Winter 12-13-2018

Investigation on Willingness of Employees to Share Information Security Advice

Sahar Farshadkhah
Louisiana Tech University

Michele Maasberg
Louisiana Tech University

T. Selwyn Ellis
Louisiana Tech University

Investigation on Willingness of Employees to Share Information Security Advice

Sahar Farshadkhah[1]
Department of CIS, Louisiana Tech University,
Ruston, LA, USA

Michele Maasberg
Department of CIS, Louisiana Tech University,
Ruston, LA, USA

T. Selwyn Ellis
Department of CIS, Louisiana Tech University,
Ruston, LA, USA

ABSTRACT

As modern organizations rely more on their information systems, mitigating information security risks becomes essential. Weaknesses in the information security management chain have continued to be challenged by employees. Therefore, enhancing employee security awareness becomes critical. Considering the effectiveness of informal methods, this research examines security advice sharing as one of the operative ways. Accordingly, in this paper, by adapting the theory of planned behavior as our theoretical lens, we propose a conceptual model of factors that are anticipated to impact the willingness of employees to share security advice. Finally, conclusion and avenues for future research are discussed.

Keywords: Advice sharing, information security, theory of planned behavior.

INTRODUCTION

In order to survive in a fast-paced business environment, organizations are more reliant than ever on Information Systems (IS). As their dependency on IS increases, ensuring that cybersecurity goals of confidentiality, integrity, and availability of these systems are met is paramount. Accordingly, the role of IS security to protect the data and strategic information of organizations becomes distinguished. Employees have been identified as the weakest links in

[1] Corresponding author. sfa005@latech.edu

organizations (Crossler et al. 2013), and therefore enhancement of employees' awareness regarding information security is crucial. Researchers and practitioners have recently found that informal security communication and people-centric workplaces have a significant impact on employees' awareness (Dang-Pham et al. 2017; Kirlappos et al. 2013). This informal communication is known as advice sharing.

Since modern organizations consider the 'comply or die' approach outdated (Kirlappos et al. 2013) and seek security through more flexible and efficient solutions, examining willingness of employees to share information security advice can be a new avenue in IS security literature. In the rest of the paper, we discuss current literature for advice sharing and propose our conceptual model with the justification of each construct. Finally, conclusion and avenues for future research are discussed.

THEORETICAL BACKGROUND AND CONCEPTUAL MODEL

In order to understand advice sharing relationships in the IS security context, we discuss the nature of advice sharing and its importance considering the theory of planned behavior (TPB) as our theoretical lens. We also discuss other factors that potentially have an impact on advice sharing relationships in organizations.

Advice Sharing

Advice sharing as an emerging topic in the behavioral security field can be referred to as a transitive and non-reciprocal (Dang-Pham et al. 2017b) relationship of the giving or taking of advice from another person (Flynn et al. 1996). This relationship can play a crucial role in developing people-centric security workplaces and there are numerous ways (e.g., engagement in daily activities) to encourage it among employees (Dang-Pham et al. 2017b).

Theory of Planned Behavior

Theory of planned behavior (TPB) is one of the most broadly used theories in behavioral security studies (Dang-Pham et al. 2017b). It surmises that individuals perform any action after they evaluate it as favorable (attitude), or there is some social pressure from their important referents (subjective norms), or there is a perception of control over behavior such as self-efficacy (behavioral control) (Ajzen 1991). Prior studies found that TPB's factors contribute to knowledge sharing in the organization (Safa and Von Solms 2016; Tohidinia and Mosakhani 2010).

Desire to Earn Reputation

Reputation is defined as the general judgment or opinions about a person and considered an extrinsic motivation that has a positive effect on employees' attitude toward information security knowledge sharing (Safa and Von Solms 2016). Since security awareness is important in modern organizations, individuals who have enough knowledge and confidence to give advice can be distinguished easily by their managers and colleagues. Therefore we propose:

P1: Desire to earn reputation is positively associated with individuals' attitude toward security advice-sharing intention.

Self-efficacy

Self-efficacy refers to an individual's judgment of his/her ability to perform given types of actions (Bandura 1997). As such, Ajzen (1991) cites compatibility of the concept of self-efficacy coincident with that of perceived behavioral control. Prior studies have empirically tested the impacts of self-efficacy on individual intentions and attitude. Tamjidyamcholo et al. (2013) confirmed that self-efficacy has a positive effect on knowledge sharing attitude. Since a higher level of self-efficacy in a person can raise their level of confidence in their abilities and

skills, attitudes toward sharing security advice with coworkers will likely emerge. Thus, we propose:

P2: Self-efficacy is positively associated with attitude toward security advice-sharing.

P3: Self-efficacy is positively associated with security advice-sharing intention.

Attitude of Security Advice Sharing

Attitude is a psychological tendency which can be negative or positive (Hepler 2015), and it has been considered by experts in many areas as a positional item to describe individuals' behavior (Safa and Von Solms 2016). The positive association between attitude and intention has been established through theory of planned behavior in a variety of different contexts. Results from prior empirical studies showed that attitude positively impacts an employee's intention toward knowledge sharing (Jeon et al. 2011), information security knowledge sharing (Bock et al. 2005; Safa and Von Solms 2016) and security advice sharing (Dang-Pham et al. 2017b). Therefore, we propose:

P4: Attitude toward security advice sharing is positively associated with security advice-sharing intention.

Perception of Security Climate

Campbell et al. (1970) described organizational climate as a set of specifications belonging to a particular organization that may be induced by its environment and the way its members perceive they are treated. Organizational climate can be considered a key mediator in the relationship between objective characteristics of working conditions and an individual's working behavior (Campbell et al. 1970; Chan et al. 2005). The effect of organizational climate on knowledge sharing has been widely studied (Bock et al. 2005; Buckman 1998; Connelly and Kelloway 2003; Constant et al. 1996; Huber 2001; Mcdermott 2001; Orlikowski 1992). Security

climate refers to the observable security environment that promotes the prioritization of security and compliance with security policies as one of the organization's goals (Dang-Pham et al. 2016). A positive security climate may help employees to understand their roles in information security management and increase their feelings of responsibility to information security (Goo et al. 2014). This definition of security climate in the context of this study is considered a proxy for subjective norm construct from the theory of Planned Behavior (Ajzen 1991). Subjective norms are defined by the perceived social pressure to perform or not perform a behavior and are positively associated with intention, and in a positive security climate social pressure for responsibility toward organizational security goals is inferred. Dang-Pham et al. (2016) demonstrated that an employee who perceives security practices more tends to share security advice or troubleshoot more often. Moreover, Goo et al. (2014) showed that creating a strong security climate limits the presence of security avoidance. Thus, we propose:

P5: Perception of security climate is positively associated with security advice-sharing intention.

Perceived Accountability

Accountability theory explains the enhancement of prosocial behaviors (Fandt and Ferris 1990). As accountability can be used to promote positive behaviors (Vance et al. 2015) and security advice sharing has been considered as an extra-role behavior in literature (Dang-Pham et al. 2017b), accountability is considered in this research as one of the motivations for voluntary security activities. Dang-Pham et al. (2016, 2017b) demonstrated that perceived accountability leads to security engagement and security advice sharing, and therefore we propose:

P6: Perceived accountability is positively associated with security advice-sharing intention.

Intention toward Security Advice Sharing

Intention can be considered a mental state which represents planning to achieve a goal or execute a particular action now or in the future (Lee 2014; Safa and Von Solms 2016). TPB predicts how individuals will behave based on their behavioral intentions (Ajzen 1991), and this relationship has been demonstrated in various contexts including information security policy compliance (Siponen et al. 2014) and intention to sharing information security knowledge (Safa and Von Solms 2016; Tamjidyamcholo et al. 2014). Based on TPB we examine this relationship in the context of security advice sharing and propose the following:

P7: Intention toward security advice sharing is positively associated with security advice sharing behavior.

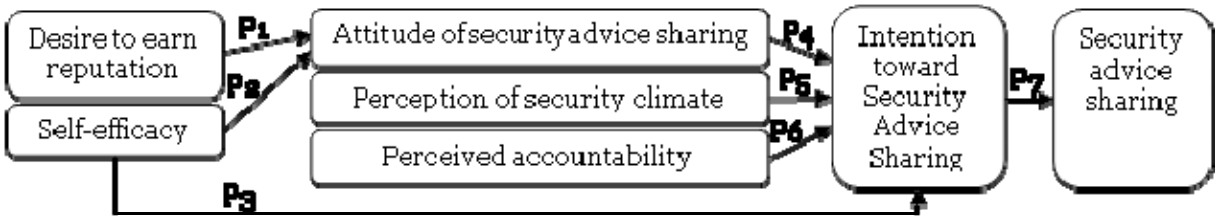

Figure 1. Proposed Conceptual Model

CONCLUSION AND FUTURE RESEARCH

In this paper, we proposed a conceptual model of the factors projected to have an effect on the willingness of employees to engage in the security advice sharing process. The conceptual model of this paper comprised of constructs surrounding the security advice-sharing relationship is derived from literature and theory, and therefore empirical research is needed. The planned empirical study involves survey methodology for data collection from a heterogeneous population of employees from at least one united states based organization with a full security management program where employees are aware of the issue-specific policies (for example,

acceptable use policy, internet use policy, etc.). Data analysis will be conducted using structural equation modeling (SEM). This research is expected theoretically to extend TPB with security advice sharing as it also considers the organizational security climate, accountability, and individual reputation. Practically, this research can provide knowledge that can help managers facilitate and increase the advice sharing process in their organizations and consequently achieve more information security awareness or compliance.

REFERENCES

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Bandura, A. 1997. *Self-Efficacy: The Exercise of Control*, Macmillan.

Bock, G.-W., Zmud, R. W., Kim, Y.-G., and Lee, J.-N. 2005. "Behavioral Intention Formation in Knowledge Sharing: Examining the Roles of Extrinsic Motivators, Social-Psychological Forces, and Organizational Climate," *MIS Quarterly* (29:1), pp. 87–111.

Buckman, R. H. 1998. "Knowledge Sharing at Buckman Labs," *The Journal of Business Strategy; Boston* (19:1), pp. 11–15.

Campbell, J. J., Dunnette, M. D., Lawler, E. E., and Weick, K. E. 1970. *Managerial Behavior, Performance, and Effectiveness*, Managerial Behavior, Performance, and Effectiveness, New York, NY, US: McGraw-Hill.

Chan, M., Woon, I., and Kankanhalli, A. 2005. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior," *Journal of Information Privacy & Security; Abingdon* (1:3), pp. 18–41.

Connelly, C. E., and Kelloway, E. K. 2003. "Predictors of Employees' Perceptions of Knowledge Sharing Cultures," *Leadership & Organization Development Journal*, pp. 294–301.

Constant, D., Sproull, L., and Kiesler, S. 1996. "The Kindness of Strangers: The Usefulness of Electronic Weak Ties for Technical Advice," *Organization Science* (7:2), pp. 119–135.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32), pp. 90–101.

Dang-Pham, D., Pittayachawan, S., and Bruno, V. 2016. "Impacts of Security Climate on Employees' Sharing of Security Advice and Troubleshooting: Empirical Networks," *Business Horizons* (59:6), pp. 571–584.

Dang-Pham, D., Pittayachawan, S., and Bruno, V. 2017a. "Why Employees Share Information Security Advice? Exploring the Contributing Factors and Structural Patterns of Security Advice Sharing in the Workplace," *Computers in Human Behavior* (67), pp. 196–206.

Dang-Pham, D., Pittayachawan, S., and Bruno, V. 2017b. "Exploring Behavioral Information Security Networks in an Organizational Context: An Empirical Case Study," *Journal of Information Security and Applications* (34), pp. 46–62.

Fandt, P. M., and Ferris, G. R. 1990. "The Management of Information and Impressions: When Employees Behave Opportunistically," *Organizational Behavior and Human Decision Processes* (45:1), pp. 140–158.

Flynn, L. R., Goldsmith, R. E., and Eastman, J. K. 1996. "Opinion Leaders and Opinion Seekers: Two New Measurment Scales," *Journal of the Academy of Marketing Science* (24:2), pp. 137–147.

Goo, J., Yim, M., and 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), pp. 286–308.

Hepler, J. 2015. "A Good Thing Isn't Always a Good Thing: Dispositional Attitudes Predict Non-Normative Judgments," *Personality and Individual Differences* (75), pp. 59–63.

Huber, G. P. 2001. "Transfer of Knowledge in Knowledge Management Systems: Unexplored Issues and Suggested Studies," *European Journal of Information Systems; Abingdon* (10:2), pp. 72–79.

Jeon, S., Kim, Y., and Koh, J. 2011. "An Integrative Model for Knowledge Sharing in Communities-of-practice," *Journal of Knowledge Management* (15:2), pp. 251–269.

Kirlappos, I., Beautement, A., and Sasse, M. A. 2013. "'Comply or Die' Is Dead: Long Live Security-Aware Principal Agents," in *International Conference on Financial Cryptography and Data Security*, Springer, pp. 70–82.

Lee, W.-K. 2014. "The Temporal Relationships among Habit, Intention and IS Uses," *Computers in Human Behavior* (32), pp. 54–60.

Mcdermott, R. 2001. "Overcoming Cultural Barriers," *Journal of Knowledge Management* (5:1), pp. 76–85.

Orlikowski, W. J. 1992. *"Learning from Notes: Organizational Issues in Groupware Implementation*, p. 9.

Safa, N. S., and Von Solms, R. 2016. "An Information Security Knowledge Sharing Model in Organizations," *Computers in Human Behavior* (57), pp. 442–451.

Siponen, M., Adam Mahmood, M., and Pahnila, S. 2014. "Employees' Adherence to Information Security Policies: An Exploratory Field Study," *Information & Management* (51:2), pp. 217–224.

Tamjidyamcholo, A., Bin Baba, M. S., Shuib, N. L. M., and Rohani, V. A. 2014. "Evaluation Model for Knowledge Sharing in Information Security Professional Virtual Community," *Computers & Security* (43), pp. 19–34.

Tamjidyamcholo, A., Bin Baba, M. S., Tamjid, H., and Gholipour, R. 2013. "Information Security – Professional Perceptions of Knowledge-Sharing Intention under Self-Efficacy, Trust, Reciprocity, and Shared-Language," *Computers & Education* (68), pp. 223–232.

Tohidinia, Z., and Mosakhani, M. 2010. "Knowledge Sharing Behaviour and Its Predictors," *Industrial Management & Data Systems* (110:4), pp. 611–631.

Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing Accountability through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations. MIS Quarterly, 39(2), 345–366.