The Self-Efficacy Variable in Behavioral Information Security Research

Wu He, Ph.D.
Department of Information Technology & Decision Sciences
Old Dominion University
Norfolk, VA 23529
whe@odu.edu

Xiaohong Yuan, Ph.D.
Department of Computer Science
North Carolina A&T State University
Greensboro, NC 27411
xhyuan@ncat.edu

Xin Tian
Department of Information Technology & Decision Sciences
Old Dominion University
Norfolk, VA 23529
xtian@odu.edu

***Abstract*—There is a lack of consistent use of measurements for factors related to people's information security behavior. Specifically, a conceptually relaxed utilization of the variable "self-efficacy" makes it difficult for researchers to perform meaningful cross-study comparisons in behavioral information security research. This study examines how self-efficacy is defined and measured when used as a research variable in behavioral information security research and provides suggestions to better define and measure self-efficacy in behavioral information security research.**

Keywords-cybersecurity; inforamtion security behavior; self-efficacy; security policy;

I. BACKGROUND

Enterprises increasingly rely on information technologies for conducting various business activities. For example, more and more enterprises process business transactions on the Internet, or offer Internet-based services. The increased dependence on information technology such as Internet has led to a corresponding increase in the number of cybersecurity incidents and breaches in enterprises. In 2013, Target, the second-largest U.S. discount chain, was hit with a major data breach that exposed to hackers data on some 40 million credit and debit cards and personal data on another 70 million customers [1]. As a result, more and more enterprises become concerned about cybersecurity and hope to enhance the security of their enterprise systems, technologies and various applications to preserve the confidentiality, integrity and resource availability of computer systems so as to protect the information in these systems [2].

Studies show that the weakest link in a security chain is human. Although enterprises adopt numerous security technologies and solutions to protect their systems from security threats, that's still not adequate [3]. The success of enterprise security depends on the compliance of security policy of their employees who play an essential role in the prevention and detection of security incidents. However, getting employees to comply with enterprise security policy and practice good security behavior is not always easy since employees have different levels of security knowledge and motivations, and often exhibit different security behavior and attitudes when they use technologies [4]. For example, many employees fail to update their computers regularly, fail to act on malware alerts, or fail to protect their passwords.

Recent NSF "Secure and Trustworthy Cyberspace" program solicitation recognizes the importance of human behavior when designing, building and using cyber security technology. Studies show that incorporating an understanding of human behavior into cyber security products and processes can lead to more effective technology [5]. With the rapid development of emerging technologies such as Web 2.0, social media, mobile technology, virtual environment, online role-playing games, massive open online course (MOOC) systems, cloud computing and Internet of Things, better understanding of human behaviors with these emerging technologies is greatly needed.

II. ISSUES

Information security refers to the protection of information and the systems that use, store, and transmit information [6]. Most research on information security focuses on the technology part. Currently, there are only a few studies on people's information security behavior. As far as enterprise information security is concerned, there is even less research on enterprise employees' cyberseucirty behavior with emerging technologies. Thus, it is important to investigate the factors that influence enterprise employees' cybersecurity attitudes, motivation, knowledge and behavior in order to design more effective enterprise security policy and educational programs. We are particularly interested in what factors would motivate enterprise employees to practice good cybersecurity behavior. As a result, we conducted a literature review of behavioral information security research to identify the potential factors.

The literature review shows that factors such as computer experience, Internet experience, perceived vulnerability, perceived severity, response efficacy, response costs, self-efficacy, habit and peer behavior are important to a user's information security behavior [7,8,9,10].

While many researchers have accounted for these factors in their research designs, there appears to be low consistency in the operational measurements for some of the factors. Researchers often use different survey questions to

978-1-4799-5554-1/14 $31.00 © 2014 IEEE
DOI 10.1109/ES.2014.52

measure these factors [11]. There is a lack of consistent use of measurements for these factors to enhance communication among the researchers in the field of behavioral information security. For example, a conceptually relaxed utilization of the variable "self-efficacy" makes it difficult for researchers to perform meaningful cross-study comparisons, prevents researchers from building on the outcomes from the previous studies, and ultimately contributes to confusion or even conflicting findings about the impact of a user's self-efficacy on information security behavior.

As an initial step to facilitate future use of self-efficacy as a research variable, we conducted a comparative review of how this variable has been measured in a sample of 28 studies published in security behavior-related publications. We then provide suggestions to better define and measure self-efficacy in behavioral information security research.

III. METHOD

In an effort to study the variable self-efficacy in a systematic way, we conducted an extensive search using Google Scholar and multiple large-scale and reputable digital libraries and databases including Web of Science, IEEE Xplore, ScienceDirect (Elsevier), ACM Digital Library, Wiley Online Library, SpringerLINK and Emerald Management Xtra to find papers related to information security behavior research. These sources contain many high-quality journal articles and conference papers. As a result, we identified 28 highly relevant articles that reported empirical research on behavioral information security research with self-efficacy as a research variable.

Next, we did a content analysis of the articles, which provided data related to the measurement of variable "self-efficacy". We recorded the following descriptive information about individual studies that were reported in these articles: operational definitions of self-efficacy variable, the questions used to measure it, and the research findings pertinent to self-efficacy.

IV. FINDINGS

A. Definition

Ozer and Bandura [12] define self-efficacy as people's belief in their abilities to mobilize the motivation, cognitive resources, and courses of action needed to exercise control over given events. People with a high level of self-efficacy typically have a stronger form of self conviction about their ability to mobilize motivation, cognitive resources, and courses of action needed to successfully execute a task [13]. Self-efficacy affect peoples' motivation and action and influences the amount of effort, self regulation, and the initiation and persistence of coping efforts in the face of obstacles [14]. Bandura [15] found that people are more likely to engage in a certain activity when they believe that they are capable of succeeding in performing the activity. Their belief is related to their self confidence. Typically high self-efficacy tends to help people complete a task successfully, and on the contrary low self-efficacy tends to hinder their progress in completing a task.

We found that self-efficacy is defined differently by researchers in the context of information security and have different emphasis including information protection, information system security, computer security, security software and compliance with IS (information system) policy. For example, Rhee, Kim & Ryu [16] define self-efficacy in information security as a belief in one's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability. Ng, Kankanhalli & Xu [17] define self-efficacy as a user's self-confidence in his/her skills or ability in practicing computer security, which is likely to increase computer security behavior. Vance, Siponen & Pahnila [10] define self-efficacy as employees' belief that they can successfully comply with IS security policies, which should enhance compliance with policies and procedures. Claar & Johnson [18] define self-efficacy as the belief that the individual can install, configure, and maintain the security software on their computer.

A list of definitions of self-efficacy in the context of information security can be found in Appendix A. From this list, we can clearly see that there is some inconsistency regarding what self-efficacy in the context of security really means. Thus, there is a need for articles to contain detailed definitions of self-efficacy variables for readers to truly understand what it means or includes. We believe that the behavioral information security research community needs to address such inconsistency and clearly define what abilities security self-efficacy has to include because people often have varying confidence on their abilities with information protection, information system security, computer security, security software and compliance with IS (information system) policy. We think that a good definition should at least cover these aspects and need to differentiate self-efficacy in different areas, such as self-efficacy in understanding and complying with security policy, self-efficacy of using security software, and self-efficacy of behavior or performance in protecting information, computers or information systems from being compromised.

In addition, the number of people using mobile phones to access the Internet services such as emails and social media has grown exponentially in recent years [19, 20]. Unfortunately, the increasing popularity of mobile phones has also attracted the attention of virus and malware writers, hackers and other cybercriminals [21]. The mobile malware and virus are rapidly developing in recent years and have caused many incidents such as leaking of user privacy, financial and information loss, and identity theft [22, 23]. Thus, it is necessary to include mobile security into the security self-efficacy. Therefore, we synthesize various definitions in the literature and propose a definition for security self-efficacy as:

A user's self-confidence in his/her skills or ability in practicing computer, mobile devices and Internet security (e.g., install, configure, and maintain the security software on their computer or mobile devices), complying with information security policies, protecting information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability.

B. Measurement

Researchers also came up with different survey questions to measure self-efficacy in the context of information security. Appendix B lists a list of survey questions we identified from some articles. We can easily see the measurement inconsistency issues from these survey questions. Some of the survey questions are specific and some are generic. Researchers use different terminologies such as "information security precautions" and "preventative measures" in their measurements, which could be confusing to general users. We further evaluated the individual measures for conceptual similarity and grouped them into a few dimensions. As these articles typically don't include questions about mobile security or social media security, we feel that future measurements have to incorporate these questions as more and more people are using mobile phones and social media. Thus, we suggest adding them into the measurement dimensions too. Table I lists measurements of security self-efficacy grouped into various dimensions.

TABLE 1: MEASUREMENTS OF SECURITY SELF-EFFICACY GROUPED INTO DIMENSIONS

Dimension	Some Examples	Articles
Email security	I am confident of recognizing a suspicious email.	Ng, Kankanhalli & Xu [2]
Use of security software	I am able to use anti-spyware software without much effort.	Rhee, Kim & Ryu [16]; Johnston & Warkentin[22]
Computer security such as file backup, upgrading computer	I feel confident managing files in my computer. I feel confident updating security patches to the operating system.	Rhee, Kim & Ryu [16]
Browser security	I feel confident setting the Web browser to different security levels.	Rhee, Kim & Ryu [16]
Password security	I use strong and multiple passwords for different online accounts	Rhee, Kim & Ryu [16]; Johnston & Warkentin [22]
Internet security including social media security	I exercise caution when downloading files from the internet;	He [19]; Bhatti [23]
Security policy	I can comply with information security policies by myself.	Vance, Siponen & Pahnila [10]; Bulgurcu et al. [24]
Mobile security	I set up password on your phone; I install antivirus software in my smartphone	Shih, Lin, Chiang, & Shih[25]; He [26]
Learning security skills	I feel confident learning advanced skills to protect my information and information system.	Rhee, Kim & Ryu [16]; Thomson & von Solms [27]

C. Previous Research Findings Pertinent to Self-Efficacy

Most articles agree that self-efficacy is an important construct in determining individuals' information security practices. They found the impact of self-efficacy on different dependent variables such as intentions to practice information security, self-reported security behavior, attitudes towards information security policy, and use of security software and features. For example, Yoon, Hwang & Kim [28] found that self-efficacy has a strong impact on students' intentions to practice information security. Johnston & Warkentin [22] found that self-efficacy has a positive effect on end user intentions to adopt recommended individual computer security actions with respect to spyware. Ng, Kankanhalli & Xu [2] found that when perceived severity is high, self-efficacy becomes less important in determining one's decision to practice security.

V. CONCLUSION

The security behavior of employees plays an important role in maintaining the information security of enterprises. The importance of self-efficacy indicates the need for security training so that users are equipped with the right skills to practice the appropriate security behavior [2]. However, so far researchers have not used a consistent and systemic way to define and measure self-efficacy in the context of information security. Such inconsistency often contributes to confusion and misunderstanding about the impact of self-efficacy on information security behavior. In this paper, we analyze the definitions and measurements of self-efficacy in security-behavior related publications, and provide suggestions to better define and measure self-efficacy in behavior information security research.

VI. ACKNOWLEDGMENT

This work was supported in part by the U.S. National Science Foundation under Grant SES-1318470 and SES-1318501.

REFERENCES

[1] Vijayan, J. (2014). Major companies, like Target, often fail to act on malware alerts. Available at http://www.computerworld.com/s/article/9246942/Major_companies_like_Target_often_fail_to_act_on_malware_alerts

[2] Ng, B.Y., Kankanhalli, A. & Xu, Y. (2009). Studying users' computer security behavior using the health belief model. Decision Support Systems, 46(4), 815-825

[3] Rhodes, K. (2001). Operations Security Awareness: The Mind has No Firewall. Computer Security Journal, 18:3.

[4] Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. Computers in Human Behavior, Volume 26, Issue 6, Pages 1739-1747.

[5] Pfleeger, S.L. & Caputo, D. (2012).Leveraging behavioral science to mitigate cyber security risk. Computers & Security, 31(4), pp. 597-611.

[6] Whitman, M., & Mattord, H. (2011). Principles of information security. Cengage Learning.

[7] Hearth, T. & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organizations. European Journal of Information Systems, 18(2): 106-125.

[8] Mohamed, N. & Ahmad, I.(2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia.Computers in Human Behavior, 28 (2012), pp. 2366–2375
[9] Son, J.Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information & Management, 48(7), 296-302.
[10] Vance, A., Siponen, M., Pahnila, S. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49, pp. 190-198.
[11] Straub, D.W. (1989). Validating instruments in MIS research, MIS Quarterly 13 (2), pp. 147-169.
[12] Ozer, E. M., & Bandura, A. (1990). Mechanisms governing empowerment effects: a self-efficacy analysis. Journal of personality and social psychology, 58(3), 472-486.
[13] Stajkovic, A. D., & Luthans, F. (1998). Self-efficacy and work-related performance: A meta-analysis. Psychological bulletin, 124(2), 240-261.
[14] Bandura, A. (1986). The explanatory and predictive scope of self-efficacy theory. Journal of Social and Clinical Psychology, 4(3), 359-373.
[15] Bandura, A. (1989). Regulation of cognitive processes through perceived self efficacy. Development Psychology, 25, 729–735.
[16] Rhee, H. S., 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.
[17] Ng, B.Y., Kankanhalli, A. & Xu, Y. (2009). Studying users' computer security behavior using the health belief model. Decision Support Systems, 46(4), 815-825
[18] Claar, C., & Johnson, J. (2010). Analysing the adoption of computer security utilizing the health belief model. Issues in Information Systems, 4(1), 286-291.
[19] He, W. (2012). A Review of Social Media Security Risks and Mitigation Techniques. Journal of Systems and Information Technology, 14(2), 171-180.
[20] Mcafee (2012).2012 Threats Predictions. Available at http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2012.pdf
[21] Chiang, H.S., & Tsaur, W.J. (2011). Identifying Smartphone Malware Using Data Mining Technology. Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), pp.1-6.
[22] Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS quarterly, 34(3).
[23] Bhatti, B. (2012). Cyber Security and Privacy in the Age of Social Networks. In J. Zubairi, & A. Mahboob (Eds.), Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies (pp. 57-74). doi:10.4018/978-1-60960-851-4.ch004
[24] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS quarterly, 34(3).
[25] Shih, D., Lin, B., Chiang, H. & Shih, M. (2008). Security aspects of mobile phone virus: a critical survey. Industrial Management & Data Systems, Vol. 108 Iss: 4 pp. 478 – 494
[26] He, W. (2013). A Survey of Security Risks of Mobile Social Media through Blog Mining and an Extensive Literature Search. Information Management and Computer Security, 21(5), pp.381–400.
[27] Thomson, M.E. & von Solms, R. (1998). Information security awareness: educating your users effectively. Information Management & Computer Security, Vol. 6 Iss: 4, pp.167 – 173.
[28] Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring Factors That Influence Students' Behaviors in Information Security. Journal of Information Systems Education, 23(4).
[29] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.
[30] Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, 51(1), 69-79.
[31] Wang, J., Chen, R., Herath, T., & Rao, H. R. (2009). Visual e-mail authentication and identification services: An investigation of the effects on e-mail use. Decision Support Systems, 48(1), 92-102.
[32] 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.
[33] Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. Mis Quarterly, 34(3), 613-643.
[34] Lai, F., Li, D., & Hsieh, C. T. (2012). Fighting identity theft: The coping perspective. Decision Support Systems, 52(2), 353-363.

Appendix A: Definitions of Self-efficacy

Article	Definition
Rhee, Kim & Ryu [16]	Self-efficacy in information security (SEIS) as a belief in one's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability.
Ifinedo [29]	Self-efficacy emphasizes the individual's ability or judgment regarding his or her capabilities to cope with or perform the recommended behavior. In the context of this research, it refers to the sorts of skills and measures needed to protect the information in one's organizational IS (Bandura, 1977, 1991; Woon et al. 2005; Pahnila et al., 2007).
Ifinedo [30]	Self-efficacy fundamentally highlights the extent to which individuals feel and think about motivating themselves to completing specific tasks or actions.
Ng, Kankanhalli & Xu [2]	Self-efficacy refers to a user's self-confidence in his/her skills or ability in practicing computer security, which is likely to increase computer security behavior.
Vance, Siponen & Pahnila [10]	Self-efficacy in our study, refers to employees' belief that they can successfully comply with IS(Information System) security policies, which should enhance compliance with policies and procedures.
Wang et al. [31]	Computer (or technology) self-efficacy, which is the individual's belief in his/her capability to use the technology, reflects individual perceptions about his/her ability to apply technology skills to a task (or broader tasks).
Bulgurcu et al. [24]	Self-efficacy is an employee's judgment of personal skills, knowledge, or competency about fulfilling the requirements of the ISP (Information Security Policy).
Claar & Johnson [18]	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.

Appendix B: Measurements of Self-efficacy

Article	Measurements
Rhee, Kim & Ryu [16]	- I feel confident handling virus infected files. - I feel confident getting rid of spyware. - I feel confident understanding terms/words relating to information security. - I feel confident learning the method to protect my information and information system. - I feel confident managing files in my computer. - I feel confident setting the Web browser to different security levels. - I feel confident using different programs to protect my information and information system. - I feel confident learning advanced skills to protect my information and information system. - I feel confident getting help for problems related to my information security. - I feel confident using the user's guide when help is needed to protect my information and information system. - I feel confident updating security patches to the operating system.
Ifinedo [29]	- I have the necessary skills to protect myself from information security violations. - I have the expertise to implement preventative measures to stop people from getting my confidential information. - I have the skills to implement preventative measures to stop people from damaging my work computer. - I believe that it is within my control to protect myself from information security violations. - I can enable security measures on my work computer but only when I have manuals for reference. - For me, taking information security precautions is Hard . . . easy - My ability to prevent information security violations at my workplace is Inadequate…adequate.
Ifinedo [30]	- I have the necessary skills to protect myself from information security violations. - I have the expertise to implement preventative measures to stop people from getting my confidential information. - I have the skills to implement preventative measures to stop people from damaging my work computer. - It is easy for me to enable security features on my work computer by myself. - I can enable security measures on my work computer but only when I have manuals for reference. - For me, taking information security precautions. - My ability to prevent information security violations at my workplace
Ng, Kankanhalli & Xu [2]	- I am confident of recognizing a suspicious email. (agree/disagree) - I am confident of recognizing suspicious email headers. (agree/disagree) - I am confident of recognizing suspicious email attachment filename. (agree/disagree) - I can recognize a suspicious email attachment even if there was no one around to help me. (agree/disagree)
Vance, Siponen & Pahnila [10]	- I can comply with information security policies by myself. - Doing the opposite of what the [scenario character] did would be difficult for me to do. - Doing the opposite of what the [scenario character] did would be easy for me to do.
Son [9]	- How would you evaluate your computer knowledge skills in general? (1. no ability. . .7. very proficient).
Wang et al. [31]	- It is easy for me to verify an e-mail as coming from authentic sender based on "from line" and "subject line". - I feel comfortable in my abilities to identify e-mails that may be forged based on "from line" and "subject line". - I feel confident in my abilities to identify e-mails that are authentic based on "from line" and "subject line". - I feel confident in my abilities to determine whether the identities of e-mails are real based on "from line" and "subject line". - I feel comfortable in my abilities to identify e-mails that may be useful to me based on "from line" and "subject line". - I feel confident in my abilities to identify e-mails that are relevant to me based on "from line" and "subject line". - I feel confident in my abilities to identify malicious e-mails, such as phishing e-mails, based on "from line" and "subject line". - I feel confident in my abilities to identify e-mails that are detrimental based on "from line" and "subject line".
Workman, Bommer, & Straub [32]	- For me, taking information security precautions is: Hard . . . easy - I have the necessary skills to protect myself from information security violations: Disagree . . . agree - I have the skills to implement the available preventative measures to stop people from getting my confidential information: Disagree . . . agree - I have the skills to implement the available preventative measures to stop people from damaging my system: Disagree . . . agree - My skills required to stop information security violations are: Inadequate . . . adequate
Anderson & Agarwal [33]	- I feel comfortable taking measures to secure my primary home computer. - I feel comfortable taking security measures to limit the threat to other people and the Internet in general. - Taking the necessary security measures is entirely under my control. - I have the resources and the knowledge to take the necessary security measures. - Taking the necessary security measures is easy.
Bulgurcu et al. [24]	- I have the necessary skills to fulfill the requirements of the ISP. - I have the necessary knowledge to fulfill the requirements of the ISP. - I have the necessary competencies to fulfill the requirements of the ISP.
Johnston & Warkentin [22]	- Anti-spyware software is easy to use. - Anti-spyware software is convenient to use. - I am able to use anti-spyware software without much effort.
Yoon, Hwang & Kim [28]	- I am able to protect my personal information from external threats. - I am able to protect the data on my computer from being damaged by external threats. - I am capable of responding to malicious software such as viruses.
Lai, Li, & Hsieh [34]	- I am confident of my skills to handle a computer security issues. - I am confident of handling computer security issues even if there is no one around to show me how to do it. - I am confident of handling computer security issues even if I have never used such software and tools before. - I am confident of handling computer security issues after observing someone else us the software.