2008

Processing Information Security Messages: An Elaboration Likelihood Perspective

Boon Yuen Ng
National University of Singapore, ngby@alumni.nus.edu.sg

A Kankanhalli
National University of Singapore, atreyi@comp.nus.edu.sg

PROCESSING INFORMATION SECURITY MESSAGES: AN ELABORATION LIKELIHOOD PERSPECTIVE

Ng, Boon-Yuen, National University of Singapore, Department of Information Systems, School of Computing, Computing 1, Law Link, Singapore 117590, Singapore, ngby@comp.nus.edu.sg

Kankanhalli, Atreyi, National University of Singapore, Department of Information Systems, School of Computing, Computing 1, Law Link, Singapore 117590, Singapore, atreyi@comp.nus.edu.sg

Abstract

The increasing number of security incidents is causing great concern to organizations. Information security awareness programs are an important approach towards educating users to prevent such incidents. However, it is unclear how to effectively design security programs and messages such that they can inform and change user behaviour. The role of individual factors in influencing the processing of security messages is also unclear. This paper attempts to investigate these problems by studying the effects of security message characteristics and recipient factors on users' attitude towards security, using the information-processing theory of elaboration likelihood. Two models are developed for this study. The first model studies two message characteristics, argument quantity and quality, as determinants of attitude towards security. A 2x2 factorial design experiment will be conducted to investigate the influence of these characteristics on attitude moderated by the elaboration likelihood towards the security message. The second model tests the effect of four recipient factors on elaboration likelihood. The model development, experimental methodology, and data analysis details are described in this research-in-progress paper. The results are expected to inform the design of effective security messages and contribute to research in this area.

Keywords: Security education and awareness, information systems security, behaviour

1 INTRODUCTION

Organizations and individuals today are highly dependent on the use of information systems for their information processing needs. The security of these systems is therefore critical to preserve the confidentiality, integrity, and availability of the information. However, the increasing frequency of security incidents is of great concern to organizations (Kankanhalli & Teo & Tan & Wei 2003). According to the annual CSI/FBI survey (Richardson 2007), 46% of respondents indicated that their organization experienced unauthorized use of computer systems within the last 12 months. Home users are also not spared from security threats as home computers are typically not secure and vulnerable to hacking (CERT 2007). It is therefore important for organizations and individuals to be aware of and protect themselves against possible security threats.

In the face of security threats, organizations have implemented a variety of technical measures such as firewalls and intrusion detection systems to bolster their defenses. However, deploying sophisticated security techniques is not sufficient in preventing security incidents. The human factor has always been regarded as the weakest link in security solutions (Siponen 2000, Sasse & Brostoff & Weirich 2001). User behaviour, e.g., choosing easy-to-guess passwords or not installing patches, is found to play a part in many security failures. Therefore, management has realized the importance of security awareness training of users (Straub & Welke 1998, Thomson & Solms 1998). In fact, security can be viewed as practices by users and not just a set of security technologies implemented by the organization (Hayes 2003). Hence, design and conduct of information security awareness programs becomes an important part of an organization's security efforts.

Security awareness of home computer users should not be neglected either. Apart from individual damages, undefended home computers can become part of networks of remotely controlled machines that are then used to attack critical infrastructures (DHS 2003). Hence, national initiatives and programs to promote security awareness among home computer users have been developed and implemented. For example, the U.S. Department of Homeland Security has designated October 2007 as the National Cyber Security Awareness Month (DHS 2007), and the U.S. Computer Emergency Readiness Team provides computer security tips to home users (US-CERT 2007).

Information security awareness programs should educate users to become more aware of the risks and their responsibilities towards information security. The purpose is to stimulate, motivate and remind users of their role in information security (Peltier 2005). However, it is not clear how to effectively design information security awareness programs such that they can have maximum impact in terms of changing user behaviour. While there are many practical guidelines for designing security awareness programs (Wilson & Hash 2003, Peltier 2005), their effectiveness has not been investigated from an empirical or theoretical standpoint.

In particular, the way in which the security messages in the awareness program are framed is important in determining their effectiveness. However, there is little knowledge of how to design these messages to maximize their effectiveness. General guidelines such as keeping the message important, relevant and interesting to the users, as well as tips on how to convey the security message, have been suggested (Peltier 2005, Pratt 2006). However, specific effects of manipulating message characteristics have not been studied. The role of individual factors and how they influence the processing of security messages is also unclear. Therefore, this study attempts to investigate how users process the information in security awareness messages and determine the effects of security message characteristics and individual recipient factors on users' attitude towards information security.

A well-known theory on attitude change through message persuasion is the elaboration likelihood model (ELM). ELM explains the conditions under which people decide to think attentively or expeditiously (Petty & Cacioppo 1984a). When people think attentively and with effort in response to a message, they are more likely to be persuaded by the message and therefore behave according to what the message advocates. This is very relevant to information security awareness, as the central

tenet of organizational security awareness programs is to persuade employees and executives that security is important to them and to the organization (Somerson 2003).

Based on ELM, this study investigates the influence of message characteristics and recipient factors on attitude in the context of information security awareness. A 2x2 factorial experiment is designed to manipulate two message properties (argument quality and argument quantity) and observe the effect on attitude. The effect of recipient factors on elaboration likelihood is also studied. The results of this study are expected to benefit security practitioners by assisting them to design more effective information security awareness programs in future. Theoretically the study should provide a basis for application of information processing theories like ELM to the security awareness domain.

2 LITERATURE REVIEW

2.1 Information Security Awareness Programs

Information security awareness in organizations refers to a state where users in an organization are aware of and ideally committed to their security mission, often expressed in their organization's end-user security guidelines (Siponen 2000). Information security awareness programs are considered as the essential tool to educate employees of the organization. Such programs typically involve delivering or disseminating security messages throughout the organization. Techniques include delivery of simple messages on awareness tools such as post-it notes and posters, or more complex messages on newsletters, videotapes, web-based, computer-based or instructor-led sessions.

Thomson et al. (1998) suggest principles that will help improve the effectiveness of these programs. They propose that the behaviour of people can be changed in three ways: (1) directly changing their behaviour, regardless of their attitude to the subject (2) using a change in behaviour to influence a person's attitude, such as through role-playing exercises; and (3) changing a person's attitude through persuasion. Persuasion refers to the presentation of persuasive arguments (Petty et al. 1984b). The focus of this study is on changing a person's attitude through persuasion, since security messages in information security awareness programs are intended for that purpose. Behavioural theories suggest that a change in attitude will ultimately change people's behaviour (Ajzen 2001). Thus, if a person's attitude is changed through persuasion, it is highly predictive of a changed behaviour.

To change a person's attitude through persuasion, a five-step persuasion method has been proposed for information security awareness programs – exposure, attention, comprehension, acceptance, and retention (Thomson et al. 1998). First, users have to listen to the security message, and they have to pay attention to the message. To increase comprehension of the message, an appropriate medium should be used to transmit the information. The user has to accept the message for the attitude change to take place. Lastly, retention deals with ensuring that the attitudes are maintained for a long period.

As information security awareness programs typically involve the delivery of messages and the persuasion of computer users through these messages, it is most appropriate to study message-based persuasion. In particular, we are interested to study how recipients process information in a security awareness message, and how that may persuade them and change their attitude. Hence, the focus of this study is on comprehension and acceptance of the security awareness message.

2.2 Elaboration Likelihood Model

ELM has been used for explaining attitude change through persuasion (Petty & Cacioppo 1986). It has been widely applied in various areas, particularly to the persuasion of consumers by advertising messages (e.g., Chebat & Charlebois & Gelinas-Chebat 2001, Laroche & Cleveland & Maravelakis 2002). Its application in information systems research has been limited but growing in recent years. Examples of phenomena studied include knowledge adoption in organizations (Sussman & Siegal

2003), sustained technology usage (Angst & Agarwal 2004), IT acceptance (Bhattacherjee & Sanford 2006), and persuasion for web personalization (Tam & Ho 2005).

As defined by Cacioppo and Petty (1984a), elaboration likelihood refers to the "likelihood one engages in issue-relevant thinking with the aim of determining the merits of the arguments for a position." ELM proposes that people are neither universally thoughtful nor mindless in evaluating persuasive messages. Instead, the amount of cognitive effort a person devotes to processing a message depends on a number of situational and individual factors (Petty et al. 1984a).

Depending on the cognitive effort expended, ELM posits that there are two different routes that lead to attitude change, i.e., central route and peripheral route. The central route involves effortful cognitive activity in which the message recipient carefully evaluates all the information presented in support of the advocated position. The recipient considers the quality of the message content and the merits of the arguments. In such a situation, the elaboration likelihood of the message is high. When elaboration likelihood is high, the most direct determinant of the recipient's reactions to the recommendation in the message is issue-relevant thinking. Consequently, the recipient is likely to derive an overall evaluation of, or attitude toward, the recommendation in the message (Cacioppo et al. 1984a).

The peripheral route involves the use of simple cues, decision rules or heuristics rather than systematically processing the message arguments. For example, upon reading a message from an expert, the message recipient may employ the heuristic that "experts are generally correct" without the message recipient devoting much effort to assess the actual merits and implications of the arguments provided (Chaiken 1987). Similarly, a message with many arguments can be accepted if a person thinks that "more arguments are better", without the need to carefully evaluate the truth of those arguments (Petty et al. 1984a). In such situations, elaboration likelihood tends to be low, and the most important determinant of persuasion tends to be cues.

Hence, the level of elaboration lies on a continuum which is defined by how motivated and able a person is to assess the merits of the attitude object (Petty & Wegener 1999). The central route is more likely to be taken if both motivation and ability to elaborate are high. The peripheral route is more likely if the motivation and/or ability to elaborate are low. Research has shown that attitude changes that result from central route processing of issue-relevant arguments will show greater temporal persistence, greater prediction of behaviour, and greater resistance to counter-persuasion than attitude changes that result from peripheral cues (Petty et al. 1986). There are various recipient factors that may affect elaboration likelihood, which are described in the next section under Hypotheses 4 to 7.

3 RESEARCH MODEL AND HYPOTHESIS

Consistent with previous studies (e.g., Petty & Cacioppo & Goldman 1981, Petty et al. 1984a, Bhattacherjee et al. 2006) and our objective, the dependent variable in our model is *attitude* towards security. A high level of *elaboration likelihood* is likely to lead to attitude changes that show greater temporal persistence and greater prediction of changed behaviour (Petty et al. 1999). Thus, our purpose is to investigate the factors that would lead to a high level of elaboration and a favourable attitude towards information security. We will focus on two particular message properties i.e., *argument quality* and *argument quantity*, which may affect the attitude of the recipient depending on whether the recipient processes the message by the central or peripheral route. In addition, we will measure four message recipient factors, i.e., *general security orientation, need for cognition*, *personal relevance* and *prior knowledge*, that may affect the elaboration likelihood of message recipients.

Argument quality refers to the persuasive strength and effectiveness of arguments in an informational message. Stronger argument quality should lead to greater persuasion and a changed attitude (Petty et al. 1986). In a recent study of influence processes for IT acceptance, findings indicate that argument quality has a positive effect on the individual's perceived usefulness and therefore attitude towards IT acceptance (Bhattacherjee et al. 2006). Hence, we hypothesize:

H1: Argument quality is positively related to attitude towards information security.

Past research has shown that increasing the number of arguments in the message can increase persuasion as it provides more information for people to think about (Petty & Cacioppo, 1984b). For those who are motivated and able to process the message, they may generate favorable issue-relevant thoughts to these arguments. For those who are unmotivated or unable to process the message, they might still be persuaded by the simple heuristic that "the more arguments the better", resulting in a change in attitude (Petty et al. 1984b). Hence, we hypothesize:

H2: Argument quantity is positively related to attitude towards information security.

Argument quality has often been regarded as a central variable, i.e., a variable that is important when the recipient processes the information in the central route (Bhattacherjee et al. 2006). This means that the effect of argument quality on the recipient's attitude is greater when the level of elaboration likelihood is higher (Petty et al. 1984b). In a laboratory experiment that examines information bias in contingent evaluation, findings indicate that willingness to pay for a good increases with argument quality, especially under conditions of high personal relevance (Ajzen & Brown & Rosenthal 1996). It is important to note that argument quality manipulation also serves as a methodological tool to examine the impact of other variables on elaboration likelihood (Petty et al. 1999). In this study, argument quality serves as a central route variable as well as a means to test the impact of recipient factors on elaboration likelihood. Under conditions of high elaboration likelihood, central route variables are likely to have a stronger influence on the recipient than peripheral cues. Hence, we hypothesize:

H3a: Under conditions of high elaboration likelihood, argument quality has a stronger effect than argument quantity on attitude towards information security.

Past studies have shown that under low issue involvement (i.e., low motivation to process arguments), people do not evaluate the message arguments but look at the number of arguments in the message as a peripheral cue (Petty et al. 1984b). Individuals may employ the heuristic that the more arguments, the more convincing the message is. Without the motivation or ability, message recipients are unmotivated or unable to process the arguments of the message and therefore rely more on peripheral cues rather than the quality of the arguments. Hence, in low elaboration likelihood, attitudes are affected mainly by argument quantity rather than argument quality. Hence, we hypothesize:

H3b: Under conditions of low elaboration likelihood, argument quantity has a stronger effect than argument quality on attitude towards information security.

A recipient's general security orientation refers to his or her predisposition and interest concerning practicing computer security (Ng & Xu 2007). This is also related to the recipient's consciousness about security issues and the strategies to deal with these issues (Dinev & Hu 2007). A person with a greater general security orientation is likely to be more concerned about security and therefore has more motivation to process security awareness messages. A person with a greater general security orientation is also likely to be more well-informed about security issues and therefore has more ability to process security awareness messages. Hence, a stronger general security orientation is likely to translate to a higher level of elaboration likelihood for security awareness messages.

H4: A message recipient's general security orientation is positively related to the elaboration likelihood of a security message.

Need for cognition is a personal disposition that refers to the scale of individuals' tendency to engage in and enjoy effortful cognitive endeavors (Cacioppo & Petty & Kao 1984b). It is regarded as a motivational variable. Past studies indicate that personal disposition, such as need for cognition, plays an important role in processing a persuasion message (e.g., Areni & Ferrell & Wilcox 2000). Hence, if a person has a high need for cognition, that is likely to translate to a high level of elaboration likelihood.

H5: A message recipient's need for cognition is positively related to the elaboration likelihood of a security message.

Another important motivational variable is personal relevance. If a person deems the message as personally relevant, he or she is likely to be more motivated to process the arguments of the message. Thus, personal relevance is likely to have a positive relationship with elaboration likelihood (Petty & Cacioppo & Shumann 1983, Celsi & Olson 1988).

H6: A message recipient's personal relevance is positively related to the elaboration likelihood of a security message.

Last, prior knowledge refers to what the individuals knows about the topic of interest. If a person has the appropriate background knowledge, this gives him/her the ability to process the arguments of the message (Petty et al. 1999) and thus have higher elaboration likelihood.

H7: A message recipient's prior knowledge of the message topic is positively related to the elaboration likelihood of a security message.

Figure 1 shows our research models. Model 1 consists of H1 to H3, and Model 2 consists of H4 to H7. The four recipient variables are not manipulated in the experiment but their effect on elaboration likelihood is tested separately in Model 2.

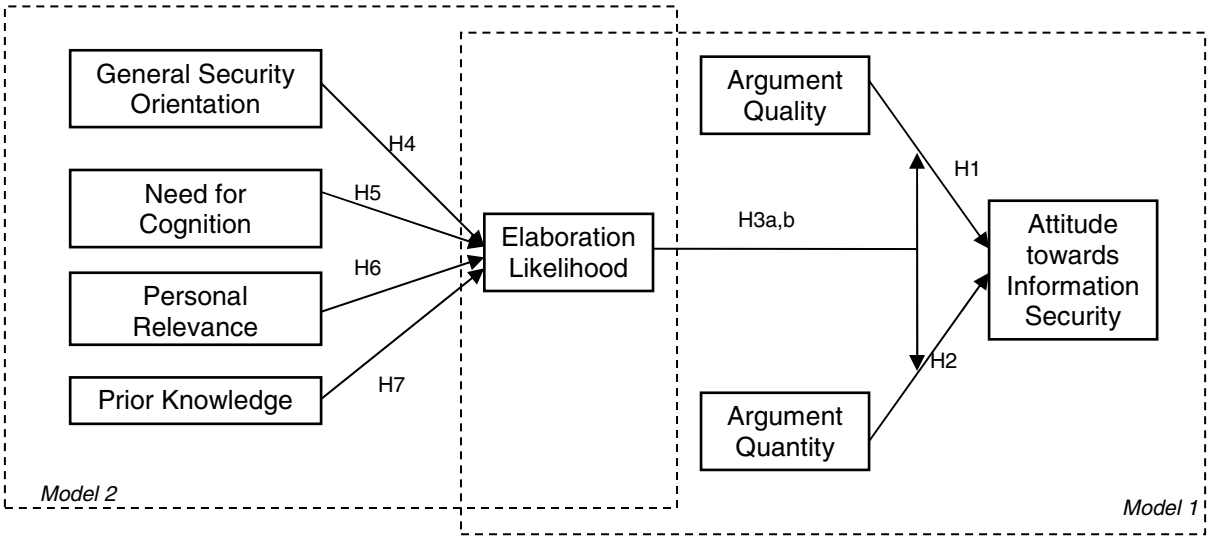

Figure 1: Research Model.

4 METHOD

To test the above hypotheses, a laboratory experiment will be conducted. The details and the method to be used are described below.

4.1 Design

The experiment is a 2 (argument quality: weak or strong) x 2 (argument quantity: low or high) between-subject design. Most of the past studies involve manipulating the level of elaboration likelihood by manipulating personal relevance (e.g., Petty et al. 1984b). However, we choose to design the experiment in a different way. Elaboration likelihood is allowed to vary freely according to recipient differences, while the two message variables are manipulated in the experiment.

4.2 Task and Procedures

Subjects will first receive instructions and a short questionnaire. They will be told that they are to answer background questions first, after which they will given a security article to read. They will then be asked to answer questions based on the article. The first questionnaire contains demographic questions as well as questions on general security orientation, need for cognition, personal relevance and prior knowledge. After completing and submitting the first questionnaire, subjects will receive the security message, which they are asked to read. The security message will be written in a "newsletter article" style. The article should be returned after reading, after which the subjects will receive a second questionnaire. The second questionnaire contains items on elaboration likelihood, argument quality, argument quantity, and attitude towards information security. After completing the questionnaire, subjects will be debriefed and given a small token of appreciation.

While it is possible to design a security message that is general and deals with basic security, we choose to design a message that is based on a relatively unknown topic to reduce the possibility that subjects know the topic well and have already formed a favorable attitude towards the topic. One of the lesser known practices is the use of a personal firewall. While most people have installed anti-virus software on their computers, less people use personal firewalls or are aware about the functionalities and benefits of a personal firewall. Hence, the article used in the experimental task is about the use and benefits of a personal firewall.

4.3 Participants

We will look for 80 volunteers from undergraduates in a large university. The subjects will come from different faculties in the university. Subjects will be randomly assigned to any of the four treatment groups such that there will be 20 subjects per cell (see Table 1).

Argument Quantity / Argument Quality	Low	High
Weak	20	20
Strong	20	20

Table 1: Treatment Groups

4.4 Manipulation

To increase the experimental realism, the article will be framed as a security newsletter article. The article will contain two main sections: (1) Why security is important (2) Personal firewall. Both sections will contain persuasive arguments. To manipulate argument quality, three strong and three weak arguments will be prepared for Section 1, and six strong and six weak arguments will be prepared for Section 2. The strong arguments are convincing and relevant arguments about why it is important to practice security and use a personal firewall. The weak arguments are trivial reasons why security is important and why it is good to use a personal firewall. The arguments will be pre-tested in a pilot test to ensure successful manipulation.

Following guidelines used in previous studies that manipulate argument quality (Petty & Harkins & Williams 1980), the strong arguments contain persuasive evidence, such as statistics and relevant studies. The weak arguments rely more on personal examples and personal opinion, and hence the weak arguments are less persuasive and more uncertain compared to the strong arguments. While it is important to effectively manipulate argument quality, it is also important to maintain experimental realism. Hence, the weak arguments should not look foolish or nonsensical. Table 2 gives examples of strong and weak arguments in the security message. To reduce any possible confounding factors, the writing style and grammar should be kept as similar as possible.

Strong Argument Quality	Weak Argument Quality
According to the annual CSI/FBI survey, unauthorized access is one of the biggest threats to a PC system. Hackers can cause severe damage by stealing your valuable personal data such as bank account numbers and passwords. A firewall can prevent unauthorized access and is therefore essential to protect your PC. (use of studies)	People feel that strangers breaking into their computers may be a big threat. A student had his bank account information stolen by hackers from his laptop, but after installing a personal firewall, he felt that his personal information is safe. (personal opinion and personal example)
PC firewalls allow only authorized traffic to pass between the Internet and your PC. Studies have shown that a PC firewall can block 80% of all unauthorized intrusions. Thus installing a PC firewall can reduce the possibility of unauthorized intrusions from occurring. (use of studies and statistics)	PC firewalls may allow only authorized traffic to pass between the Internet and your PC. People believe that installing a PC firewall can block unauthorized access. (personal opinion)

Table 2: Examples of Arguments

Argument quantity will be manipulated by varying the number of arguments in Sections 1 and 2. For the low argument quantity group, there will be one argument for Section 1 and two arguments for Section 2, giving a total of three arguments. For the high argument quantity group, there will be three arguments for Section 1 and six arguments for Section 2, giving a total of nine arguments. The numbers three and nine are chosen because these numbers were demonstrated to be adequately different in a prior study (Petty et al. 1984b). The arguments in the low argument quantity message are a subset of the arguments used in the high argument quantity message.

With the above manipulations, Table 3 shows what each subject would see in his/her message, according to the treatment group that he/she is randomly assigned to.

Argument Quantity / Argument Quality	Low	High
Weak	3 weak arguments	9 weak arguments
Strong	3 strong arguments	9 strong arguments

Table 3: Messages of Treatment Groups

4.5 Measures

The following variables are to be measured through the questionnaire: elaboration likelihood, attitude towards security, need for cognition, personal relevance, prior knowledge, and general security orientation. Argument quality and argument quantity are to be measured too for the purposes of manipulation checks. In operationalizing these constructs, it is important to ensure the content validity, construct validity, and reliability of these constructs (Straub 1989). How each construct is measured is described below.

General Security Orientation – Ng et al. (2007) has developed a scale consisting of four items to measure general security orientation. It has demonstrated adequate reliability and is hence adopted for this study.

Need for Cognition (NFC) – Cacioppo and Petty (1982) developed an instrument consisting of 34 items to measure individuals' NFC. To enhance its efficiency as an assessment instrument, the number of items was subsequently reduced to 18 (Cacioppo et al. 1984b) without sacrificing reliability and it

shows strong correlation with the original scale (Cacioppo et al. 1984b). To keep the questionnaire to a reasonable length, we chose eight items from the revised scale for this study.

Personal Relevance – Zaichkowsky (1985) developed an instrument (Personal Involvement Inventory) to measure level of involvement. This instrument is also used to measure personal relevance as perceived personal relevance is the essential characteristic of involvement (Celsi et al. 1988). The complete instrument consists of 20 items. We chose four items which are more relevant to this study.

Prior Knowledge – Adapting the scale from Chebat et al. (2001), prior knowledge is measured through two items – level of general knowledge in security, and level of knowledge concerning the functionalities of a personal firewall. An additional item is added to find out subjects' prior knowledge in the benefits of a personal firewall.

Elaboration Likelihood – We chose two methods employed by Petty et al. (1986) to measure elaboration likelihood: (1) Self-reported cognitive effort – This involves asking subjects directly the amount of effort they expended in processing the message. (2) Argument recall – This procedure involves giving subjects an amount of time to recall and list all the arguments from the message. Independent judges are appointed to assess the validity of the arguments and count the number of arguments listed. Self-report is more subjective while argument recall is more objective. Hence, the combination of the two methods will increase the validity of the measure. Subjects will be asked to evaluate how much effort they spent to evaluate the security message and list the arguments they can recall. The number of arguments will be coded and mapped to a number that is consistent with the Likert scale used in the rest of the questionnaire.

Argument Quality – Sussman et al. (2003) has developed a Likert scale that measures completeness, consistency, and accuracy as dimensions of argument quality. This scale was adapted by Bhattarcherjee et al. (2006) to measure whether the information provided during training sessions is informative, helpful, valuable and persuasive. Here, we adapt the scale from Bhattarcherjee et al. (2006) to measure the perceived argument quality of the security message.

Argument Quantity – Petty et al. (1984b) suggested including a question to check subjects' perceptions of the number of arguments. Adapting from their original question, the question used in this study will be "About how many arguments are there in the article you read?" Subjects may record any number they wish (Petty et al. 1984b).

Attitude towards Information Security – The standard scale for attitude can be taken from Ajzen (2002). While it is possible to adapt the scale to measure attitude towards security in general, here we choose to operationalize this construct according to the context of the security message, to more accurately measure the persuasive effect of the message. Hence, the items measure specifically one's attitude towards using a personal firewall.

5 DATA ANALYSIS AND FUTURE PLAN

There are two stages in data analysis i.e., scale validation and hypothesis testing. Scale validation is necessary to assess instrument reliability and construct validity. It is also important to check if the manipulation of argument quality and argument quantity is successful.

5.1 Scale Validation

To assess reliability of the scale, Cronbach Alpha will be calculated for each construct. For internal consistency, Cronbach Alpha should have a value of at least 0.707 (Nunnally 1978). To further validate the scale, convergent and discriminant validity will be tested. Three criteria for convergent validity are suggested by Fornell and Larcker (1981): (1) all item loadings should exceed 0.70 (2) composite reliability of each construct should exceed 0.80 (3) the square root of each average variance extracted (AVE) for each construct should exceed 0.71. For discriminant validity, square root of AVE

for each construct should exceed the correlations between that and all other constructs (Fornell et al. 1981).

5.2 Manipulation Check

To check the effectiveness of manipulating argument quality, one-way ANOVA can be used to measure the difference between those in the strong argument quality group and those in the weak argument quality group using the items to measure argument quality. To assess the effectiveness of manipulating argument quantity, subjects will be asked to record the number of arguments they perceive. Again, one-way ANOVA can be used to measure the difference between the two treatment groups.

5.3 Hypothesis Testing

For Model 1, H1 and H2 can be tested using two-way ANOVA, as there are two independent categorical variables and one continuous dependent variable. H3a and H3b involve a moderator i.e., elaboration likelihood. As the moderator is a continuous variable, ANOVA will not be suitable as it will require artificially dichotomizing the variable, which is not recommended (MacCallum & Zhang & Preacher & Rucker 2002). The recommended approach for interactions with continuous variables is to use multiple regression analysis (Cohen & Cohen & West & Aiken 2003). Argument quality and argument quantity can be coded using dummy variables. Moderated multiple regression can be used to test the interaction effect (Jaccard & Turrisi & Wan 1990).

For Model 2, the effect of recipient variables on elaboration likelihood can be tested through regression. Another possibility is to use structural equation modelling methods (such LISREL or PLS) to test the entire model.

5.4 Future Plan

We have conducted a pre-test and carried out the experiment. We will analyze the data and present the findings at the conference.

6. CONCLUSION

This study uses an information processing and persuasion theory, the Elaboration Likelihood Model, to explore how individuals process security awareness messages. Two models have been developed. The first model investigates the effect of message argument quality and quality on attitude towards security. Elaboration likelihood is likely to moderate the relationships between message properties and attitude. An experiment has been designed to test the model by manipulating the message properties. The second model studies the effect of recipient factors on elaboration likelihood. Procedures for data analysis are outlined. The findings of the study can contribute in several ways. First, this study applies ELM to a domain not studied before i.e., elaboration likelihood of security messages. Second, the study addresses the lack of theoretically-grounded empirical studies to explain the influence of message properties and recipient factors on security attitude. Third, the study can offer practical suggestions on the design of persuasive security messages once it is empirically validated. Overall, it can provide a better understanding of how responsible security practices can be encouraged in current business environments where security is an important organizational concern.

References

Ajzen, I. (2001). Nature and operation of attitudes. Annual Review of Psychology, 52, 27-58.

Ajzen, I. (2002). Constructing a TpB Questionnaire: Conceptual and Methodological Considerations, September 2002 (Revised January 2006), accessed 1 November 2007, available at http://www.people.umass.edu/aizen/pdf/tpb.measurement.pdf

Ajzen, I., Brown, T.C., & Rosenthal, L.H. (1996). Information bias in contingent valuation: Effect of personal relevance, quality of information, and motivational orientation. Journal of Environmental Economics and Management, 30, 43-57.

Angst, C. M., & Agarwal, R. (2004). Central and peripheral routes to sustained technology usage. Proceedings of the Workshop of the Special Interest Group on Diffusion, Transfer, and Implementation of IT (DIGIT), Washington DC.

Areni, C.S., Ferrell, M.E., & Wilcox, J.B. (2000). The persuasive impact of reported group opinions on individuals low vs. high in need for cognition: Rationalization vs biased elaboration? Psychology and Marketing, 17(10), 855-875.

Bhattacherjee, A., & Sanford, C. (2006). Influence processes for information technology acceptance: an elaboration likelihood model. MIS Quarterly, (30:4), 805-825.

Cacioppo, J.T. and Petty, R.E. (1982). The need for cognition. Journal of Personality and Social Psychology, Vol. 42, No. 1, pp. 116-131.

Cacioppo, J.T., & Petty, R.E. (1984a). The elaboration likelihood model of persuasion. Advances in Consumer Research, 11(1), 673-675.

Cacioppo, J.T., Petty, R.E., & Kao, C.F. (1984b). The efficient assessment of need for cognition. Journal of Personality Assessment, 48(3), 306-307.

Celsi, R.L., & Olson, J.C. (1988). The role of involvement in attention and comprehension process. Journal of Consumer Research, 15, 210-224.

CERT (2007). Information for new and home users, accessed 5 September, 2007, available at http://www.cert.org/homeusers/

Chaiken, S. (1987). The heuristic model of persuasion. In M.P. Zanna, J.M. Olson, and C.P. Herman (Ed.), Social Influence: The Ontario Symposium. Hillsdale: Erlbaum, 3-39.

Chebat, J.C., Charlebois, M., & Gelinas-Chebat, C. (2001). What makes open vs. closed conclusion advertisements more persuasive? The moderating role of prior knowledge and involvement. Journal of Business Research, 53, 93-102.

Cohen, J., Cohen, P., West, S.G., & Aiken, L.S. (2003). Applied multiple regression/correlation analysis for the behavioral sciences (3rd ed). Mahwah, N.J.: L/ Erlbaum Associates.

DHS (2003). The national strategy to secure cyberspace, accessed 5 September, 2007, available at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

DHS (2007). Cyber security: make it a habit, accessed 5 September, 2007, available at http://www.dhs.gov/xprevprot/programs/gc_1158611596104.shtm

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 386-408.

Fornell, C., & Larcker, D.F. (1981). Evaluating structural equations with unobservable variables and measurement error. Journal of Marketing Research, 18, 39-50.

Hayes, F. (2003). Secure your users. Computerworld, 37(16), 50.

Jaccard, J., Turrisi, R., & Wan, C.K. (1990). Interaction effects in multiple regression. Series: Quantitative Applications in the Social Sciences, No. 72. Thousand Oaks, CA: Sage Publications.

Kankanhalli, A., Teo, H.H., Tan, B.C.Y., & Wei, K.K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23, 139-154.

Laroche, M., Cleveland, M., & Maravelakis, I. (2002). Attitude accessibility, certainty and the attitude-behavior relationship: an empirical study of ad repetition and competitive interference effects. International Journal of Advertising, 21, 149-174.

MacCallum, R.C., Zhang, S., Preacher, K.J., & Rucker, D.D. (2002). On the practice of dichotomization of quantitative variables. Psychological Methods, 7, 19-40.
Ng, B.Y., & Xu, Y. (2007). Studying users' computer security behavior using the health belief model. Proceedings of the Eleventh Pacific Asia Conference on Information Systems, Auckland, New Zealand.
Nunnally, J. (1978). Psychometric Theory, (2nd ed). New York: McGraw-Hill.
Peltier, T. R. (2005). Implementing an information security awareness program. Information Systems Security, 14(2), 37-49.
Petty, R.E., & Cacioppo, J.T. (1984a). Source factors and the elaboration likelihood model of persuasion. Advances in Consumer Research, 11(1), 668-670.
Petty, R.E., & Cacioppo, J.T. (1984b). The effects of involvement on responses to argument quantity and quality: central and peripheral routes to persuasion. Journal of Personality and Social Psychology, 46(1), 69-81.
Petty, R.E., & Cacioppo, J.T. (1986). Communication and Persuasion: Central and Peripheral Routes to Attitude Change. New York, NY: Springer-Verlag.
Petty, R.E., Cacioppo, J.T., & Goldman, R. (1981). Personal involvement as a determinant of argument-based persuasion. Journal of Personality and Social Psychology, 41(5), 847-855.
Petty, R.E., Cacioppo, J.T., & Shumann, D. (1983). Central and peripheral routes to advertising effectivenss: the moderating role of involvement. Journal of Consumer Research, 10(2), 135-146.
Petty, R.E., Harkins, S.G., & Williams, K.D. (1980). The effects of group diffusion of cognitive effort on attitudes: An information-processing view. Journal of Personality and Social Psychology, 38(1), 81-92.
Petty, R.E., & Wegener, D.T. (1999). The elaboration likelihood model: Current status and controversies. In S. Chaiken and Y. Trope (Ed.), Dual process theories in social psychology. New York: Guilford Press.
Pratt, M. K. (2006). Beyond posters. Computerworld, 40(16), 42-43.
Richardson, R. (2007). 2007 CSI/FBI Computer Crime and Security Survey, accessed 11 October, 2007, available at http://www.gocsi.com
Sasse, M.A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link": a human/computer interaction approach to usable and effective security. BT Technology Journal, 19, 122-131.
Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness. Information Management and Computer Security, 8(1), 31-41.
Somerson, I.S. (2003). Are security awareness programs undervalued? Security Management, 47(8), 158.
Straub, D.W. (1989). Validating instruments in MIS research. MIS Quarterly, 13(2), 147-169.
Straub, D., & Welke, R. (1998). Coping with systems risk: Security planning models for management decision-making. MIS Quarterly, 22(4), 441-469.
Sussman, S.W., & Siegal, W.S. (2003). Informational influence in organizations: An integrated approach to knowledge adoption. Information Systems Research, 14(1), 47-65.
Tam, K.Y., & Ho, S.Y. (2005). Web personalization as a persuasion strategy: an elaboration likelihood model perspective. Information Systems Research, 16(3), 271-291.
Thomson, M.E., & Solms, R.V. (1998). Information security awareness: Educating your users effectively. Information Management and Computer Security, 6(4), 167-173.
US-CERT (2007). Cyber security tips, accessed 5 September, 2007, available at http://www.uscert.gov/cas/tips/
Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program, accessed on August 11, 2006, available at http://csrc.nist.gov/publications/nistpubs/index.html.
Zaichkowsky, J.L. (1985). Measuring the Involvement Construct. Journal of Consumer Research, 12, 341-352.