2010

Analyzing The Adoption of Computer Security Utilizing The Health Belief Model

Chet L. Claar

Jeffrey Johnson

ANALYZING THE ADOPTION OF COMPUTER SECURITY UTILIZING THE HEALTH BELIEF MODEL

Chet L. Claar, Central Washington University, chet.claar@cwu.edu
Jeffrey Johnson, Utah State University, jeffrey.johnson@usu.edu

ABSTRACT

The home Internet user faces a hostile environment abundant in potential attacks on their computers. These attacks have been increasing at an alarming rate and cause damage to individuals and organizations regularly, and have the potential to cripple the critical infrastructures of entire countries. Recent research has determined that some individuals are not utilizing additional software protections available to mitigate these potential security risks. This paper seeks to further examine the reasons by proposing a conceptual framework that utilizes the Health Belief Model as a possible way to explain why some people do not perceive a threat sufficient to prompt the adoption of computer security software.

Keywords: Information Security, User Adoption, Health Belief Model (HBM).

INTRODUCTION

The phenomenal growth of the Internet has brought many new and exciting opportunities to the home computer user. Online shopping and banking, communication with friends and relatives, access to sources of information for research and homework, entertainment sources, up-to-the-minute weather and news, and countless other possible online activities have made the internet indispensible for most online-enabled households. However, while providing these new opportunities for home Internet users, it has also provided an opportunity-rich environment for criminals and others with malicious intent. They seek to exploit computer users who do not adequately protect themselves from the ever-increasing number of cyber threats. Using computer security solutions available in the form of anti-virus, anti-spyware, and firewall software in addition to ensuring that operating systems are properly updated provides effective protection from these online threats.

In June of 2009, the U.S. Census Bureau released the most recent statistics from a population survey collected November of 2007 [26]. The statistics show there are over 72 million households in the United States with Internet access. Considering that these households have at least one computer connected to the Internet, and sometimes more, this equates to at least 72 million potential targets for Internet-borne attacks.

Internet-borne attacks can take many forms. One form is email based attacks such as spam and phishing schemes designed to get users to reveal confidential data. Other attack types result in infections such as computer viruses designed to cause damage, Trojan Horses designed to create back doors or spread viruses or spyware, or computer worms designed to spread themselves as rapidly as possible creating network disruptions. These programs designed to compromise computers are collectively referred to as malware.

While some malware programs are designed to immediately cause noticeable interference with the normal operations of an infected computer, the more common and insidious type is spyware, which silently resides on the host machines to steal private data stored on the computer, or watch and report online activity looking for details about bank accounts, credit card numbers, and login and password information for a variety of exploitations.

Often these malware programs also initiate the host into a botnet, a network of similarly infected computers all under the control of an unknown individual called a botmaster. Either for their own agendas, or for rent, botmasters can use compromised computers, also called zombies to email spam, gather personal data, store and distribute illegal material, attack other computers and networks, or use them to launch attacks to cripple the critical infrastructures of nations such as power grids, telecommunications, commerce, or government services [28].

U.S. Strategic Command Chief General James E. Cartwright told Congress in March 2007 that "America is under widespread attack in cyberspace." During fiscal year 2007, the Department of Homeland Security received 37,000 reports of attempted breaches on government and private systems, which included 12,986 direct assaults on federal agencies and more than 80,000 attempted

attacks on Department of Defense computer network systems [24]. Most of these attacks are launched using zombie computers to mask the true source. Cyber criminals are continuing to refine their attack methods to remain undetected and to create global, cooperative networks to support the ongoing growth of criminal activity [22]. A study by MacAfee Avert Labs reported that in the first quarter of 2009 over 12 million new machines worldwide had been assimilated into botnets. That equates to an infection rate of 4 million new computers infected per month. The United States was responsible for 18% of all newly infected machines during that time. Overall, the United States accounts for 35% of all zombie machines under the control of spammers. This same study also reported that the number of unique viruses found in March 2009 was nearly double that found in any month in the previous year. This trend indicates that the threat continues to grow at an ever-increasing rate. [15]. According to Symantec Corporation, these patterns of attack will continue to increase as the financial payoff for compromising individual data increases [22].

The continued success of exploits is directly related to a failure of many computer users to adequately protect their systems with available computer security solutions. America Online and the National Cyber Security Alliance conducted a survey of Internet users in the United States in order to assess their level of security awareness and good practice [1]. Study participants were interviewed and then their computers were examined by computer specialists for common security issues. Based upon a sample of 329 homes, the study discovered several disturbing facts about security measures on respondent's computers.

The study revealed that approximately 75 percent of all respondents feel that their computer is very safe from online attacks or from viruses. Thus, 84 percent of respondents keep sensitive information on their computer and 72 percent use their computers for sensitive transactions. During the examination of the respondents' systems by computer specialists, it was revealed that 15% had no anti-virus software installed and that 67% had not updated it within the previous week. The study also revealed that 19% of these computers had an active viral infection, and that 63% had been the victims of a previous viral infection. The study also discovered that fully 67% of computers had no firewall software installed, and 72% with firewalls installed were not properly configured.

With the millions of households currently on the internet, the percentages of inadequately protected computers represented by the AOL/NCSA study equate to tens of millions of vulnerable computers in the United States that are potential victims, and attackers, in the online world of the Internet. With the possibility of these infected machines being used to disrupt or destroy critical infrastructures and disrupt vital services, the necessity of determining the factors involved in the adoption of computer security solutions becomes clear.

The behavioral antecedents of adoption and use of computer security solutions of home computer users is the focus of this research. The concept of perceived vulnerability in online activities would be an appropriate aspect to examine when trying to understand adoption and usage behavior for computer security solutions. Additionally, the severity of a security incident to the user would also be an important user perception to examine in an effort to better understand adoption behavior. Focusing this research on the individual home computer user will contribute to a better understanding of computer security adoption behavior. Also, it may reveal appropriate motivational methods to encourage home computer users to implement the necessary precautions.

The primary purpose of this research is to explore the factors that affect the adoption of computer security. Little research has been found in Information Systems adoption literature that adequately identifies the factors which affect computer security adoption. This research asserts that current models used in technology acceptance research do not adequately reflect the factors affecting acceptance and usage of computer security in the home environment.

CONCEPTUAL MODEL

The current predominant models in information systems used to examine user adoption and usage behavior are the Theory of Reasoned Action [11], the Theory of Planned Behavior [2], the Technology Acceptance Model [10], the Unified Theory of Acceptance and Usage of Technology [26], the Model of Adoption of Technology in Households [5], the Model of PC utilization [23], and the Innovation Diffusion Theory [18]. However, these MIS research models tend to focus on technologies that promote positive outcomes and offer the user some sort of utility. However, computer security software is classified as a protective technology, which is strictly

designed to avert negative outcomes and offers little obvious utility [9].

In an attempt to resolve the deficiency of MIS models adequate for security adoption, this study will examine the effectiveness of the constructs found in the Health Belief Model, a healthcare model from outside the information systems domain. While, it is common practice for MIS researchers to "borrow" from other fields, or "reference disciplines", this practice has been criticized [12]. In 1999, Eli Cohen said, "But reference disciplines are an excellent way for identifying pockets of research that are uncharted" [8]. However, in 1993, John King stated "Discipline is important for us, and obtaining it by reference is a perfectly sensible way for us to proceed, despite the inherently marginalizing consequence of our dependence on 'outside' versus 'inside' disciplinary traditions" [13]. Using the Health Belief Model may facilitate better determination of causal factors, or behavioral antecedents, which affect the acceptance, and usage of computer security software.

The Health Belief Model (HBM) is a psychological model that attempts to explain and predict health behaviors. This is done by focusing on the attitudes and beliefs of individuals. The HBM was first developed in the 1950s by social psychologists Hochbaum, Rosenstock and Kegels working in the U.S. Public Health Services. The model was developed in response to the failure of a free tuberculosis (TB) health-screening program. Since then, the HBM has been adapted to explore a variety of long- and short-term health behaviors. The HBM is based on the understanding that a person will take a health-related action if that person feels that a negative health condition can be avoided, has a positive expectation that by taking a recommended action, they will avoid a negative health condition, and believes that they can successfully take a recommended health action. [20].

The original HBM contained four core constructs representing the perceived threat and net benefits: perceived susceptibility, perceived severity, perceived benefits, and perceived barriers. These concepts were proposed as accounting for people's "readiness to act." An added concept, cues to action, would trigger that readiness and stimulate behavior [19, 20]. An addition to the HBM in 1988 by Rosenstock, Strecher, and Becker [21] is the concept of self-efficacy, which is one's confidence in the ability to successfully perform an action [3].

There are striking similarities in the beliefs and perceptions in protecting one's health and those involved in protecting one's computer from infection and attack. A stream of research in MIS is being conducted by various researchers [6, 14, 17, 27, 29, 30] examining this phenomenon using another health related model, the Protection Motivation Theory, which is an outgrowth of the HBM. Only one other study using the Health Belief Model has been found. It was published in 2009 by Ng, Kankanhalli, and Xu [16]. However, the model used in their study was modified from the original HBM as it did not include the modifying demographic variables proposed by Hochbaum et al. In contrast, we explore the behaviors of home computer users in relation to the security measures taken on their computers using the HBM as a reference, including relevant demographic variables as outlined by Rosenstock et al in 1988. The conceptual model can be found in figure 1 below.

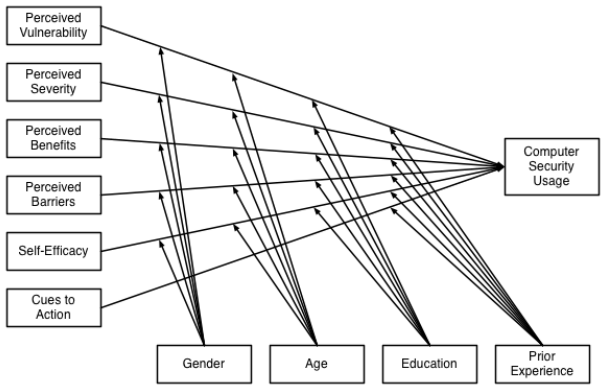

Figure 1. Research Model

Research Model Constructs

Perceived Vulnerability (VUL)

"Perceived susceptibility" is an individual's judgment of the risk of his or her computer contracting a particular security related issue. The construct has been renamed "Perceived Vulnerability" for the research model. This construct will be evaluated using questions designed to measure the respondent's belief about the chances of their computer becoming compromised due to various security threats. This leads to our first hypothesis for the model depicted in figure1.

H1 – Perceived Vulnerability to security incidents is positively related to computer

security usage.

Perceived Severity (SEV*)*

Perceived Severity corresponds to the original HBM construct, perceived seriousness. It is the individual's belief in the severity of the security compromise and its impact on lifestyle. This construct will be evaluated using questions designed to measure the respondent's belief about the seriousness of a particular compromise due to various security threats. Our hypothesis for this construct is as follows:

> H2 – Perceived severity of security incidents is positively related to computer security usage.

Perceived Benefits (BEN)

Perceived benefits of an action is the belief in the effectiveness of the actions required to prevent a security risk (or health risk in the original HBM). Questions for this construct will measure how strongly the individual believes the use of security precautions will protect their computer from security-related issues. Our hypothesis for this construct is as follows:

> H3 – Perceived benefits of practicing computer security are positively related to computer security usage.

Perceived Barriers (BAR)

The Perceived Barriers to Action construct is the individual's belief in the benefits compared to the perceived costs of action. It is designed to determine if there are perceived obstacles to adoption and usage of security software for home computers. Questions for this construct will include items for time cost, monetary cost, change in habits, and expected effort. Our hypothesis for this construct is as follows:

> H4 - Perceived barriers of practicing computer security are negatively related to computer security usage.

Self-Efficacy (SEF)

Self-efficacy is an individual's belief in his or her own ability to carry out a particular task. For this study it specifically relates to the belief that the individual can install, configure, and maintain the security software on their computer. Our hypothesis for this construct is as follows:

> H5 – Information Security Self-efficacy is positively related to computer security usage.

Cues to Action (CTA)

When a person is motivated and can perceive a beneficial action to take, actual change often occurs when some external or internal cue triggers action. The questions for this construct will assess likeliness to act based on media influence, social influence, computer exhibiting symptomatic behavior, and direct contact by OS vendor about new vulnerabilities. Our hypothesis for this construct is as follows:

> H6 - Cues to action are positively related to computer security usage.

Moderating Variables

The Health Belief Model theorizes that there is a moderated relationship between the above constructs and the dependent variable, Computer Security Usage by demographic and socio-psychological factors. This research will use the following moderators to determine the level of impact each may have on the relationship between the variables VUL, SEV, BEN, BAR, SEF and the dependent variable Computer Security Usage. In addition to the hypothesized demographic interactions, prior experience with computer security attacks and the moderating effects on the variables VUL, SEV, BEN, BAR, SEF, and CUE will be examined.

Gender (GEN)

> H7a-e - Gender significantly moderates the relationships of VUL, SEV, BEN, BAR, and SEF on Computer Security Usage.

Age (AGE)

> H8a-e - Age significantly moderates the relationships of VUL, SEV, BEN, BAR, and SEF on Computer Security Usage.

Education (EDU)

> H9a-e - Education significantly moderates the relationships of VUL, SEV, BEN, BAR, and SEF on Computer Security Usage.

Prior Experience (PXP)

> H10a-f - Prior Experience significantly

moderates the relationships of VUL, SEV, BEN, BAR, SEF, and CUE on Computer Security Usage.

Dependent Variable

Computer Security Usage (CSU)

This is the dependent variable of the study as depicted in figure 1. The measurement for this construct will be actual usage of computer security software. It will be assessed using questions to determine if the individual has anti-virus, firewall, and anti-spyware software installed and the level of usage.

RESEARCH DESIGN AND METHODOLOGY

This research will use an Internet-based survey to test the proposed model. The survey will use questions formulated by the researchers as well as those adapted from previous research [3] [8] [15]. The population of interest is all owners of a computer that connect to the Internet, and are at least partially responsible for the selection, installation, and maintenance of the software on their computers. A pilot study will be used to test the reliability and validity of the survey since adaptation of the original questions will be necessary for changes in context, and the addition of self-developed questions. The pilot study will be administered using a snowball collection starting with a convenience sample of university students. The pilot study data is currently being collected.

The main data collection will occur immediately following the analysis of the pilot data. The sampling method employed to recruit participants in this study will be a snowball sampling method. The sampling will be initiated through multiple participants recruited through university students, or study invitations posted on Internet newsgroups.

Data analysis will be conducted using Multiple Regression techniques to determine the significance of the relationships of the main predicting variables VUL, SEV, BEN, BAR, SEF and CUE on Computer Security Usage.
The regression model will also test the moderating relationships of GEN, AGE, EDU, and PXP on the main predictor variables.

CONCLUSIONS

This research aims to extend the body of knowledge relating to security adoption behavior by using a protective technology approach utilizing the Health Belief Model. This application of the Health Belief Model should provide new insights into the individual perceptions that lead to security adoption behavior. Should the proposed model, and specifically the constructs of Vulnerability and Severity prove to be significant predictors of usage behavior, this research can provide the foundations for a more comprehensive adoption model to be constructed. This research also may provide insights useful in designing methods to change incorrect perceptions in order to increase computer security usage behavior.

Limitations

This research uses anti-virus, firewall, and anti-spyware as measures of usage. This could result in a narrow scope that does not adequately capture all beliefs and behaviors relating to security such as email handling and password protocols. Self-reported usage also presents a potential bias issue with this research design.

REFERENCES

1. AOL and National Cyber Security Alliance (NCSA), (2005). AOL/NCSA Online Safety Study.
2. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*, 179-211.
3. Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84, 191-215.
4. Boss, S. (2007). Control, perceived risk and information security precautions: External and internal motivations for security behavior. Ph.D. dissertation, University of Pittsburgh, United States -- Pennsylvania. Retrieved September 27, 2009, from Dissertations & Theses: Full Text.(Publication No. AAT 3284534).
5. Brown, S.A., Venkatesh, V. (2005). Model of Adoption of Technology in Households: A Baseline Model Test and Extension Incorporating Household Life Cycle, *MIS Quarterly*, *29*(3), 399-426
6. Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of Protection Motivation Theory to Adoption of Protective Technologies, In *System sciences, 2009. HICSS 2007. 42nd annual hawaii international conference on.*

7. Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern Methods for Business Research, 295*, 336.
8. Cohen, E. (1999). Reconceptualizing Information Systems as a Field of the Transdiscipline Informing Science: From Ugly Duckling to Swan, *Journal of Computing and Information Technology. 7*(3), 213-219
9. Conklin, Wm. Arthur (2006). Computer security behaviors of home PC users: A diffusion of innovation approach. Ph.D. dissertation, The University of Texas at San Antonio, United States -- Texas. Retrieved September 27, 2009, from Dissertations & Theses: Full Text.(Publication No. AAT 3227760).
10. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13(*3), 319-340.
11. Fishbein, M. & Ajzen, I. (1975). Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Boston: Addison-Wesley.
12. Hassan, Nik R., (2008). Conceptual Development in IS: The Case of MISQ 1995-2004, *MWAIS 2008 Proceedings.* Paper 19.
13. King, J. L. (1993), "Editorial Notes," *Information Systems Research*, 4(4), pp. 291-298.
14. LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Commun. ACM*, *51*(3), 71-76.
15. McAfee Avert Labs, (2009). McAfee Threats Report: First Quarter 2009, Retrieved April 10, 2010, from http://resources.mcafee.com/content/AvertReportQ109
16. Ng, B. -Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.
17. Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on.*
18. Rogers, E.M., *Diffusion of Innovations*. Fifth ed. 2003, New York, New York, U.S.A.: The Free Press.
19. Rosenstock, I.M., (1966). Why people use health services, *The Milbank Memorial Fund Quarterly 44*(3)
20. Rosenstock, I. (1974). Historical Origins of the Health Belief Model. *Health Education Monographs.* Vol. 2 No. 4.
21. Rosenstock, I. M., Strecher, V. J., & Becker, M. H. (1988). Social learning theory and the health belief model. *Health Education & Behavior*, *15*(2), 175.
22. Symantec Corporation, (2007). Symantec Reports Rise in Data Theft, Data Leakage, and Targeted Attacks Leading to Hackers' Financial Gain. Retrieved April 10, 2010, from http://www.symantec.com/about/news/release/article.jsp?prid=20070319_01
23. Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: Toward a conceptual model of utilization. *MIS Quarterly, 15(*1), 131.
24. Tkacik Jr, J.J. (2007). Trojan dragons: China's international cyber warriors. *The Heritage Foundation.*
25. U.S. Census Bureau, (2007), Computer and Internet Use in the United States: October 2007, *Population Division, Education & Social Stratification Branch*
26. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27(*3), 425-478.
27. Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion: A first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on new security paradigms.*
28. Wilson, C. (2005). Computer attack and cyberterrorism: Vulnerabilities and policy issues for congress. *Federation of American Scientists, Washington DC.*
29. Woon, I. M.Y., Tan, G.W., and Low, R.T., "A Protection Motivation Theory Approach to Home Wireless Security," in *Proceedings of the Twenty-Sixth International Conference on Information Systems*, Las Vegas, Nevada, USA, 11-14 December, 2005
30. Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799-2816.