3-25-2017

A Common Description and Measures for Perceived Behavioral Control in Information Security for Organizations.

Noory Etezady
Nova Southeastern University, etezady@gmail.com

A COMMON DESCRIPTION AND MEASURES FOR PERCEIVED BEHAVIORAL CONTROL IN INFORMATION SECURITY FOR ORGANIZATIONS

Noory Etezady
Nova Southeastern University
etezady@gmail.com

ABSTRACT

Understanding employee's security behavior is required before effective security policies and training materials can be developed. The Anti-virus software, secure systems design methods, information management standards, and information systems security policies; which have been developed and implemented by many organizations; have not been successfully adopted. 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 based on Attitude, subjective norm, and perceived behavioral control (PBC) constructs, considers intentions as cognitive antecedents of actions or behavior. This study reviews various research on PBC and finds the most common measures for PBC, which can be used in organizations to develop a method to influence employees perceived behavioral control positively with the goal of inducing positive security behavior. Further, a conceptual model for operationalizing the obtained measures for enhancing information security in organizations is presented.

Keywords

Information Security, Theory of Planned Behavior, User Behavior, perceived behavioral control

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. Understanding employees' security behavior is required before effective security policies and training materials can be developed.

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

It is important to know why individuals do certain practices and not others. The underlying reasons that individuals perform certain security tasks and not others should be understood. 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. The theory of planned behavior has been validated in various information technology research. According to the theory of planned behavior, one factor that affects information security behavior is Perceived Behavioral Control (PBC). Behavioral information security research indicates that PBC has significant effect on behavioral intention, which greatly impacts intended behavior (Cox, 2012; Hazari, Hargrave, and Clenney, 2008; Hernandez and Mazzon, 2007; Hu, Dinev, Hart, and Cooke, 2012; Ifinedo, 2014; Lee and Rao, 2012; Liao, Luo, Gurung, and Li, 2009; Mussa and Cohen, 2013; Seyal and Turner, 2013; Zhang, Reithel, and Li, 2009). There are also some studies that show no significant impact from perceived behavioral control on intentions (Caldwell and McGarvey, 2013; Saeri, Ogilvie, La Macchia, Smith, and Louis, 2014).

Previous research has indicated positive impact from the three factors that contribute to intention and behavioral change from the theory of planned behavior. However, there is no research showing how to operationalize the results of prior research. In order to operationalize the results of prior research with the goal of reducing security breaches, a more frequently used description and measure for perceived behavioral control is needed.

Having the knowledge of the most frequently used perceived behavioral control description and measurements in information security will also 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 for organizations and perceived behavioral control in order to obtain a common description for perceived behavioral control. Then the measures used by existing research are compared in order to obtain the most commonly used measures. Upon obtaining the most commonly used perceived behavioral control in information security, it will be possible for organizations to develop a method to measure and influence employees' perceived behavioral control 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 1).

LITERATURE REVIEW

The four dominant behavioral theories are the theory of planned behavior, which states that intentions are cognitive antecedents of actions or behavior; general deterrence theory, which is based on rational decision making; protection motivation theory, which explains the coping process with potential threats through predicting a variety of protective behaviors; and technology acceptance model, which explains antecedents of technology acceptance through perceived usefulness and perceived ease of use. However, the theory of planned behavior has been validated by more research than the other ones (Lebek, Uffen, Breitner, Neumann, and Hohler, 2013).

Theory of Planned Behavior (TPB) was set forward by Ajzen(1985) and is an extension of Theory of reasoned action (TRA). 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. 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 and Ajzen, 1975, p. 302).

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 and Mazzon, 2007). TPB asserts that personal attitude, subjective norm, and perceived behavioral control form an individual's intention. When there is sufficient actual control over the behavior, intentions are carried out. Intentions are therefore antecedents of behavior when there is an opportunity (Ajzen, 2002). Application of TPB provides a series of information that helps in understanding behavior and implement interventions that will be effective in changing behavior (Ajzen, 2002). Aurigemma and Mattson (2015) noted that researchers have used TPB extensively in studying information security behavior of employees.

Perceived behavioral control "simply denotes subjective degree of control over performance of the behavior itself" (Ajzen, 2002, p. 4). It refers to the one's perception of one's ability to perform a given behavior. Higher perceived behavioral control reflects a greater belief that one can perform an action despite difficulties or easiness (Aurigemma and Mattson, 2015).

Perceived behavioral control reflects beliefs about self-efficacy and controllability according to TPB (Ajzen, 2002). Therefore, measures for perceived behavioral control need to have carefully selected items from both self-efficacy and controllability for high internal consistency (Ajzen, 2002). Having a measure of perceived behavioral control can contribute to predicting a behavior. Perceived behavioral control can be measured directly by asking questions about one's capability to perform a behavior or indirectly by asking about their believes to deal with the factors that help or inhibit performance of a behavior. Most studies have used the direct approach (Ajzen, 2002).

Self-efficacy reflects one's confidence in having the ability to perform a behavior. It deals with easiness or difficulty of performing a behavior. Whereas controllability indicates the extent which one believes one has power over performing a behavior. The majority of studies use measures of self-efficacy alone or a combination of self-efficacy and controllability items. Self-efficacy impacts intentions significantly. Controllability has a significant impact on predicting a behavior but not the intention. Empirical evidence indicates that perceived self-efficacy greatly differs from perceived controllability (Ajzen, 2002). Self-efficacy and controllability do not necessarily represent beliefs about either internal or external factors. They can consist of beliefs about both internal and external factors. As Ajzen noted, for some studies a single overall index of perceived behavioral control is needed and for some studies separate measures of self-efficacy and controllability is fitting. Similarity of perceived behavioral control and self-efficacy concepts has resulted in some researcher's employing of self-efficacy measures for perceived behavioral control (Aurigemma and Mattson, 2015).

Cox (2012) found that perceived behavioral control had significant impact on intended behavior. In Cox's study Locus of control (controllability) had no significant impact and self-efficacy had a significant impact on perceived behavioral control. Hazari et al. (2008) also found that perceived behavioral control (the confidence aspect) had a significant impact on behavioral

intention. Ifinedo (2014) found that perceived behavioral control in terms of both Self-efficacy and behavioral control had a significant effect on behavioral intention. However, measuring perceived behavioral control has been controversial (Dinev and Hu, 2007; Ajzen, 2002).

Some researchers have inquired about common and concrete security measures. Herath, Herath, and Bremser (2010) inquired about the common IT security measures. Concrete measures and processes are needed to affect employee's security awareness and behavior based on existing theoretical models.

Although there are several studies that have investigated perceived behavioral control 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 perceived behavioral control in the area of information security. In this paper 16 research studies from IS security behavioral publications on perceived behavioral control were compared. Then suggestions were made for a common description and measures of behavioral control.

METHOD

The topic, title, abstract, and author keyword fields in ACM, IEEE, EBSCO Host, ProQuest, Inspec (Thomson Reuters), SpringerLink, and Wiley Online Library databases were searched for terms "security", "perceived behavioral control", and "theory of planned behavior". A total of 16 high quality articles were obtained (table 1). These articles were analyzed to obtain the most commonly used definition for perceived behavioral control and its measurement.

Author(s)	**Paper Title**	**Dimension**
Aurigemma & Mattson, 2015)	The role of social status and controllability on employee intent to follow organizational information security requirements.	Compliance with Information Security Policy in a hierarchical organization
Chan, Ma, & Wong (2013)	The software piracy decision-making process of Chinese computer users.	Software Piracy, decision making process underlying software piracy.
Chu, Chau, & So (2015)	Explaining the misuse of information systems resources in the workplace: a dual-process approach.	Information Systems Misuse
Cox (2012)	Information systems user security: A structured model of the knowing-doing gap.	IS Security Policy For organizations with more than 500 employees.
Dauda, Santhapparaj, Asirvatham, Raman (2007)	The impact of E-Commerce security, and national environment on consumer adoption of Internet banking in Malaysia and Singapore.	E-commerce security in Internet banking
Dinev & Hu (2007)	The centrality of awareness in the formation of user behavioral intention toward protective information technologies.	User behavior toward protective technologies.
Godlove (2012)	Examination of the factors that influence teleworkers' willingness to comply with information security guidelines.	Teleworkers and compliance with information security guidelines
Hazari, Hargrave, & Clenney (2008)	An empirical investigation of factors influencing information security behavior.	Work related home computing users information security awareness
Hernandez & Mazzon (2007)	Adoption of internet banking: proposition and implementation of an integrated methodology approach.	Internet banking
Hu, Dinev, Hart, & Cooke (2012)	Managing employee compliance with information security policies: the critical role of top management and organizational culture.	Information Security Policy compliance
Ifinedo(2014)	Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition.	Information Security Policy violation
Lee & Rao (2012)	Service source and channel choice in G2C service environments: a model comparison in the anti/counter-terrorism domain.	E-government
Liao, Luo, Gurung, & Li (2009)	Workplace management and employee misuse: Does punishment matter.	Access control in healthcare
Mussa & Cohen (2013)	Prudent access control behavioral intention: Instrument development and validation in a healthcare environment.	Biometric user authentication in government
Seyal & Turner (2013)	A study of executives' use of biometrics: an application of theory of planned behavior.	Biometric authentication
Zhang, Reithel, & Li (2009)	Impact of perceived technical protection on security behaviors.	Security policies compliance

Table 1. Literature Review Summary

FINDINGS

Description for Perceived Behavioral Control

Comparison of the descriptions for perceived behavioral control in the area of information security indicated that the information systems research employed the same description provided by Ajzen. More than half (10 studies) of the studies either implied or directly used the description from (Ajzen, 2002). The remaining 6 studies used a definition for PBC which was based on Ajzen's definition. Therefore, the definition that was set forward by Ajzen(2002) is the most commonly used definition for PBC. This definition is: "perceived behavioral control refers generally to people's expectations regarding the degree to which they are capable of performing a given behavior, the extent to which they have the requisite resources and believe they can overcome whatever obstacles they may encounter (Ajzen, 2002, p.9)."

Measurement

The review of the information systems research on perceived behavioral control showed that they were performed in various dimensions. Among the research dimensions were: Internet banking, e-commerce security, e-government, software piracy, teleworking, and IS security policy.

As Ajzen (2002) noted, perceived behavioral control is usually assessed through self-efficacy and controllability. Self-efficacy refers to easy or difficulty of performing a behavior. Controllability refers to the degree that one perceives performance is up to the individual. This study found that 2 studies employed self-efficacy as a measure. 14 studies used measures for both self-efficacy and controllability. As Ajzen stated, the context of measurement should determine which component to measure.

Most of the survey questions that were used in various research studies were adapted from prior research. Table 2 contains a sample list of various types of questions that were used in measuring perceived behavioral control with the associated dimensions. Since measurement questions vary depending on the research context, a cookie cutter set of questions is not suggested. It will be left to the researcher or practitioner who is measuring PBC to select the closest dimension to the context of their study and modify it accordingly (The table containing all common measures for PBC and their various dimensions will be made available upon request). A conceptual model is provided in Figure 1 that shows how the measures can be utilized to assess perceived behavioral control (PBC) of employees of an organization. Training and education which is designed based on the employees assessed PBC will enhance information security intention of employees. Employees perceived behavioral control should be periodically assessed and the shown steps repeated.

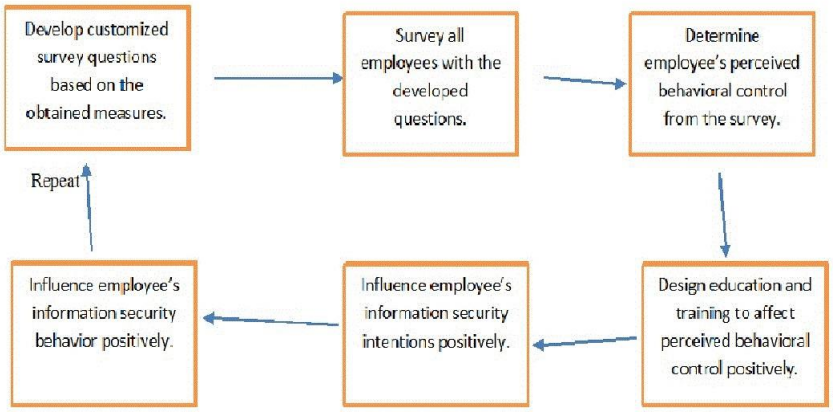

Figure 1. Conceptual model for applying PBC measures to induce positive employee behavior in organizations

Information Systems Misuse	**Measurement through self-efficacy and controllability** . I would be able to commit IS resource misuse. . Committing IS resource misuse is entirely within my control. . I have the resource and the knowledge and the ability to commit IS resource misuse.	Chu, Chau, & So (2015)
Information Security Policy compliance	**Measurement through self-efficacy and controllability** . I am able to follow the policies and procedures and use the security technologies. . I have the resources and knowledge to follow the policies and procedures and use the security technologies.	Hu, Dinev, Hart, & Cooke (2012)

	. I have adequate training and skills to follow the policies and procedures and use the security technologies.	
User behavior toward protective technologies (information technologies that protect data and systems from disturbances such as viruses, unauthorized access, disruptions, spyware, and others)	**Measurement through self-efficacy and controllability** **Perceived behavioral control:** . Please rate the difficulty for you to clean spyware from your computer using anti-spyware applications. (Extremely difficult – Extremely easy) . Please rate the difficulty for you to protect your computer from spyware. (Extremely difficult – Extremely easy) **Controllability:** . I have the skill and resources to clean spyware from my computer. . I have the skill and resources to protect my computer from spyware. .Whether or not to clean spyware from my computer is completely under my control. **Self-efficacy:** . I am confident that I can clean spyware off my system . I am confident I can prevent unauthorized intrusion to my computer. . I believe I can configure my computer to provide good protection from spyware.	Dinev & Hu (2007)

Table 2. Sample Perceived Behavioral Control Measures and their Dimensions

(The full table of PBC measures will be made available upon request)

CONCLUSION

The information system users are primary contributors to the security of information systems (Shava and Van Greunen, 2013). As users can be a threat to security, they also can be a valuable resource in building quality security efforts.

In order to motivate good security behavior, factors that affect security behavior needed to be studied. Behavioral information security research indicates that perceived behavioral control has significant effect on behavioral intention, which greatly impacts intended behavior.

Although there were several studies that investigated perceived behavioral control and its effect on information security, there was no study that synthesized the previous research in order to operationalize the findings of previous research. In order to operationalize the previous research findings with the goal of reducing security breaches, the most commonly used description and measures for perceived behavioral control were needed. Having the most commonly used description and measures for perceived behavioral control in the area of information security enables organizations to devise a method to manage and control information users' security behavior.

To obtain a consistent definition for perceived behavioral control, 16 high quality peer reviewed research articles were identified and reviewed. A consistent definition for perceived behavioral control was obtained based on this review. A list of questions which were used to measure perceived behavioral control was also identified. This list of questions with their associated survey dimensions can be used as a guideline by practitioners for survey design in order to measure perceived behavioral control in organizations. A conceptual model was presented that shows how to operationalize the findings from this study (Figure 1).

From the research point of view, this paper presents a consistent definition and gathered the common measures for perceived behavioral control in one place to be used in future empirical information security research. From the practical point of view, this research contributes to further understanding of perceived behavioral control and measures that can be used for managing security behavior in organizations.

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

This paper addressed only one factor, perceived behavioral control, that affects behavioral intention. There are many other factors that affect behavioral intention, including attitude and subjective norm, which were not addressed in this paper. It is hoped that other factors will be addressed by future research. Future research will attempt to provide a consistent definition and common measures for attitude. Future research also needs to empirically test the findings of this paper.

REFERENCES

1. Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckman (Eds.), *Action-control: From cognition to behavior*(pp. 11- 39). Heidelberg, Germany: Springer.

2. Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology, 32*, 665-683.
3. Aurigemma, S., & Mattson, T. (2015). The role of social status and controllability on employee intent to follow organizational information security requirements. *The proceedings of the 48th Hawaii International Conference on Systems Sciences*, 3527-3536.
4. Caldwell, A., & McGarvey, J. (2013). Modeling user behavior in response to cyberthreats. *Signals and Systems Conference (ISSC 2013)*, 1-7.
5. Chan, R. Y. K., Ma, K. H. Y., & Wong, Y. H. (2013). The software piracy decision-making process of Chinese computer users. *The Information Society, 29*, 203-218.
6. Chu, A. M. Y., Chau, P. Y. K., & So, M. K. P. (2015). Explaining the misuse of information systems resources in the workplace: a dual-process approach. *Journal of Business Ethics, 131*, 209-225.Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in human behavior, 28*, 1849-1858.
7. Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in human behavior, 28*, 1849-1858.
8. 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).
9. 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.
10. 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
11. 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.
12. 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.
13. 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.
14. 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.
15. Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: the critical role of top management and organizational culture. *Decision Sciences Journal, 43*(4), 615-659.
16. Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management, 51*, 69-79.
17. 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.
18. 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.
19. 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.
20. 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 Systems, Chicago, Illinois*, 1-11.
21. Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook users' online privacy protection: risk, trust, norm focus theory, and the theory of planned behavior. *The Journal of Social Psychology, 154*, 352-369.
22. 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.
23. 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.
24. Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*(4), 330-340.