_IHSS_Cyber_Final_ReportFINAL.pdf.

Sawtooth Software, Inc. (2010). *SSI Web v.6.6.12: Choice based conjoint* [Computer Software]. Sequim, WA.

Smith, A. (2010). *Home broadband adoption 2010*. Retrieved June 3, 2011, from http://www.pewinternet.org/~/media//Files/Reports/2010/Home%20broadband%202010.pdf.

Smith, V., & Mansfield, C. A. (2006). *Valuing airline security: An analysis of the MANPADS program*. Paper presented at the Workshop on Benefit Methodologies for Homeland Security Analysis, Washington, DC, June 8–9.

StreamShield Networks. (2004). *Consumers prepared to pay extra for clean and safe Internet service*. Press release. Retrieved April 24, 2009, from http://www.streamshield.com/index.php?option=com_content&task=view&id=59&Itemid=130.

Train, K. (2003). *Discrete choice methods with simulatio*n. Cambridge: Cambridge University Press.

Varian, H. (2000). Managing online security risks. *The New York Times*. Retrieved June 3, 2011, from http: //www.nytimes.com/library/financial/columns/060100econ-scene.html.

Zwerina, K., J. Huber, and W. F. Kuhfeld. (1996). A *general method for constructing efficient choice designs*. SAS Working Paper. Retrieved June 3, 2011, from http://support.sas.com/techsup/technote/mr2010e.pdf.