Subjective Norm and Measuring Its Impact on Information Security Behavioral Intention in Organizations.

Nooredin Etezady
etezady@gmail.com
College of Engineering and Computing
Nova Southeastern University
Ft. Lauderdale, FL 33314 USA

Abstract

Understanding employee's security behavior is required before effective security policies and training materials can be developed. Anti-virus software, secure systems design methods, information management standards, and information systems security policies have been developed and implemented. However, many organizations have not been successful in adopting these measures. Information systems research is encompassing social aspects of systems research more and more in order to explain user behavior and improve technology acceptance. Theory of planned behavior (TPB), which is an extension of the theory of reasoned action, considers intentions as cognitive antecedents of actions or behavior. Attitude, subjective norm, and perceived controllability are the three constructs on which TPB is based. Several studies have investigated subjective norm and its effect on information security. This study reviews various research on subjective norm and information security in order to obtain the most commonly used description for subjective norm in the area of information security. The most commonly used measures for subjective norm are also obtained from reviewing the existing research. Utilizing the commonly used subjective norm measures, it will be possible to develop a method to measure and influence employees' subjective norm positively with the goal of inducing positive information security behavior. Finally, a conceptual model for operationalizing the obtained subjective norm measures and enhancing information security in organizations is presented.

Keywords: information security, subjective norm, organizational security, Theory of Planned Behavior

1. INTRODUCTION

Anti-virus software, secure systems design methods, information management standards, and information systems security policies have been developed and implemented. However, many organizations have not been successful in adopting these measures (Li, He, Ivan, Xu, Anwar, & Yuan, 2014). Understanding employees' security behavior is required before effective security policies and training materials can be developed (Li et al.).

The information system users are primary contributors to the security of information systems (Shava & Van Greunen, 2013; Cheng, Li, Li, Holm, & Zhai, 2013). As users can be a threat to security, they can also be a valuable resource in building quality security efforts (Abraham, 2011). However, there is a gap in research on IS security from the socio-organizational perspective and human factors (Cheng, Li, Li, Holm, & Zhai, 2013).

The issues impacting use of security features by end users' needs further research as the number of security breaches caused by poor usage or no usage of security features is on the increase (Shava & Van Greunen, 2013).

It is important to know why individuals do certain practices and not others (Crossler & Belanger, 2014). The underlying reasons that individuals perform certain security tasks and not others should be understood. Crossler and Belanger pointed out that understanding the way people behave in a certain way could assist researchers in making recommendations for solutions that address the causes instead of the symptoms.

In order to motivate good security behavior, factors that affect security behavior need to be studied. Behavioral information security research indicates that subjective norm has significant effect on behavioral intention which greatly impacts intended behavior (Cox, 2012; Dinev, Hu, & Yayla,2009; Herath & Rao, 2009; Ifinedo, 2012; Ifinedo, 2014; Karahanna, Straub, & Chervany, 1999; Mussa & Cohen, 2013; Taylor & Todd, 1995; Venkatesh & Davis, 2000; Venkatesh, Morris, Davis, & Davis, 2003).

Several studies have investigated subjective norm and its effect on information security. However, there is no study that shows what the most commonly used description and measures are for subjective norm in the area of information security.

In order to operationalize the results of prior research with the goal of reducing security breaches, the most frequently used description and measures for subjective norm is needed. Having the most frequently used description and measure for subjective norm in the field of information security can be utilized to contribute to security management and control.

On the theoretical side having the knowledge of the most frequently used subjective norm description and measurements in information security will help researchers to investigate information security behavior in various dimensions such as the Internet use and teleworking.

This study draws on previous research on information security and subjective norm in order to obtain a common description for subjective norm. Then the measures used by existing research are compared in order to obtain the most commonly used measures for subjective norm. Upon obtaining the most commonly used subjective norm measures in information security, it will be possible for organizations to develop a method to measure and influence employees' subjective norm positively with the goal of inducing positive information security behavior. A conceptual model that illustrates how the findings from this paper can be utilized by organizations to improve their employees' security behavior is shown at the end (Figure 2).

2. LITERATURE REVIEW

Theory of reasoned action (TRA) introduced by Fishbein and Ajzen (1975) states that the attitude towards behavior and subjective norm explain behavioral intention. Attitude is described as positive or negative feelings about some object (Fishbein & Ajzen). Subjective norm is "the person's perception that most people who are important to him think he should or should not perform the behavior in question" (Fishbein & Ajzen, p. 302).

Theory of Planned Behavior (TPB), which is shown in Figure 1, was set forward by Ajzen(1985) and is an extension of TRA. Perceived behavioral control was added to the behavioral intention and the attitude towards behavior constructs in order to reflect one's belief of easiness or difficultness of performing a certain behavior (Hernandez & Mazzon, 2007).

Subjective norms are formed by normative beliefs (an individual's most important beliefs) on whether certain group of important people (such as peers, superiors, teachers, etc.) think that he/she should perform a behavior (Seyal & Turner, 2013). The study by Hazari, Hargrave, and Clenney (2008) indicated that attitudes, subjective norm, and perceived behavioral control impact information security awareness.

IT literature uses various labels such as normative commitment and social influence for subjective norm constructs. However, each of these constructs has the notion that that one's behavior is impacted by what important others expect one to do (Herath & Rao, 2009). In organizational setting the important others can be peers, co-workers, managers, and superiors.

Goo, Yim, and Kim (2014) define normative commitment as the perceived obligation or social pressure to behave according to an organization's expectations. "Normative commitment is a crucial trigger for individual's self-monitored and self-adjusted behaviors, which corrects an individual's security avoidance when recognizing a deviation from what others do with the security guidelines." (Goo, Yim, & Kim, 2014, P. 294). Normative commitment should be used to enhance employee's compliance intention to security policies rather than stopping security avoidance (Goo, Yim, & Kim).

Based on the Unified Theory of Acceptance and Use of Technology (UTAUT) by Venkatesh, Morris, Davis, and Davis (2003); Lewellen, Hooper, and Oliver (2014) further defined social influence as how much a person perceives that important others think he should use a new system. Social influence was defined as a broader term encompassing subjective norm, social factors, and image. Subjective norm, social factors, and image; each express the same explicit or implicit notion that an individual's behavior is influenced by his perception of how others view him in having used the technology (Lewellen, Hooper, & Oliver).

Empirical research findings indicate that subjective norm significantly influence behavioral intention (Cheng, Li, Li, Holm, & Zhai, 2013; Dinev, Hu, & Yayla,2009; Flores & Ekstedt, 2012; Karahanna, Straub, & Chervany, 1999; Mussa & Cohen, 2013; Taylor & Todd, 1995; Venkatesh & Davis, 2000; Venkatesh, Morris, Davis, & Davis, 2003). On the other hand, statistically insignificant relationship between subjective norm and behavioral intention have also been reported (Godlove, 2012; Mathieson, 1991; Pavlou & Fygenson, 2006).

Several researchers have inquired about common and concrete security measures (Herath, Herath, & Bremser, 2010; Lebek, Uffen, Breitner, Neumann, & Hohler, 2013; Lewellen, Hooper, & Oliver, 2014). Herath, Herath, and Bremser inquired about the common IT security measures. Lebek, Uffen, Breitner, Neumann, and Hohler deemed necessary concrete measures to affect employee's security awareness and behavior. Lewellen, Hooper, and Oliver noted the importance of having improved measures of the impacts of social norms and culture on technology adoption and use.

Although there are several studies that have investigated subjective norm and its effect on information security, there is no study that synthesizes the previous research in order to come up with the most commonly used description and measures for subjective norm in the area of information security. In this paper, 18 research studies from IS security behavioral publications on subjective norm were compared. Then suggestions were made for common description and measures of subjective norm in information security.

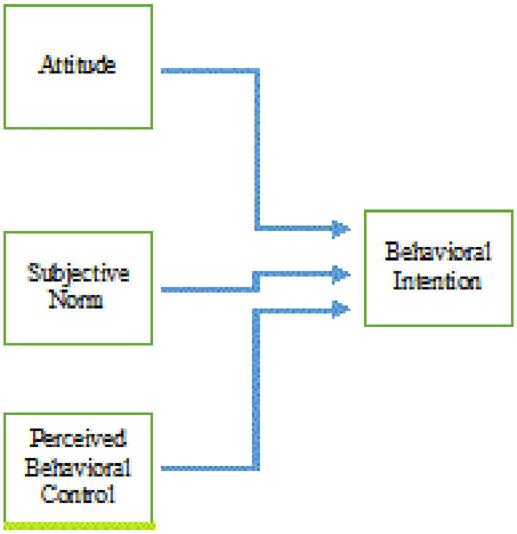

Figure 1. Theory of Planned Behavior

3. METHOD

The topic and title field tags in ACM, IEEE, EBSCO Host, ProQuest, Inspec (Thomson Reuters) and the searchable database fields title, author supplied keywords, and abstract in SpringerLink, and Wiley Online Library databases were searched for terms "information" "security" and "subjective norm". A total of 21 high quality articles were obtained. Three of the articles (Cox, 2012; Godlove, 2012; and Seymour & Nadasen, 2007) did not include description and measures for subjective norm. The remaining 18 articles were analyzed for the most commonly used subjective norm definition and measures.

4. FINDINGS

Description for subjective norm

Comparison of the descriptions for subjective norm from the reviewed research on subjective norms and information security indicates that the most common description used was the description originally set forth by Fishbein and Ajzen (1975), which is: "the person's perception that most people who are important to him think he should or should not perform the behavior in question". Subjective norm definitions that were found in the reviewed research are listed in Table 1.

Measurement

The review of the research on subjective norm and information security showed that they were performed in various dimensions. Among the research dimensions were: Internet security, IS security policy, handling sensitive information, and password management. Most of the survey questions that were used in various research studies were adapted from prior research. Table 2 contains all the subjective norm survey questions and the associated dimensions. After studying the questions in Table 2, some commonality was found among the questions with various dimensions. These common questions were then generalized and presented in Table 3. Therefore, Table 3 contains a list of various types of questions that were used in measuring subjective norm for information security. A conceptual model is provided in Figure 2 that shows how the measures shown in Table 3 can be utilized to assess subjective norm of employees of an organization. Training and education which is designed based on the employees the subjective norm assessment will enhance information security intention of employees. Employees subjective norm should be periodically assessed and the steps shown in Figure 2 repeated.

5. CONCLUSION

The information system users are primary contributors to the security of information systems (Shava & Van Greunen, 2013; Cheng, Li, Li, Holm, & Zhai, 2013). As users can be a threat to security, they also can be a valuable resource in building quality security efforts (Abraham, 2011).

In order to motivate good security behavior, factors that affect security behavior need to be studied. Behavioral information security research indicates that subjective norm has significant effect on behavioral intention which greatly impacts intended behavior (Cox, 2012; Dinev, Hu, & Yayla,2009; Herath & Rao, 2009; Ifinedo, 2012; Ifinedo, 2014; Karahanna, Straub, & Chervany, 1999; Mussa & Cohen, 2013; Taylor & Todd, 1995; Venkatesh & Davis, 2000; Venkatesh, Morris, Davis, & Davis, 2003).

Although there are several studies that have investigated subjective norm and its effect on information security, there was no study that synthesized the previous research in order to come up with the most commonly used description and measures for subjective norm in the area of information security. In order to operationalize the previous research findings with the goal of reducing security breaches, the most commonly used description and measures for subjective norm were needed. Having the most commonly used description and measures for subjective norm in the area of information security can be utilized to devise a method to manage and control information users' security behavior.

To obtain a common definition for subjective norm in the area of information security, 18 articles were reviewed. It was found that other terms (e.g., normative commitment and social influence) are interchangeably used for subjective norm. A common definition for subjective norm was obtained based on this review. A list of questions which were used to measure subjective norm were also identified (listed in table 3). A list of all questions with their survey dimensions are listed in Table 2, which can be used as a guideline by practitioners for survey design in order to assess subjective norm of their employees in their organization. A conceptual model was presented that shows how to operationalize the findings from this study (Figure 2).

From the research point of view, this paper offers the most commonly used definition and measures for subjective norm which could be used in future behavioral information security research. From the practical point of view, this research contributed to further understanding of information security, subjective norm, and its measures that can be used for managing security behavior in organizations.

The most commonly used definition for subjective norm and the questions used for measuring it can be used by information security professionals to design their own survey to measure the subjective norm in the area of information security for employees of an organization. Previous research has shown that subjective norm has a significant impact on employees' information security behavior. The result of the conducted survey in an organization can assist management in developing programs to measure and influence employees' subjective norm for information security and in managing information security more effectively.

This paper addressed only one factor, subjective norm, that affects behavioral intention. There are many other factors that affect behavioral intention, including attitude and perceived behavioral control, which were not discussed in this paper. It is hoped that other factors will be address by future research.

Future research will synthesize a common definition and measures for perceived behavioral control (Theory of Planned Behavior, Ajzen, 1985). Perceived behavioral control was added to the behavioral intention and the attitude towards behavior constructs in order to reflect one's belief of easiness or difficultness of performing a certain behavior (Hernandez & Mazzon, 2007).

This and future research attempts to define common definitions and measures for factors that previous research has indicated to have significant impact on information security behavior intention. These common definitions and measures can be used by various organizations to measure factors that contribute to users' information security behavior based on Theory of Planned Behavior, which may result in more effective management of organizational information security behavior.
The findings of this paper and the proposed conceptual model will also need to be empirically tested by future research.

6. REFERENCES

Abraham, S. (2011). Information security behavior: factors and research directions. *Proceedings of the seventeenth Americas Conference on Information Systems (2011)*, Paper 462, 1-13.

Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding and measuring information security culture. *Proceedings of the Pacific Asian Conference on Information Systems (PACIS 2012)*, paper 144.

Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly, 35*(2), 397-422.

Cheng, D., Han, J., & Song, Y. (2011). Is value sufficient? Empirical research on the impact of value and trust on intention*. Journal of Software, 6*(1), 124-131.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39*, 447-459.

Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in human behavior, 28*, 1849-1858.

Crossler, R., & Belanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *The Data Base for Advances in Information Systems, 45*(4), 51-71.

Das, S., Kramer, A. D. I., Dabbish, L. A., & Hong, J. I. (2013). Increasing security with social proof: a large-scale experimental confirmation. *Proceedings of the 21st ACM Conference on Computer and Communications Security (CS'14)*, 739-749.

Dauda, Y., Santhapparaj, A. S., Asirvatham, D., & Raman, M. (2007). The impact of E-Commerce security, and national environment on consumer adoption of Internet banking in Malaysia and Singapore. *Journal of Internet Banking & Commerce, 12*(2).

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.

Dinev, T., Hu, Q., & Yayla, A. (2009). Is there an on-line advertisers' dilemma? A study of click fraud in the pay-per-click model*. International Journal of Electronic Commerce, 13*(2), 29-59.

Dunkerley, K. , & Tejay, G. (2009). Developing an Information Systems Security Success Model for eGovernment Context. *Proceedings of the 15th Americas Conference on Information Systems (AMCIS)*, San Francisco, California.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley Pub. Co. Retrieved on 10/09/2015 from:

http://people.umass.edu/aizen/f&a1975.html

Flores, W. R., & Antonsen, E. (2013). The development of an instrument for assessing information security in organizations: Examining the content validity using quantitative methods. *Proceedings of the International Conference on Information Resources Management (CONF-RIM 2013)*, paper 44.

Flores, W. R., & Ekstedt, M. (2012). A model for investigating organizational impact on information security behavior. *Proceedings of the Seventh Pre-ICIS workshop on Information Security and Privacy (SIGSEC)*, 1-15.

Flores, W. R., & Korman, M. (2012). Conceptualization of constructs for shaping information security behavior: Towards a measurement instrument. *Proceedings of the Seventh Pre-ICIS workshop on Information Security and Privacy (SIGSEC)*, 1-14.

Godlove, T. (2012). Examination of the factors that influence teleworkers' willingness to comply with information security guidelines. *Information Security Journal: A Global Perspective, 21*, 216-229.

Goo, J., Yim, M.-S., & Kim, D. J. (2014). A path to successful management of employee security compliance: an empirical study of information security climate. *IEEE Transactions on Professional Communication, 57*(4), 286-308.

Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior*. Journal of Information Privacy & Security (Ivy League Publishing), 4*(4),3-20.

He, W., Yuan, X., Tian, X. (2014). The self-efficacy variable in behavioral information security research. *Proceedings of the 2014 Second International Conference on Enterprise Systems*, 28-32.

Herath, T., Herath, H., & Bremser, W. G., (2010). Balanced scorecard implementation of security strategies: A framework for IT security performance management. *Information Systems Management, 27*, 72-81.

Herath, T. & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*, 154-165.

Hernandez, J. M. C. & Mazzon, J. A. (2007). Adoption of internet banking: proposition and implementation of an integrated methodology approach. *International Journal of Bank Marketing, 25*(2), 72-88.

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*, 83-95.

Jenkins, J. L., Durcikova, A., & Burns, M. B. (2012). Forget the fluff: Examining how media influences the impact of information security training on secure behavior. *Proceedings of the 45th Hawaii International Conference on System Sciences*, 3288-3296.

Karahanna, E., Straub, D.W., & Chervany, N.L. (1999). Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly, 23*(2), 183–213.

Lankton, N. K., McKnight, D. H., & Thatcher, J. B. (2012). The moderating effects of privacy restrictiveness and experience on trusting beliefs and habit: an empirical test of intention to continue using a social networking website. *IEEE Transactions on Engineering Management, 59*(4), 654-665.

Lee, J. & Rao, H. R. (2012). Service source and channel choice in G2C service environments: a model comparison in the anti/counter-terrorism domain. *Information Systems Journal, 22*, 313-341.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature Review. *Proceedings of 2013 46th Hawaii International Conference on System Sciences*, 2978-2987.

Lewellen, M., Hooper, V., & Oliver, G. (2014). Unpacking the subjective norm: Applying structuration theory to traditional measures of social influence. *Proceedings of the 2014 Pacific Asia Conference on Information Systems (PACIS).*

Li, L., He, W., Ivan, A., Xu, L., Anwar, M., & Yuan, X. (2014). Does explicit information security policy affect employee's cyber security behavior? A pilot study. *Proceedings of the 2014 Second International Conference on Enterprise Systems*, 169-173.

Liao, Q., Luo, X., Gurung, A., & Li, L. (2009). Workplace management and employee misuse: Does punishment matter. *The Journal of Computer Information Systems, 50*(2), 49-59.

Lin, C., & Kunnathur, A. S. (2013). Toward developing a theory of end user information security competence. *Proceedings of the Americas Conference on Infomation Systems (AMCIS)*, 1-10

Mathieson, K. (1991). Predicting user intentions: Comparing the Technology Acceptance Model with the theory of planned behavior. *Information Systems Research, 2*(3), 173–191.

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information and Management Sciences Journal, 14*(2), 91-116.

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Sytems Research*, *2*(3), 192–222.

Mussa, C., & Cohen, M. (2013). Prudent access control behavioral intention: Instrument development and validation in a healthcare environment. *Proceedings of the Nineteenth Americas Conference on Information Sytems, Chicago, Illinois*, 1-11.

Pavlou, P.A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly, 30*(1), 115–143.

Seyal, A. H. & Turner, R. (2013). A study of executives' use of biometrics: an application of theory of planned behavior. *Behavior & Information Technology, 32*(12), 1242-1256.

Seymour, L., & Nadasen, K. (2007). Web access for IT staff: a developing world perspective on web abuse. *The Emerald Electronic Library, 25*(5), 543-557.

Sari, P. K., Candiwan, & Trianasari, N. (2014). Information security awareness measurement with confirmatory factor analysis. *Proceedings of the 2014 International Symposium on Technology Management and Emerging Technologies (ISTMET)*, 218-223.

Savola, R. M. (2012). Strategies for security measurement objective decomposition. *Proceedings of the 2012 Information Security for South Africa (ISSA)*, 1-8.

Shava, B. H., & Van Greunen, D. (2013). Factors affecting user experience with security features: A case study of an academic institution in Namibia. *Proceedings of the 2013 Information Security Conference for South Africa*, 1-8.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503-522.

Sun, J., Ahluwalia, P., & Koong, K. S. (2011). The more secure the better? A study of information security readiness. *Industrial Management & Data Systems, 111*(4), 570-588.

Takemura, T. (2011). Empirical analysis of behavior on information security. *2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing*, 358-363.

Taylor, S., & Todd, P.A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research, 6(3),* 144–176.

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal Computing: Toward a Conceptual Model of Utilization. *MIS Quarterly*, *15*(1), 125–143.

Uffen, J., Guhr, N., & Breitner, M. H. (2012). Personality traits and information security management: An empirical study of information security executives. *Proceedings of the International Conference on Information Systems (ICIS),*1-22.

Urbanska, M., Roberts, M., Ray, I., Howe, A., & Byrne, Z. (2013). Accepting the inevitable: Factoring user into home computer security.

Proceedings of the Third ACM Conference on Data and Application Security and Privacy (CODAPSY'13), 325-332.

Van Bruggen, D., Liu, S., Kajzer, M., Striegel, A., Crowell, C. R., & D'Arcy, J. (2013). Modifying Smartphone user locking behavior. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS) 2013*, 1-14.

Vekil, T., Solic, K., & Ocevcic, H. (2014). Development of users' information security awareness questionnaire (UISAQ) – Ongoing work. *Proceedings of the 37TH International Convention on Microelectronics (MIPRO) 2014*, 1417-1421.

Yoshikai, N. , Kurino, S., Komatsu, A., Takagi, D., Ueda, M., Inomata, A., & Numata, H. (2011). Experimental research on personal awareness and behavior for information security protection. *2011 International Conference on Network-Based Information Systems*, 213-220.

Young, R. F., & Windsor, J. (2010). Empirical evaluation of information security planning and integration. *Communications of the Association for Information Systems, 26*(13), 245-266.

Vaishnavi, V., & Kuechler, W. (2004). "Design Science Research in Information Systems", January 20, 2004; last update: October 23, 2013. Retrieved on 03/29/2015 from: http://www.desrist.org/design-research-in-information-systems/.

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*, *27*(3), 425–478.

Woon, I. M. Y., Kankanhalli, A. (2007). Investigation of IS professionals' intention to practice secure development of applications. *Int. J. Human-Computer Studies, 65*, 29-41.

APPENDIX

Subjective Norm Definitions	Research Paper
subjective norm is the perception of an individual regarding how people who are important in that individual's life would feel about certain behavior.	Cheng, Han, & Song (2011)
Subjective norms refer to the perceived social pressure to perform (or not perform) the behavior in question.	Cheng, Li, Li, Holm, & Zhai (2013).
Subjective norm refers to a person's perception that most people who are important to him or her think he or she should or should not perform the behavior in question.	Dauda, Santhapparaj, Asirvatham, Raman (2007)
Subjective norm is a person's perception of the social pressure to perform or not perform the behavior in question.	Dinev & Hu (2007).
One's perception of the social pressure to perform or not perform the behavior in question.	Dinev, Hu, & Yayla (2009).
Normative Commitment: The perceived obligation or social pressure to behave according to an organization's expectations.	Goo, Yim, & Kim (2014).
Subjective norm is the influence of others and social pressure that may lead to performing a behavior.	Hazari, Hargrave, & Clenney (2008)
Subjective norm is the belief as to whether or not a significant person wants the individual to perform the behavior in question.	Herath & Rao (2009)
Subjective norm is the "perception that most people who really matter to the individual think that he either should or should not perform the behavior in question"	Hernandez & Mazzon (2007).
Subjective norms describe an individual's perception of what people important to them think about a given behavior.	Ifinedo (2012)
Subjective norms describe an individual's perception of what people important to them think about a given behavior.	Ifinedo(2014)
Subjective norm: Perceptions that most important others think one should perform the behavior.	Lankton, McKnight, & Thatcher (2012).
No Description provided.	Lee & Rao (2012).
Subjective Norm: "the person's perception that most people who are important to him think he should or should not perform the behavior in questions." Social influence: "the degree to which an individual perceives that important others believe he or she should use the new system"	Lewellen, Hooper, & Oliver (2014).
Subjective norm reflects the perceived opinions of referent others. Normative belief is an individual's perception of a referent other's opinion about the individual's performance of a behavior. A referent other is a person or group whose beliefs may be important to an individual.	Liao, Luo, Gurung, & Li (2009).
Not provided.	Mussa & Cohen (2013).
Subjective norm is an individual's perception of whether most people important to that person think that he or she should or should not perform the behavior in question.	Seyal & Turner (2013).
Subjective norm refers to the perceived social pressure to perform or not perform the behavior.	Woon & Kankanhalli (2007)

Table 1. Subjective Norm Definitions

Dimension	Subjective Norm Measures	Research Paper
Online shopping – Security	. In my immediate social environment, the Internet is frequently used. . In my immediate social environment, attitudes toward Internet shopping are mainly positive. . In my immediate social environment, people have bought products or services over the Internet. . In my immediate social environment, people have bought products or services using the company’s interactive online system.	Cheng, Han, & Song (2011)
IS Security Policy	. My immediate supervisor believes that I shouldn’t violate the organization’s IS security policy. . My co-workers believe that I shouldn’t violate the organization’s IS security policy. . My organization believes that I shouldn’t violate the organization’s IS security policy. . My family believes that I shouldn’t violate the organization’s IS security policy.	Cheng, Li, Li, Holm, & Zhai (2013)
E-commerce security in Internet banking	Survey questions not provided.	Dauda, Santhapparaj, Asirvatham, Raman (2007)
User behavior toward protective technologies (information technologies that protect data and systems from disturbances such as viruses, unauthorized access, disruptions, spyware, and others)	. Most people who are important to me think it is a good idea to clean spyware from my computers. . Most people who are important to me think it is a good idea to prevent spyware from running on my computer.	Dinev & Hu (2007)
Online advertising	. People who are important to me think that our company should place ads on search engines. . People who are influential to me think that it is good for our company to place ads on search engines. . My peers in other companies think that it is a good idea to market goods and services through placing ads on search engines.	Dinev, Hu, & Yayla (2009)
Information Security Policy	. Top management thinks I should follow organizational IS security policies. . My boss thinks that I should follow organizational IS security policies. . My colleagues think that I should follow organizational security policies. . People who influence my behavior would think that I should follow organizational IS security policies. .People who are important to me would think that I should follow organizational IS security policies.	Goo, Yim, & Kim (2014)
Home computing security	. My friends/family would think highly of me if they knew I maintain security on my computer. . I recommend to my friends/family that they should use security programs on their computers. .When browsing the Internet I use security on my computer because I have heard from others it is the proper thing to do.	Hazari, Hargrave, & Clenney (2008)
IS security policies	. Top management thinks I should follow organizational IS security policies. . My boss thinks that I should follow organizational IS security policies. . My colleagues think that I should follow organizational IS security policies. .The information security department in my organization thinks that I should follow organizational IS security policies. . Computer technical specialists in the organization think that I should follow organizational security policies. .I believe other employees comply with the organization IS security policies. . I am convinced other employees comply with the organization IS security policies. .It is likely that the majority of other employees comply with the organization IS security policies to help protect organization's information systems.	Herath & Rao (2009)
Internet banking	Survey questions not provided.	Hernandez & Mazzon (2007)
Information Security Policy	. My boss thinks that I should follow the organization’s ISSP (IS Security Policy) . My colleagues think that I should follow the organization’s ISSP . My organization’s IT department pressures me to follow the organization’s ISSP . My subordinates think I should follow the organization’s ISSP	Ifinedo (2012)
Information Security Policy	. My boss thinks that I should follow the organization’s ISSP . My colleagues think that I should follow the organization’s ISSP . My subordinates think I should follow the organization’s ISSP	Ifinedo(2014)
Social networking Web site	.People who influence my behavior think that I should use MySNW.com. .People who are important to me think I should use MySNW.com .My friends think that I should use MySNW.com.	Lankton, McKnight, & Thatcher (2012)
E-government	. Most Americans will rely on the Web site of the FBI for information about the biochemical events. . Most Americans will use the Web site of the FBI to report the information.	Lee & Rao (2012)
Technology acceptance	Subjective Norm / Social Influence . People who influence my behavior think that I should use the system.	Lewellen, Hooper, &

	. People who are important to me think that I should use the system. . The senior management of this organization support the use of the system. . In general, the organization has supported the use of the system. . I use the system because many of my co-workers also use the system. . People in my organization who use the system are more highly regarded than those who do not. . People in my organization who use the system are more dependable than those who do not. . People in my organization who regularly use the system acquire a higher profile. . Using the system increases my chances of getting recognition in the workplace – e.g., contributes to promotion chances. . Placing my documents in the system – where other people may view them – may positively affect my reputation.	Oliver (2014)
Workplace Internet use	. If I committed Internet misuse, most of the people who are important to me would approve/disapprove. . Most people who are important to me would/would not look down on me if I committed Internet misuse. . No one who is important to me thinks it is/is not okay to commit Internet misuse.	Liao, Luo, Gurung, & Li (2009)
Access control in healthcare	**Items measuring TPB (Theory of Planned Behavior) construct for password management:** . People whose opinions I value would approve of me reusing my passwords. . People who are important to me would agree that keeping my passwords secret is good practice. . People who are important to me would agree that using strong passwords is good practice. **Items Measuring TPB Constructs for Careful Handling of Sensitive Information:** . People who influence my behavior would think that logging out of applications containing patient health or sensitive medical center information before leaving a computer/workstation is good practice. . People who are important to me would agree that following the medical center's guidelines regarding disposal of media (e.g., paper, flash drives, etc.) containing patient information is good practice. . People who influence my behavior would think that unauthorized disclosure of sensitive medical center information is not good practice.	Mussa & Cohen (2013)
Biometric user authentication in government	. People who are important to me encourage use of biometric. . People with whom I work with use biometric technology. . People who influence my behavior would think that I should use the biometric equipments. . People who are important to me would think that I should use the biometric technology.	Seyal & Turner (2013)
Secure development of applications	. People who influence my behavior think that I should practice SDA (Secure Development of Applications). . People who are important to me think that I should practice SDA. . People whose opinions I value prefer that I practice SDA.	Woon & Kankanhalli (2007)

Table 2. Subjective Norm Measures' dimensions

Common Subjective Norm Measures
. My immediate supervisor believes that I should /shouldn't ……. . Top management thinks that ……. . My boss thinks that ……. . My colleagues think that ……. . My co-workers believe that I should/shouldn't ……. . My organization believes that I should/shouldn't ……. . My peers in other companies think ……. . My subordinates think ……. . The information security department in my organization ……. . Computer technical specialists in the organization ……. . I believe other employees ……... . I am convinced other employees……. . It is likely that the majority of other employees …….
. People in my organization who perform ……. Are more highly regarded than those who do not. . People in my organization who perform ……. Are more dependable than those who do not. . People in my organization who regularly do ……. Acquire a higher profile. . Doing ……. Increases my chances of getting recognition in the workplace – e.g., contributes to promotion chances. . Doing ……. May positively affect my reputation.
. My family believes that I should/shouldn't ……. . My friends think that ……. . People who are important to me think ……. . People whose opinions I value ……. . People who are influential to me think ……. . I have heard from others that ……. . Most Americans will rely on or use …….

Table 3. Subjective Norm Measures

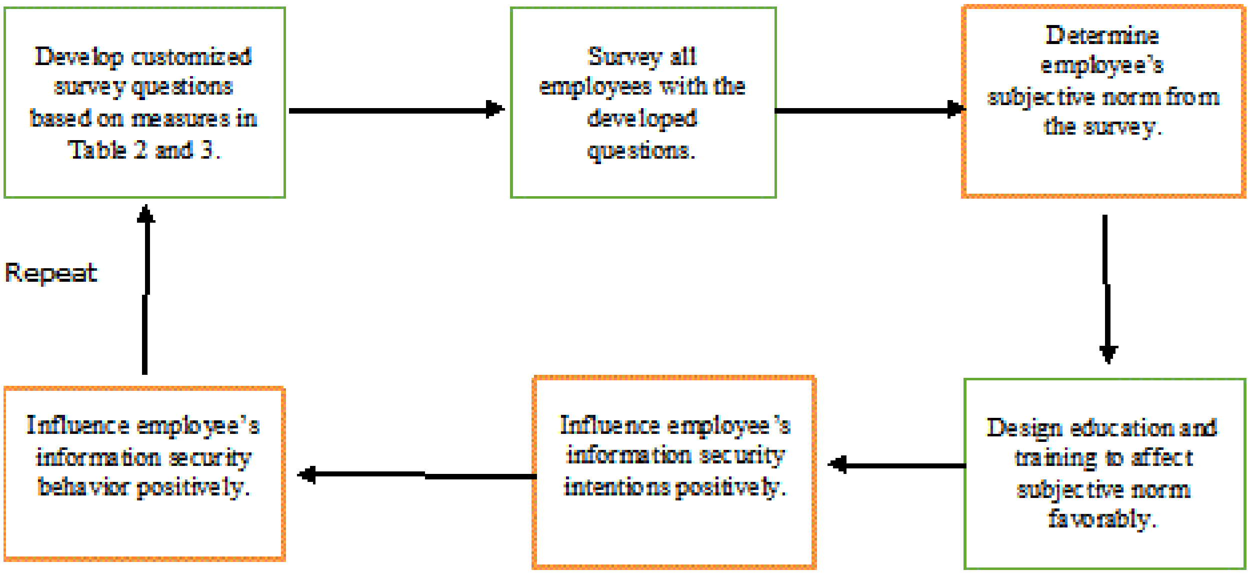
Develop customized survey questions based on measures in Table 2 and 3.
Survey all employees with the developed questions.
Determine employee's subjective norm from the survey.
Design education and training to affect subjective norm favorably.
Influence employee's information security intentions positively.
Influence employee's information security behavior positively.
Repeat

Figure 2. Conceptual model for applying Subjective Norm measures to induce positive employee behavior in organizations.