DECISION SCIENCES INSTITUTE
The merits of information security awareness program: a longitudinal study

Xiaofeng Chen
Western Washington University
Email: chenx@wwu.edu

ABSTRACT

Information Security Policy (ISP) plays an important role in information security management in organizations. Past research investigated various factors that may impact employee behavior toward security policy compliance. The results of prior studies are inconclusive. One of the reasons for the inconsistent results may be that the information security awareness (ISA) was not thoroughly investigated in the research models. All prior studies used snapshot data. The aim of this study is to investigate using longitudinal data how ISA influences different constructs that play a critical role in affecting employee's behavior of ISP compliance.

KEYWORDS: Information Security Policy, SETA, Longitudinal Study

INTRODUCTION

Research shows that a security policy is an essential part of an information security management (ISM) program (Sommestad et al. 2014) and the weakest link of an ISM program is the one that involves human element (e.g., Bulgurcu et al. 2010). What influence employee's ISP compliance behavior has drawn extensive research using various theories from criminology and human behavior, such as the theory of reasoned action (e.g., Bulgurcu et al. 2010), the theory of planned behavior (TPB) (e.g., Bulgurcu et al. 2010), protection and motivation theory (PMT) (e.g., Herath and Rao 2009; Johnston and Warkentin 2010), and general deterrence theory (GDT) (e.g., D'Arcy and Devaraj 2012, Straub and Welke 1998). Although the prior research has solid theoretical foundation, the results are mixed and inconclusive. For example, according to GDT and PMT, fear appeal should have a significant impact on employee ISP compliance; however, prior empirical study results revealed conflicting results. Some research shows that fear of penalties does influence ISP compliance (e.g., D'Arcy et al. 2014; Johnston and Warkentin 2010], whereas others show that a penalty is an insignificant factor in ISP compliance (e.g. Jacobs 2010].

One of the possible reasons for the mixed results may be that the research models missed one of the critical influential factors. There is a lack of research on the effect of user awareness and training of security policy on security compliance. Conceptually the importance of ISA has been suggested (D'Arcy et al. 2009; Furnell et al. 2002; Siponen 2000, 2001). Bulgurcu et al. (2010) started the empirical investigation of the role of ISA on employee's ISP compliance behavior. Their study shows the direct influence of ISA on an employee's attitude toward compliance as well as the relationship between ISA and an employee's outcome beliefs. As acknowledged in their research, the correlation between ISA and employee's ISP compliance intention can't be inferred as a causal relationship.

Bulgurcu et al. (2010) indicated that a longitudinal study is needed to unveil the causal relationship between ISA and employee's ISP compliance intention and behavior. We follow Bulgurcu et al. (2010)'s suggestion and continue on the empirical investigation of the role of ISA on employee's ISP compliance behavior. To the best of our knowledge, this study is the only one that attempted to investigate the causal relationship.

In this study, we use the awareness-motivation-capability (AMC) model to further elaborate on why ISA is important in understanding employee's ISP compliance behavior. We conducted two surveys that are two years apart to introduce the time dimension into the empirical study so that it is possible to investigate the causal relationship between ISA and employee's ISP compliance behavior. If the causal relationship can be established, it can help change the perspectives of how information security management should be conducted. For example, in addition to invest in security hardware and software, more attention of information security managers may need to be placed on awareness and training programs. These programs cannot be treated as something that can be placed on the back burner because their critical effects on motivating and empowering employees to comply with the policies. Furthermore, we expect the research findings may help shift the research direction of information security more toward, as started recently by other researchers (e.g. D'Arcy et al. 2014; Hsu et al. 2015; Johnston et al. 2015), how to build a security culture and using informal and social influences to protect information assets.

In sum, this study continues our prior research (Chen et al. 2016) of security policy compliance from a new perspective. We employed the AMC framework to understand personal actions in MIS research. We believe that the three action drivers outlined by AMC not only influence an organization's decision to act, but also shape individual decisions and behavior.

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Effect of Security education, training, and awareness (SETA) program on information security awareness (ISA)

Information security awareness includes awareness of ISP and awareness of general security importance (Bulgurcu et al. 2010). SETA was proposed to be one of the countermeasures to reduce user's IS misuse (D'Arcy et al. 2009). Bulgurcu et al. (2010) also suggested that SETA program is an important part of any information security management program. We argue that SETA program is important because it can improve employee's ISA, which is a critical driver for employee's ISP compliance behavior. We propose:

H_1: SETA is one of the causes for employee's ISA

Effect of awareness on ISP compliance intention

In our prior study (Chen et al. 2016), we argue that the contrary findings of the effects of various factors derived from PMT, DT, or RCT on ISP compliance may be due to low employee awareness of the information security policy. Siponen (2000) proposed that security awareness is the most important factor in influencing employees to change their compliance actions. Empirical results supported the significant correlation between awareness component and employee's ISP compliance intention and action (Bulgurcu et al. 2010; Chen et al. 2016). With the time dimension introduced in this study, we posit that there is a causal relationship between awareness and employee's ISP compliance intention.

We propose our first hypothesis:

H_2: Awareness of the importance of information security is one of the causes for employee's intention to comply with their organization's ISP.

Effect of motivation on ISP compliance intention

Chen et al. (2016) justified the importance of employee's motivation on their ISP compliance intention. However, their empirical evidences do not support the hypothesis. We speculate that the unsupported hypothesis may be due to the lack of the awareness of ISP. With improved awareness through education and training, the motivation driver may play critical role in employee's ISP compliance behavior. Accordingly, our second set of hypotheses regarding employee intentions to comply with their organization's ISP are:

H_3: Motivation is one of the causes for employee's intention to comply with their organization's ISP.

Effect of capability on ISP compliance intention

Based on the AMC framework, Chen et al. (2016) also theorized that employees' capability to comply significantly influences their intention to comply with their ISP. Their empirical evidence supports the theory. With the time dimension introduced in this study, we hypothesize:

H_4: Capability is one of the causes for employee's intention to comply with their organization's ISP.

Effect of awareness of information security on motivation and capability to comply with ISP

Chen et al. (2016) proposed that to be motivated to take an action, an individual needs to be aware of what is expected from him/her and the importance of the action and its results. Therefore, the awareness driver of AMC framework should have a direct influence on the motivation driver of an action. Their empirical results support the

proposal. We also argue that the awareness of organizational ISP can influence employees' capability to comply simple because organizational ISPs include the guidelines of what employees need to do in certain circumstances. With the awareness of what they are expected to do, employees may have the knowledge of what they need to do ahead of time, therefore, change their perceptions of their self-efficacy and controllability to comply with their organization's ISP. As a result, we propose that, in the ISP compliance context:

H_5: Awareness of the importance of information security is one of the causes for employee's motivation to comply with their organization's ISP.

***H_6: Awareness of the importance of information security is one of the causes for employee's capability to comply with their organization's ISP*.**

Our research model is pictured in Figure 1.

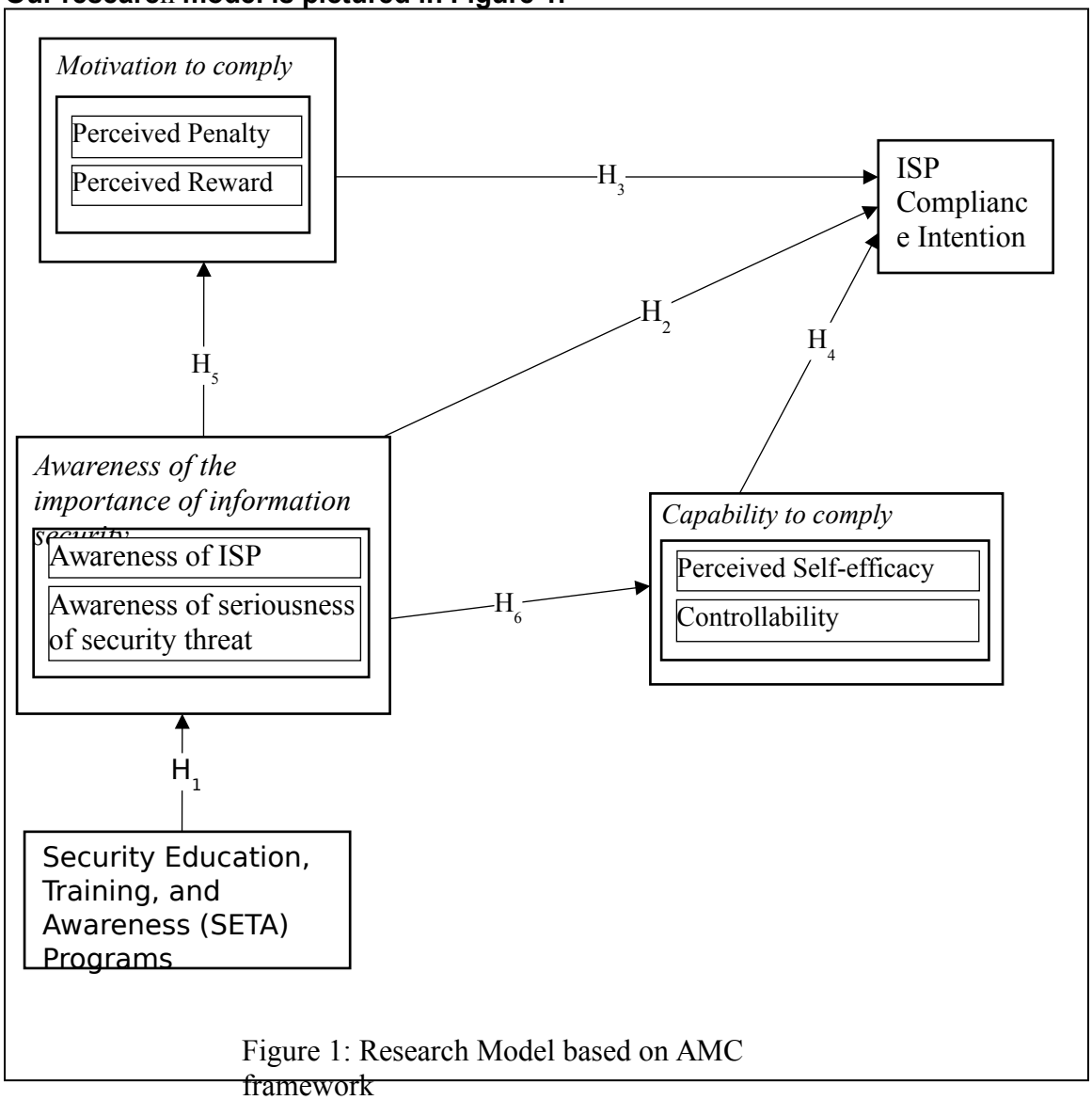

Figure 1: Research Model based on AMC framework

RESEARCH METHOD

The survey is a main approach in the literature investigating ISP compliance behaviors [e.g., 13, 26]. However, the majority of the research uses cross-sectional data, which can't infer the causal relationships among the factors. Bulgurcu et al. (2010) recommended a future study that collects data across time by surveying the same individuals at different time instances for causation. This study is a continuation of our prior study (Chen et al. 2016). The data for this study will be collected two years after the data was collected for our prior study (Chen et al. 2016). With the introduction of the time dimension, we want to investigate if there is a causal relationship between the action drivers and the employee's ISP compliance behavior.

Participants and data collection

The participants of this study are employees of a mid-size regional university in the northwest of the USA. The office of the CIO of the university approved our request to conduct an online survey regarding employee ISP compliance intentions. We used Qualtrics.com to host both surveys that are two years apart. Both surveys lasted for four weeks with three email invitations sent to the employees of the university: the first email invitation was sent on the first day of the first week of the quarter to all university employees; two follow-up email invitations were sent one week apart. The survey was closed at the end of the fourth week.

References

Bulgurcu, B., Cavusoglu, H, and Benbasat, I "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* 34(3), 2010, pp. 523-548.

Chen, X., Chen, L., and Wu, D. "Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective," Journal of Computer Information Systems (forth coming), 2016, available electronically at http://dx.doi.org/10.1080/08874417.2016.1258679.

D'Arcy, J. and Devaraj, S. "Employee misuse of information technology resources: testing a contemporary deterrence model," *Decision Sciences* (43:6), 2012, pp. 1091-1124.

D'Arcy, J., Herath, T., and Shos, M.K. "Understanding employee responses to stressful information security requirements: a coping perspective," *Journal of Management Information Systems* 31(2), 2014, pp. 285-318.

D'Arcy, J., Hovav, A., and Galletta, D. "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information Systems Research* 20(1), 2009, pp. 79-98.

Furnell, S. M., Gennatou, M., and Dowland, P. S. "A Prototype Tool for Information Security Awareness and Training," Logistics Information Management (15:5), 2002, pp. 352-357.

Herath, T. and Rao, H.R. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* 18(2), 2009, pp. 91-109.

Hsu, J. (S.C.), Shih, S.P., Hung, Y.W., Lowry, P.B. "The role of extra-role behaviors and social controls in information security policy effectiveness," *Information Systems Research* 26(2), 2015, pp. 282-300.

Jacobs, B.A. "Deterrence and deterrability," Criminology, (48:2), 2010, 417-441.

Johnston, A. and Warkentin, M. "Fear appeals and information security behaviors: an empirical study," MIS Quarterly 34(3), 2010, pp. 549-566.

Johnston, A.C., Warkentin, M., and Siponen, M. "An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric," MIS Quarterly (39:1), 2015, 13-134.

Siponen, M. T. "A Conceptual Foundation for Organizational Information Security Awareness," Information Management and Computer Security (8:1), 2000, pp. 31-41.

Siponen, M. T. "Five Dimensions of Information Security Awareness," Computers and Society (31:2), 2001, pp. 24-29.

Sommestad, T. Hallberg, J., Lundholm, K., and Bengtsson, J. "Variables influencing information security policy compliance," *Information Management & Computer Security* 22(1), 2014, pp. 42-75.

Appendix A: Survey Instrument

Employees' ISP Compliance Intention:

1. **I intended to comply with the information security policies of my organization in the last year**
2. **I intended to protect information and technology resources according to the information security policies of my organization in the last year**
3. **I intended to carry out my responsibilities prescribed in the information security policies of my organization when I used information and technology in the last year**

Awareness of Organizational ISP:

1. **My organization has specific security policies that describe acceptable use of e-mail**
2. **My organization has a formal security policy that forbids employees from accessing computer systems that they are not authorized to use**
3. **My organization has specific security policies that describe acceptable use of computer passwords**
4. **My organization has specific security policies that govern what employees are allowed to do with their computers**
5. **My organization has established security policies of behavior for use of computer resources**
6. **I know the rules and regulations prescribed by the information security policies of my organization**
7. **I know my responsibilities as prescribed in the information security policies to enhance the information systems security of my organization**

Awareness of Information Security Threats:

1. **I have received information security threat alerts from my organization's IT department**

2. **My organization has a forum for employees to discuss information security threats**

3. **In my organization, information security threats are publicized immediately after they are detected**

4. **I am informed of the potential information security threats when they are detected by my organization**

Perceived Self-Efficacy to Compliance:

1. **I have the necessary skills to comply with the information security policies of my organization**
2. **I have the necessary knowledge to comply with the information security policies of my organization**

3. **I can comply with the information security policies of my organization by myself**

4. **It is easy to comply with the information security policies of my organization**

Perceived Controllability

1. **I have the necessary management support to comply with the information security policies of my organization**
2. **I have the necessary technical support to comply with the information security policies of my organization**

3. **Compliance with the information security policies is completely under my control**

Perceived Sanction Severity:

1. **The organization disciplines employees who break information security policies**
2. **My organization terminates employees who repeatedly break information security policies**

3. **If I were caught violating my organization's information security policies, I would be severely punished**

Perceived Reward:

5. **If I would follow the information security policies of my organization, I would save time**
6. **If I would follow the information security policies of my organization, I would save work time**
7. **My compliance with the information security policies would result in benefits to me**
8. **My compliance with the information security policies would provide gains to me**