Identifying Multiple Categories of Cybersecurity Skills that Affect User Acceptance of Protective Information Technologies

Emergent Research Forum Papers

Dinesh S Reddy
The University of Texas at San Antonio
dinesh.reddy@utsa.edu

Glenn Dietrich
The University of Texas at San Antonio
Glenn.dietrich@utsa.edu

Abstract

Cybersecurity threat is one of the major national security challenges confronting the United States, making it imperative to achieve safe user security behavior on information systems. Safe user security behavior hinges on the attitude of a computer user to accept the usage of Protective information technologies (PIT), including security software. Past studies focused on user acceptance of PIT with antecedents such as usefulness, capabilities, and self-efficacy but rarely addressed specific cybersecurity skills needed to improve the user attitude and acceptance of security software use. The purpose of this study is to examine what category of cybersecurity skills can improve the user acceptance of PIT. We propose a theoretical model that examines the effect of cybersecurity computing skills, cybersecurity initiative skills and cybersecurity action skills on user attitude and acceptance of PIT. This research addresses the national cybersecurity threat and has both theoretical and practical implications.

Keywords

Protective information technologies, cybersecurity computing skills, initiative skills, action skills.

Introduction

Cybersecurity is one of the crucial functions to be considered when computers are involved. Cybersecurity can be compromised using "negative technologies such as computer viruses, spyware, and tools for breaking into systems and databases, which are designed to disrupt or harm their users. Protective information technologies (henceforth PIT) are designed to deter, neutralize, disable, or eliminate the negative technologies" (Dinev and Hu 2007:p387). Two out of top three security threats coming from Spyware (55%) and virus/worm (49%), are classified under negative technologies (CompTIA 2009). Although cybersecurity is promised by securing computers and networks using a combination of PIT such as firewalls, anti-virus software, anti-spyware software, the security can still succumb to human failure (Rhee et al. 2009). Thompson (2005) highlighted reasons why malicious software such as spyware can pose multiple threats to cybersecurity. Spyware harms computer performance by helping unauthorized users gain access to a computer in order to disclose private information. Spyware's primary means of gaining access is through accidental or careless activation of a worm or virus from an e-mail or a website download (Mattord and Whitman 2004). Also, a research analysis revealed that only 77% of the computers have security software running (PC_Pitstop 2010). These examples imply that security posture ultimately depends on end user attitude to promptly accept and use PIT such as security software. So, it is required to maximize the benefits offered by PIT in order to mitigate risks in a forced environment.

Prior studies have examined a few factors to acceptance of PIT. The studied factors include self-efficacy, perceived expense, perceived reliability (Yu et al. 2009), perceived ease of use, perceived usefulness (Shropshire et al. 2015; Wang 2010; Davis and Venkatesh 2004; Szajna 1994), technology awareness, controllability (Dinev & Hu 2007), cultural effects (Dinev et al. 2006, Dinev et al. 2009),

perceived vulnerability, perceived severity, perceived benefits, perceived barrier, cues to action (Claar and Johnson 2012; Claar et al. 2013). The most widely used contexts of PIT are anti-virus and anti-spyware.

As per technology acceptance model (henceforth TAM), the attitude towards the use of new technology further predicts it's user acceptance (Davis 1993). Consequently, it is imperative to understand the enhancement of user attitudes towards acceptance and usage of PIT in addition to deploying PIT to control and manage the ever-evolving cybersecurity threats (Dinev et al. 2009). There is a significant body of research supporting computer skills as a predictor of technology acceptance and use (Eg: Compeau et al. 1999). Extending this relationship to cybersecurity domain, cybersecurity skills (henceforth CS) can predict user attitude and acceptance of security software. In this article we categorize CS into multiple categories based on prior studies, with each category being either technical or non-technical.

The CS construct has not been categorized and examined as factors influencing user attitude and acceptance of PIT. Hence, the purpose of this article is to examine what categories of CS can improve the user attitude and acceptance of PIT. Accordingly, this article addresses two research questions: (1) Do multiple categories of CS influence the attitude and user acceptance of PIT? (2) What categories of CS are most needed by a computer user in order to improve the attitude and acceptance of PIT? Extending past literature on multiple categories of skills to cybersecurity domain and incorporating TAM constructs of attitude and acceptance, we present a research model and three associated propositions. This model can be empirically tested in future using surveys completed by home computer users.

The remaining part of the article is organized in the following manner. First, we present literature review on key concepts related to PIT, TAM, CS and its categories. Next, our research model is developed in support of three propositions. Finally, we conclude with a conclusion and future research.

Literature Review

Protective Information Technologies

Cybersecurity can be compromised by negative technologies such as computer viruses, spyware, and tools for breaking into systems and databases. Negative technologies harm the user's information stored on computers. "PIT are designed to deter, neutralize, disable, or eliminate the negative technologies or to reduce the effectiveness of such negative technologies" (Dinev and Hu 2007:p387). A few examples of PIT that 'home users' install and manage on their own systems include anti-spyware tools, anti-virus software, and firewalls. Computer users make effective use of PIT with voluntary and conscious involvement in safeguarding the computer against negative technologies by performing independent tasks such as installing, running and updating PIT such as anti-virus (Dinev & Hu 2007).

Hu and Dinev (2005) show that user behavior towards using PIT such as anti-spyware software is often determined by their motivation level in accurately performing the tasks offered by anti-spyware. The annoying factor that prevented user's motivation came from the fear of performing tasks on anti-spyware. Hu et al. (2006) found that while users know that security is important, they still don't view it as high priority since they get busy with other tasks. On some computers, anti-virus software may be 'turned off' as a requirement to use certain heavy graphical processes and applications (Dinev & Hu 2007). Such distinctive user attitudes towards using security software create a need to better understand the user attitudes towards acceptance and usage of PIT.

Cybersecurity Skills

End user computing skills form the foundation of CS, since an appropriate level of end user computing skill is needed to effectively learn and utilize the CS (Lerouge et al. 2005). End user computing skill is defined as "user's knowledge and ability to utilize computer hardware, software, and procedures to design, develop, and maintain specific applications for task-related activities. This definition includes skills related to the analysis of information requirements, evaluation of application features, and the ability to improve or modify input and output forms/screens." (Torkzadeh and Lee 2003:pg608). Extending this definition to cybersecurity domain, CS can be defined as the knowledge and ability to utilize security related features in specific applications such as anti-virus software. Studies show that user behavior towards using anti-spyware software is often determined by their motivation level in accurately performing the tasks offered by anti-spyware (Hu and Dinev (2005). This implies that computing skills

which are technical in nature, while necessary to perform security tasks, is not sufficient to improve the accuracy of performing security tasks. Hence we categorize the CS into both technical and non-technical skills. Accordingly, the categories of CS include cybersecurity computing skills (CCS), cybersecurity initiative skills (CIS) and cybersecurity action skills (CAS) (Choi et al. 2013).

Cybersecurity Computing Skills

CCS is defined as "the knowledge, experience and ability of users to use applications like antivirus software to protect computers and information systems" (Choi et al. 2013:pg4). Lerouge et al. (2005) studied the appropriateness of skill set of a systems analyst in order to effectively utilize and explore technology. They found the relevance between each skill dimensions and the role played in utilizing that skill. Extending to cybersecurity, we need relevant CCS in the form of technical security knowledge and experience in order to effectively utilize new innovations and functions in cybersecurity offered by PIT.

Cybersecurity Initiative Skills

CIS is defined as "the knowledge, experience and ability needed to seek out and take advantage of best security practices and security software like antivirus" (Choi et al. 2013:pg5). Rank et al., (2004) argue that there are three psychological processes namely initiative, creativity and innovation, which are required to achieve the desired outcome for any given role. Consistent to their argument, they define personal initiative as a proactivity concept that makes an individual a self-starter and highly motivated to put extra efforts at work irrespective of barriers. Larson (2000) takes a slightly different approach and talks about initiative in quantitative terms of ability to focus on a challenging task over a period of time from youth to adolescence. Dworkin et al., (2003) extends the initiative concept to skills acquired during the growth process involved in transition from youth to adolescence, and defines initiative skill as the capacity to spend effort and attention to achieve a challenging goal over time and to learn strategies for emotional stability by setting specific goals and managing time effectively to achieve those goals within a given timeframe. In cybersecurity context, we posit that CIS will self-motivate a computer user to proactively use and extract the benefits of PIT irrespective of obstacles created by lack of technical skills. CIS motivates a computer user to proactively make right decisions and seek out solutions to cyber threats.

Cybersecurity Action Skills

CAS is defined as "the ability, experience and knowledge to commit to objectives that meet security compliance" (Choi et al. 2013:pg6). Korukonda (1992) reviewed an exhaustive background on action skills in the context of managerial action skills where an action is something very practical in nature and should be result oriented. In the context of cybersecurity, Choi (2013) provides some examples of action such as managing security updates and antivirus software, or compliance with security policies and procedures. We posit that users with CAS should be result-oriented by enforcing a solution to a threat. Users with CAS will commit to making things work while using PIT. Users with CAS will adapt and get familiar to a specific PIT so that the usage gets better on every subsequent usage. CAS is gained by repeatedly performing the required steps on software, without actually knowing the technical details.

Research Model and Propositions

There is a whole body of literature that links computer skills to attitude and adoption of technology. The ability to learn a skill is closely related to increasing a person's efficiency and positive behavior (Carruth et al. 2010). Compeau and Higgins (1995) stated that a user's confidence in their computer skills results in better computer use. Skills closely relate to individual reactions to technology usage and adoption (Compeau et al. 1999). Skills are also shown to influence people's experience and attitude (Udo et al. 2010). Extending the same to CS, we derive three propositions that relate all three categories of CS to the user attitude and acceptance towards using PIT.

*Proposition1: Cybersecurity **c**omputing skill will have a significant positive effect on attitude and acceptance towards using protective information technologies.*

*Proposition2: Cybersecurity **i**nitiative skill will have a significant positive effect on attitude and acceptance towards using protective information technologies.*

Proposition3: Cybersecurity action Skill will have a significant positive effect on attitude and acceptance towards using protective information technologies.

As per TAM, we posit that a right attitude for using PIT implies improvement in user acceptance of PIT. So, a relationship between attitude and acceptance is not hypothesized in this article.

User acceptance is studied in different contexts of software such as internet banking (Wang et al. 2003), e-shopping (Shih 2003), Business Management (Hernandez 2008), and so on. In this article, we are extending user acceptance to the 'security' software context. Figure-1 shows proposed research model.

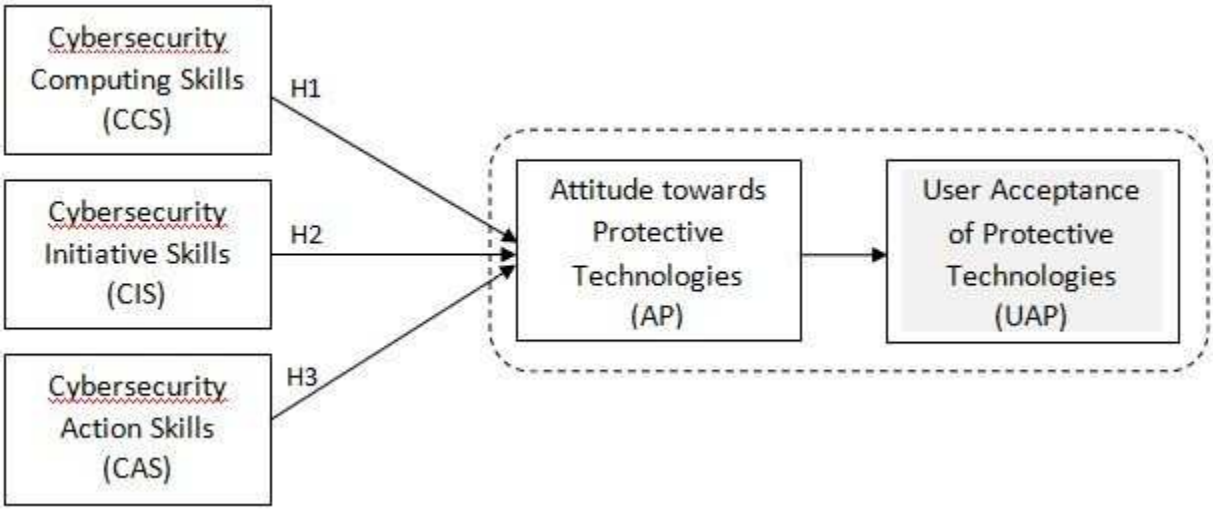

Figure -1 Research model

Conclusion

The purpose of this article is to examine the influence of multiple categories of CS on the user acceptance of PIT. Using TAM as a theoretical lens, we present a model where CCS, CIS and CAS are conceptualized as multiple categories of CS that influence the user acceptance of PIT. We present three propositions which can be empirically explored using surveys in future research, to demonstrate the need for categorization of CS, and that cybersecurity technical skills while necessary to perform security tasks, is not sufficient to improve attitude towards user acceptance of PIT. Once empirically validated, the research would suggest what categories of CS influence the user acceptance of PIT, thus opening up future research avenues in those categories.

REFERENCES

Choi, M. S., Levy, Y., & Hovav, A. (2013, December). The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and CS Influence on Computer Misuse. In *Proceedings of the pre-ICIS workshop on information security and privacy (WISP2013), Milan, Italy*.

Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems*, *52*(4), 20-29.

Claar, C. L., Shields, R. C., Rawlinson, D., & Lupton, R. (2013). COLLEGE STUDENT HOME COMPUTER SECURITY ADOPTION. *Issues in Information Systems*, *14*(2).

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS quarterly*, 189-211.

Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS quarterly*, 145-158.

CompTIA. (2009). (http://www.3coast.com/shocking-network-security-numbers/)

Davis, F. D. (1993). User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. *International journal of man-machine studies*, *38*(3), 475-487.

Davis, F. D., & Venkatesh, V. (2004). Toward preprototype user acceptance testing of new information systems: implications for software project management. *Engineering Management, IEEE Transactions on*, *51*(1), 31-46.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2006). User behavior toward preventive technologies-cultural differences between the United States and South Korea. In *ECIS* (pp. 1815-1826).
Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward PIT. *Journal of the Association for Information Systems*, *8*(7), 23.
Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards PIT: the role of national cultural differences.*Information Systems Journal*, *19*(4), 391-412.
Dworkin, J. B., Larson, R., & Hansen, D. (2003). Adolescents' accounts of growth experiences in youth activities. *Journal of youth and adolescence*,*32*(1), 17-26.
Hernandez, B., Jiménez, J., & Martín, M. J. (2008). Extending the technology acceptance model to include the IT decision-maker: A study of business management software. *Technovation*, *28*(3), 112-121.
Hu, Q., & Dinev, T. (2005). Is spyware an internet nuisance or public menace?.*Communications of the ACM*, *48*(8), 61-66.
Hu, Q., Hart, P., & Cooke, D. (2006, January). The role of external influences on organizational information security practices: an institutional perspective. In*System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on* (Vol. 6, pp. 127a-127a). IEEE.
Korukonda, A. 1992. "Managerial Action Skills in Business Education: Missing Link or Misplaced Emphasis?," Advanced Management Journal (57:3), pp. 27-35.
Larson, R. W. (2000). Toward a psychology of positive youth development.*American psychologist*, *55*(1), 170.
Lerouge, C., Newton, S., & Blanton, J. E. (2005). Exploring the systems analyst skill set: perceptions, preferences, age, and gender. *Journal of Computer Information Systems*, *45*(3).
Mattord, H. J., & Whitman, M. E. (2004). Principles of Information security.*Thomson Course Technology,[13] SITE.(nd),"The Search for International Terrorist Entities", http://www. siteinstitute. org/. Boston, MA, Appendix*, 326.
PC Pitstop. (2010). http://techtalk.pcpitstop.com/2010/05/13/the-state-of-pc-security/
Rank, J., Pace, V. L., & Frese, M. (2004). Three avenues for future research on creativity, innovation, and initiative. *Applied Psychology*, *53*(4), 518-528.
Rhee, H., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8), 816-826.
Shih, H. P. (2004). An empirical study on predicting user acceptance of e-shopping on the Web. *Information & Management*, *41*(3), 351-368.
Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior.*Computers & Security*, *49*, 177-191.
Szajna, B. (1994). Software evaluation and choice: Predictive validation of the technology acceptance instrument. *MIS quarterly*, 319-324.
Thompson, R. (2005). Threats to Security. *Communications of the ACM*, *48*(8), 41.
Torkzadeh, G., & Lee, J. (2003). Measures of perceived end-user computing skills. *Information & Management*, *40*(7), 607-615.
Udo, G. J., Bagchi, K. K., & Kirs, P. J. (2010). An assessment of customers'e-service quality perception, satisfaction and intention. *International Journal of Information Management*, *30*(6), 481-492.
Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, *46*(2), 186-204.
Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425-478.
Wang, Y. S., Wang, Y. M., Lin, H. H., & Tang, T. I. (2003). Determinants of user acceptance of Internet banking: an empirical study. *International Journal of Service Industry Management*, *14*(5), 501-519.
Wang, P. A. (2010, June). Information security knowledge and behavior: An adapted model of technology acceptance. In *Education Technology and Computer (ICETC), 2010 2nd International Conference on* (Vol. 2, pp. V2-364). IEEE.
Yu, C., Yao, Q., & Jie, L. (2009, September). An Empirical Study on Influence Factors of the Implementation of Using Genuine Software. In *Management and Service Science, 2009. MASS'09. International Conference on* (pp. 1-4). IEEE.