Cyber Security Awareness and Its Impact on Employee's Behavior

Ling Li, Li Xu, Wu He, Yong Chen, Hong Chen

Cyber Security Awareness and Its Impact on Employee's Behavior

Ling Li(✉), Li Xu, Wu He, Yong Chen, and Hong Chen

Old Dominion University, 5115 Hampton Blvd, Norfolk, USA
{ lli, lxu, whe, y7chen, hchen001} @odu.edu

Abstract. This paper proposes a model that extends the Protection Motivation Theory to validate the relationships among peer behavior, cue to action, and employees' action experience of cyber security, threat perception, response perception, and employee's cyber security behavior. The findings of the study suggest that the influence from peer behavior and employees action experience of cyber security is an important factor for improving cyber security behavior in organizations. Peer behavior positively affects cue to action, which positively impacts employees' action experience. Employees' action experience then would have positive impacts on their threat perception and response perception. As a result, employees' threat perception and response perception are positively related to their cyber security behavior. This process is a chain reaction.

Keywords: Cyber security awareness · Employee cyber security behavior

1 Introduction

Recent cyber security breaches have caught attention of many organizations to take appropriate measures to security their database and business, and to develop effective cyber security policies. The top 5 cyber security threats identified by a Sungard Availability Services survey [1] in 2014 are vulnerable web applications, being overall security aware, out-of-date security patches, failure to encrypt PCs and sensitive data, and obvious or missing passwords. Among these threats, security awareness was ranked the second as the most important

cyber security issue and was noted by 51% of respondents. Therefore, designing and implementing security awareness programs, such as cyber security policy enforcement [2, 3, 4] and mandated trainings [3, 5, 6], security communication and computer monitoring [6], and top management commitment [6], are essential to improve cyber security.

2 Background and Hypotheses

This paper proposes a model by integrating the protection motivation theory (PMT) and the Health Belief Model (HBM) to test the cyber security awareness and its impact on employee's behavior. Figure 1 shows the relationships among peer behavior, cue to action, employees' action experience of cyber security, threat perception (perceived severity, perceived vulnerability and perceived barriers), response perception (response efficacy and self-efficacy), and cyber security behavior.

Prior research has explored the reasons why security awareness programs are not effective. Specifically, Herath and Rao [7] developed and tested a theoretical model of the incentive effects of penalties, pressures and perceived effectiveness of employee actions. They found that employees' cyber security behaviors were influenced by intrinsic and extrinsic motivators. Ng and Xu [8] adopted the Health Belief Model (HBM) in user security study and found that users' perceived susceptibility, perceived benefits, and self-efficacy would determine their security behavior. A number of published studies adopt the protection motivation theory (PMT) to investigate how employees' threat perception and response perception regarding cyber security impact their compliance behaviors (e.g. [9-13]).

However, findings reported by these studies are inconsistent. For example, Ng and Xu [8] find that individuals exposed to higher levels of cue to action do not have a higher level cyber security behavior than others; whereas Johnston and Warkentin [10] find that social influence have a positive effect on individuals' intention to adopt cyber security actions. Individuals' perceived severity of cyber-attacks have been found have both positive impacts [9, 13, 14], or negative impacts [8], or even no impact [15] on their intention to comply with cyber security policies. Similarly, individuals' perceived vulnerability of cyber-attacks has been found to be both positively [14] or negatively [13] influence

their intention to comply with cyber security policies. Furthermore, individuals' response efficacy of cyber-attacks is found to be both positively [9, 10] or negatively [13, 14] affect their intention to comply with cyber security policies as well.

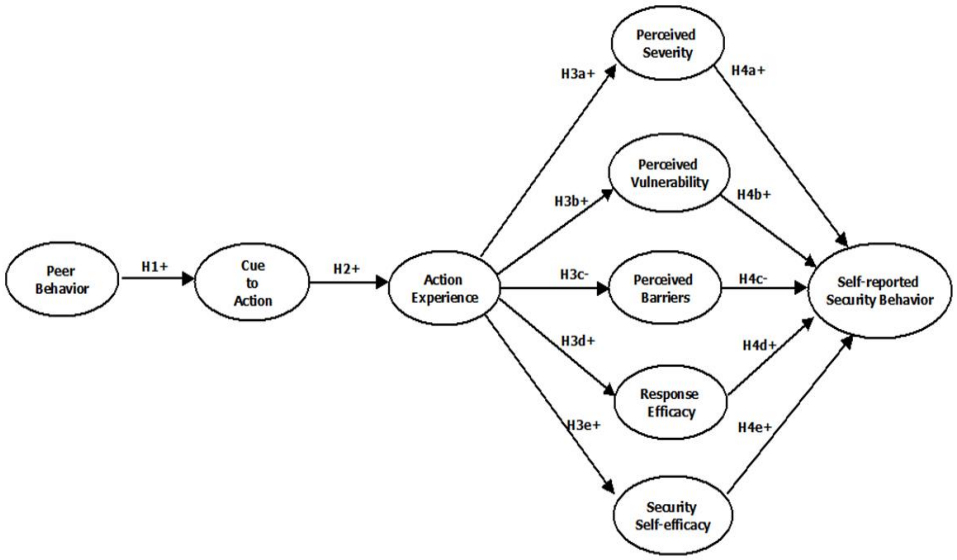

Fig.1. Conceptual Model

However, findings reported by these studies are inconsistent. For example, Ng and Xu [8] find that individuals exposed to higher levels of cue to action do not have a higher level cyber security behavior than others; whereas Johnston and Warkentin [10] find that social influence have a positive effect on individuals' intention to adopt cyber security actions. Individuals' perceived severity of cyber-attacks have been found have both positive impacts [9, 13, 14], or negative impacts [8], or even no impact [15] on their intention to comply with cyber security policies. Similarly, individuals' perceived vulnerability of cyber-attacks has been found to be both positively [14] or negatively [13] influence their intention to comply with cyber security policies. Furthermore, individuals' response efficacy of cyber-attacks is found to be both positively [9, 10] or negatively [13, 14] affect their intention to comply with cyber security policies as well.

We intend to provide a clearer picture on employee cyber security behavior by proposing a model (Figure 1) that integrates the protection motivation theory (PMT) and the Health Belief Model (HBM) to validate the relationships among peer behavior, cue to action, employees' action experience of cyber security, their threat perception (perceived severity, perceived vulnerability, and perceived barriers) and response perception (response efficacy and self-efficacy), and their cyber security behavior. A number of hypotheses based on Figure 1 have been developed.

Hypothesis 1. Peer behavior is positively associated with cues to action for employees' cyber security behaviors.

Hypothesis 2. Cues to action positively affect employees' action experience of cyber security.

Hypothesis 3a. Employees' action experience positively affects their perceived severity of cyber security incidents.

Hypothesis 3b. Employees' action experience positively affects their perceived vulnerability caused by cyber security incidents.

Hypothesis 3c. Employees' action experience negatively affects their perceived barriers about cyber security incidents.

Hypothesis 3d. Employees' action experience positively affects their response-efficacy about cyber security incidents.

Hypothesis 3e. Employees' action experience positively affects their self-efficacy about cyber security incidents.

Hypothesis 4a. Employees' perceived severity positively affects their self-reported cyber security behavior.

Hypothesis 4b. Employees' perceived vulnerability positively affects their self-reported cyber security behavior.

Hypothesis 4c. Employees' perceived barriers negatively affect their self-reported cyber security behavior.

Hypothesis 4d. Employees' response efficacy positively affects their self-reported cyber security behavior.

Hypothesis 4e. Employees' self-efficacy positively affects their self-reported cyber security behavior.

3 Research Method

The empirical data was collected using a survey questionnaire in the US in 2015. Sample size in this study is 579. The socio-demographic characteristics data are reported in Table 1. About 35% of the respondents are male and 65% are female. Among the participants, 68.58% are under 30 years old. Respondents are from diverse industries. When they were asked whether their company had an explicit cyber security policy, about 46% of the participants answered "yes", 14.68% answered "no", and a little over a third of the participants (39.21%) said that they knew nothing about their company's information security policy. Variables about behavior and belief are assessed via a seven-point Likert scale, ranging from strongly disagree (1) to strongly agree (7).

Structural equation modeling (SEM) method was applied to explore the relationships among the constructs in the conceptual model. SEM follows a two-step approach that includes constructing the measurement model and testing the structural model. Specifically, we test the proposed model and assess the overall fit using the maximum likelihood method in Amos.

Nine latent constructs and their observed variables are measured in the proposed model. Most of measurements in this study were tested in previous studies. To assess the reflective constructs in our measurement model, we examined construct reliability and validity, convergent validity, and discriminant validity. First, we conducted principal component analysis to identify and to confirm the different factors under each construct in our model. Specifically, we ran exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) in SPSS. EFA using principal-component factor analysis with Varimax rotation was performed to examine the factor solution among the nine factors in the study. The results reveal that the nine factors have eigenvalues greater than 1. Next, CFA is conducted to confirm the factors under each latent variable. The results of CFA are shown in Table 2.

The results of CFA confirm the significance of all paths between observed variables and the first order latent variables at the significant level $p < 0.001$. The construct validity of our model is explained through the percentage of variance extracted [16]. The total variance explained by each construct is in the range of 53% - 73% (see Table 2). Reliability for the constructs is assessed via Cronbach's alpha. The reliability for all constructs is considered acceptable

[17], because all the values are bigger than the threshold 0.70 (Table 2). Hence, we claim that both the construct validity and the construct reliability of our model are satisfactory.

Table 1. Socio-Demographic Characteristics

Gender	**Frequency**	**Percent (%)**
Male	200	34.54
Female	379	65.46
	579	100.00
Age		
Younger than 18	2	0.35
18-20	168	29.02
21-30	227	39.21
31-40	81	13.99
41-50	56	9.67
51 and above	45	7.77
	579	100.00
Industry		
Government	44	7.60
Education	165	28.50
Finance/Banking/Insurance	18	3.11
Information Technology	31	5.35
Retail/wholesale	74	12.78
Real estate	43	7.43
Telecommunications	8	1.38
Healthcare/Medical	60	10.36
Military	19	3.28
Others	117	20.21
	579	100.00
Security Policy Awareness		
NO	85	14.68
Yes	267	46.11
Don't know	227	39.21
	579	100.00

Table 2. Results of Factor Analysis

Indicator	Loading	S.E.	R^2	Total	Cronbac	AVE
Action experience(AE)				62.45	0.80	0.43
AE1	0.60***	0.11	0.36			
AE2	0.50***	0.10	0.25			
AE3	0.68***	0.07	0.46			
AE4	0.81***	0.10	0.65			
Perceived vulnerability(PV)				68.72	0.85	0.55
PV1	0.74***	0.09	0.54			
PV2	0.71***	0.09	0.51			
PV3	0.72***	0.06	0.52			
PV4	0.81***	0.07	0.65			
Perceived severity(PS)				73.41	0.82	0.68
PS1	0.72***	0.12	0.52			
PS2	0.77***	0.10	0.59			
PS3	0.97***	0.10	0.94			
Perceived barriers(PBA)				54.61	0.72	0.48
PBA1	0.70***	0.10	0.50			
PBA2	0.75***	0.10	0.57			
PBA3	0.67***	0.11	0.45			
PBA4	0.62***	0.09	0.39			
Response efficacy(RE)				64.01	0.81	0.58
RE1	0.83***	0.06	0.68			
RE2	0.82***	0.06	0.67			
RE3	0.79***	0.05	0.62			
RE4	0.61***	0.05	0.37			
Cues to action(CA)				68.48	0.85	0.60
CA1	0.82***	0.09	0.68			
CA2	0.88***	0.09	0.77			
CA3	0.65***	0.10	0.42			
CA4	0.74***	0.10	0.55			
Security self-efficacy(SE)				62.25	0.88	0.66
SE1	0.75***	0.10	0.56			
SE2	0.75***	0.09	0.57			
SE3	0.85***	0.10	0.72			
SE4	0.81***	0.10	0.65			
SE5	0.86***	0.08	0.73			
SE6	0.85***	0.08	0.72			
Peer behavior(PBE)				67.50	0.76	0.57
PBE1	0.78***	0.08	0.61			
PBE2	0.81***	0.09	0.66			
PBE3	0.67***	0.08	0.45			
Self-reported security behavior(SCB)				53.46	0.71	0.38
SCB1	0.63***	0.08	0.40			
SCB2	0.65***	0.06	0.42			
SCB3	0.46***	0.08	0.21			
SCB4	0.71***	0.08	0.51			

Convergent validity assesses consistency across multiple items. It is shown when the indicators load much higher on their hypothesized factor than on other factors (i.e., own loadings are higher than cross loadings). Items that do not exceed the threshold will be dropped from the construct list. For our model, all estimated standard loadings are significant at the significant level of $p< 0.001$ [18] with acceptable magnitude (>0.50, ideal level is >0.70) [19] except SCB3. The results indicate that the measurements in our model have good convergent validity.

The fit statistics of the structural model is reported in Table 3. The fit indices chosen for our model represent two characteristics: the global fit measures and comparative fit measures. The chi-square test (χ^2) with degrees of freedom is commonly used as the global model fit criteria. The chi-square statistic must, however, be interpreted with caution especially for a large sample size because the hypothesized model may be rejected if the discrepancy is not statistically equal to zero. We choose comparative fit index (CFI), goodness of fit index (GFI), incremental fit index (IFI), and root mean square error of approximation (RMSEA) to assess the congruence between the hypothesized model and the data.

The goodness of fit indices for the specified model are displayed in Table 3. The χ^2 value for the structural equation model is 1882 (DF=582). The ratio of χ^2 and the degrees of freedom (DF) is 3.23. The comparative fit index (CFI) is 0.87, the goodness-of-fit index (GFI) is 0.84 and the incremental fit index (IFI) is 0.87. All the values are closed to the generally accepted minimum norms for satisfactory fit of 0.90.

The test of the structural model includes estimating the path coefficients, which indicate the strength of the relationships between the independent and dependent variables, and the R^2 values, which are the amount of variance explained by the independent variables. The full set of relationship for the structural model is provided in Table 4.

The hypotheses in our structural model test the relationships among peer behavior, cue to action, employees' action experience of cyber security, threat perception (perceived severity, perceived vulnerability, and perceived barriers), response perception (response efficacy and self-efficacy), and their cyber security behavior. The results of our study support 11 out of 12 hypotheses that have been developed based on the conceptual model in Figure 1. Hypothesis 4a

(Employees' perceived severity positively affects their self-reported cyber security behavior) is the only one that is not supported. Table 4 shows the summary of hypotheses test result for the structural model.

Table 3. Fit Statistics for Structural Model

Model goodness of fit statistics	**Model value**
χ^2	1882
df	582
χ^2/DF	3.23
Root mean square error of approximation (RMSEA)	0.062
Comparative fit index (CFI)	0.87
Goodness-of-fit index (GFI)	0.84
Incremental fit index (IFI)	0.87

4 Discussions

This paper proposes a model that integrates the protection motivation theory and the Health Belief Model to validate the relationships among peer behavior, cue to action, employees' action experience of cyber security, threat perception (perceived severity, perceived vulnerability, and perceived barriers), response perception (response efficacy and self-efficacy), and their self-reported cyber security behavior. The results confirm that (a) peer behavior is a significant factor in enhancing the cue to action for employee's behavior towards cyber security; (b) cue to action significantly influences employees' action experience related to cyber security; (c) employees' action experience of cyber security positively affects their perceived severity, perceived vulnerability, response efficacy, and security self-efficacy but negatively affects their perceived barriers; (d) employees' perceived severity, perceived vulnerability, response efficacy, and self-efficacy positively impact their self-reported security behavior and employees' perceived barriers negatively impacts their self-reported security behavior. These findings concur with the results in previous research regarding the factors that regarding employees' cyber security behavior in workplace [8-10, 12, 14].

This study explores self-reported cyber security behavior to measure employees' cyber security activities; this approach is different from prior cyber

security studies that used behavioral intention or likelihood of behavior as their dependent variables. Our measurement reflects employees' actual behavior, not their intentions. Therefore, the results achieved in this study are more convincing.

Table 4. Summary of Hypotheses Test Result for the Structural Model

	Paths	**Standard path coefficient**	**p-value**
H1	Peer behavior → Cue to action	0.53	< 0.001
H2	Cue to action → Action experience	0.74	< 0.001
H3a	Action experience → Perceived severity	0.17	< 0.001
H3b	Action experience→Perceived vulnerability	0.62	< 0.001
H3c	Action experience → Perceived barriers	-0.19	< 0.001
H3d	Action experience → Response efficacy	0.47	< 0.001
H3e	Action experience → Security self-efficacy	0.43	< 0.001
H4a	Perceived severity→ Self-reported security behavior	0.03	> 0.5
H4b	Perceived vulnerability → Self-reported security behavior	0.12	< 0.05
H4c	Perceived barriers → Self-reported security behavior	-0.24	< 0.001
H4d	Response efficacy → Self-reported security behavior	0.21	< 0.001
H4e	Security self-efficacy → Self-reported security behavior	0.49	< 0.001

The results of this study reveal that the influence from peer behavior and employees own action experience of cyber security is an important factor for improving cyber security in organizations. Peer behavior positively affects cue to action, which positively impacts employees' action experience (H1 and H2). Employees' action experience then would have positive impacts on their threat perception and response perception (H3a, H3b, H3d, and H3e). As a result, employees' threat perception and response perception positively affect their cyber

security behavior (H4a, H4b, H4d, and H4e). This process is a chain reaction.

5 Conclusions

From the findings of the study, we may suggest that organizations may consider developing a system of rewards to create a pro-security internal atmosphere. Particularly, those employees who follow cyber security regulations and rules should be encouraged. In this way, employees can get clear cues from their peers in terms of taking cyber security action. Meanwhile, organizations should promote experience sharing regarding mitigating cyber security risks and reducing cyber security threat. This could be realized through effective training programs.

This study has limitations that should be taken into account. Future research need to compare the results of self-reported behavior and behavioral intention/likelihood of behavior. Future research may also analyze the moderating effect of cyber security policy awareness level, industry, employee age, and other factors with other statistical tools. Moreover, future research should explore the underlying causes of the moderating effect of gender and examine the effect using empirical tests.

Acknowledgements. This work was supported by the National Science Foundation of the U.S. under [Grant Number 1318470].

References

1. DeMetz, A..: The #1 Cyber Security Threat to Information Systems Today (2015). http://www.forbes.com/sites/sungardas/2015/03/12/cyber-security-threats-to-information-systems-today/#6b46ca2bb1b0
2. Chen,Y., He, W. .: Security risks and protection in online learning: A survey. The International Review of Research in Open and Distributed Learning, 14(5)(2013)
3. D'Arcy, J., Hovav, A., Galletta, D. .: User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research 20(1), 79-98(2009)
4. Yayla, A. .: Enforcing Information Security Policies through Cultural Boundaries: A Multinational Company Approach. In Proceedings of 2011 ECIS, Paper 243, pp

1-11 (2011)
5. Stoneburner, G., Goguen, A.Y., Feringa, A. .: Sp 800-30. Risk management guide for information technology systems (2002)
6. D'Arcy, J., Greene, G. .: Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security 22(5),474-489(2014)
7. Herath, T., Rao, H. R. .: Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems 47(2),154-165(2009)
8. Ng, B.Y., Xu, Y. .: Studying users' computer security behavior using the Health Belief Model. PACIS 2007 Proceedings 45, pp 423-437(2007)
9. Herath, T., Rao, H.R. .: Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 18(2),106-125(2009)
10. Johnston, A.C., Warkentin, M. .: Fear appeals and information security behaviors: an empirical study. MIS quarterly, 549-566(2010)
11. Siponen, M., Mahmood, M. A., Pahnila, S. .: Technical opinion Are employees putting your company at risk by not following information security policies? Communications of the ACM, 52(12), 145-147(2009)
12. Steinbart, P. J., Keith, M. J., Babb, J. .: Examining the Continuance of Secure Behavior: A Longitudinal Field Study of Mobile Device Authentication. Information Systems Research (2016)
13. Vance, A., Siponen, M., Pahnila, S. .: Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management 49(3), 190-198 (2012)
14. Siponen, M., Mahmood, M.A., Pahnila, S. .: Employees' adherence to information security policies: An exploratory field study. Information & management, 51(2), 217-224(2014)
15. Ng, B.Y., Kankanhalli, A., Xu, Y.C. .: Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825(2009)
16. Fornell, C., Larcker, D.F. .: Structural equation models with unobservable variables and measurement error: Algebra and statistics. Journal of marketing research, 382-388(1981)
17. Gefen, D., Straub, D., Boudreau, M.C. .: Structural equation modeling and regres-

sion: Guidelines for research practice. Communications of the association for information systems, 4(1), 7 (2000)
18. Gefen, D., Straub, D. .: A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. Communications of the Association for Information systems, 16(1), 5 (2005)
19. Chin, W., Marcolin, B. .: The holistic approach to construct validation in IS research: examples of the interplay between theory and measurement. In administrative sciences association of Canada annual conference- (Vol. 16, pp. 34-43). Administrative Sciences Association of Canada (1995)