การศึกษาพฤติกรรมการระวังป้องกันภัยคุกคามบนสมาร์ทโฟน

Protection Motivation Theory Model for Smartphone User

Varin Kheara, Suthee Chantrapunth, and Chun Che Fung

Murdoc University

Navaminda Kasatriyadhiraj Royal Thai Air Force Academy

School of Information Technology, Murdoch University, Australia

E-mail: varin@gmail.com, suthee_c@gmail.com, l.fung@murdoch.edu.au

บทคัดย่อ

สมาร์ทโฟนกลายเป็นสิ่งจำเป็นที่อำนวยความสะดวกให้กับชีวิตประจำวันของเราอย่างที่ไม่เคยมีมาก่อน ทำให้เราสามารถเชื่อมต่อกับโลกภายนอกผ่านเครือข่ายอินเตอร์เน็ตได้ เป็นการเสริมสร้างศักยภาพการทำงานและความบันเทิงในชีวิตประจำวัน อย่างไรก็ตาม การพัฒนาทางด้านไซเบอร์จะมาควบคู่กับการโจมตีทางอินเตอร์เน็ต ซึ่งปัจจุบันการโจมตีไม่ได้เกิดขึ้นเฉพาะบนคอมพิวเตอร์เท่าไร แต่ยังเกิดขึ้นกับสมาร์ทโฟนเช่นกัน การโจมตีอาจเป็นการปล่อยมัลแวร์ การโจรกรรมข้อมูล หรือการเรียกค่าไถ่ข้อมูล ซึ่งจัดเป็นภัยคุกคามที่ร้ายแรงที่สร้างความเสียหายให้แก่ผู้ใช้สมาร์ทโฟนเป็นอย่างมาก การศึกษานี้ได้นำทฤษฎีแรงบันดาลใจในการป้องกันตนเอง (Protection Motivation Theory: PMT) ของ Roger R.W. (1983) ซึ่งเป็นทฤษฎีที่ถูกออกแบบมาเพื่อศึกษาความหวาดกลัวของคนไข้ (fear appeal) ที่ไปกระตุ้นให้เกิดพฤติกรรมในการระวังป้องกันตนเอง (protection behavior) จากการเจ็บป่วยมาใช้เป็นทฤษฎีฐานในการศึกษาพฤติกรรมการระวังป้องกันภัยคุกคามบนสมาร์ทโฟน การวิจัยนี้มีจุดประสงค์เพื่อสร้างตัวแบบพฤติกรรมการระวังป้องกันภัยคุกคามทางไซเบอร์ของผู้ใช้สมาร์ทโฟน ผลที่ได้การวิจัยนี้จะเป็นประโยชน์สำหรับการนำไปใช้ในการศึกษาความสัมพันธ์เชิงสาเหตุของแต่ละปัจจัยในตัวแบบด้วยวิธีการวิเคราะห์สมการเชิงโครงสร้าง (Structural Equation Model: SEM) ต่อไป

คำสำคัญ: ภัยคุกคามทางไซเบอร์ สมาร์ทโฟน ทฤษฎีแรงบันดาลใจในการป้องกัน

Abstract

Smartphones are becoming a necessity that facilitates our daily life, allowing us to connect with the outside world via the internet, and empowering work and entertainment. It is considered as an essential part of our daily lives like that never happens before. However, the more growing up using internet, the more development of cyber attacks. The attacks are not only attack on the computer system, but they are more likely to attack on smartphones as well. These attacks can be malware, identity theft, ransom, or etc. which can create various damages to the owners. The researcher used Roger R.W. (1983)'s Protection Motivation Theory (PMT),[1] originally created for studying fear appeals of patients that affected their behaviors in protecting themselves from health threats, as the base theory for studying protection behaviors of smartphone users. Objective of this study is to find factors for creating a protection behavior model and instrument for gathering data. Results of this study are useful for studying the causal relationships among factors in the proposed model with the technique called Structural Equation Model (SEM) analysis.

Key words: Cyber threat, Smartphone, Behavior, Protection Motivation Theory

1. Objective and Benefit of this Study

As more and more people adopt smartphones, cyber security landscapes are now changing. Cyber attacks are now coming to smartphones. Now-a-day it is quite clear that the amount of new viruses and malwares that was created for smartphone is increasing as technologies of smartphones are advancing. Smartphones are now as powerful as personal computers. There is more direct information contained in the smartphones while there is very little to no protection. As we already know that any successful cyber security program must consist of a balance between the three critical elements, which are the people, process, and technology. However, majority of research has been conducted on the technical aspect of security whereas limited research has been conducted on the weakest link of the chain, which is the people and how they adopt the process to secure themselves. To fill out these gaps, this study aimed to invent factors that affect behaviors of smartphone users in preventing themselves from cyber threats. The study adopted Roger, R.W. (1983)'s the Protection Behavior Theory (PMT) [1] which was originally used for studying effects of patients' fear appeal towards their protection behavior from ailment disease threats. The proposed model will be useful for performing causal relationship study with the technique called Structural Equation Model or SEM.

2. Protection Motivation Theory

R.W. Rogers developed the Protection Motivation Theory (PMT) in 1975 [2] and was later expanded to a more general theory of persuasive communication in the social psychology and health domains (Rippetoe & Rogers 1987).[3] PMT model is very popular and has been considered as one of the most powerful explanatory theories for predicting an individual's intention to engage in protective actions (Anderson & Agarwal 2010).[4] PMT is used to explain if a threat is perceived by people as fearful, they will be more cautious and prevent the possible threat (Humaidi & Balakrishnan 2012).[5] Originally, PMT was designed to be used in the health area, to study how people react when diagnosed with health related illnesses. Currently, PMT has been extended to other areas of study such as information security. Many recent studies used the PMT in predicting behaviors related to an individual's computer security behaviors both at home and in organizations (Srisawang, Thongmak & Ngarmyarn, 2015).[6]

PMT is a concept for understanding the fear appeals of people by focusing on how people behave and cope during stressful situations.[1] People can be motivated to take a particular action, divert behavior through the threat of impending danger or harm, by arousing fear (Maddux & Rogers, 1983).[7] PMT describes the adaptive and maladaptive coping with particular health threat through process of appraisal of the health threat, an individual's assessment of the level of danger posed by a threatening event (Woon, Tan, & Low 2005),[8] and through the process of appraisal of the coping responses result that will increase the behavior in lessening the threat (Boer & Seydel, 1996).[9]

PMT model consists of threat appraisal and the coping appraisal that can increase the behaviors in protecting themselves from threats (Boer & Seydel, 1996).[9] For threat appraisal, three factors are used to appraise the threats: (1) the perceived severity of a threatening event; (2) the perceived probability of the occurrence, the probability that one will experience harm; and (3) rewards, the positive aspects of starting or continuing the unhealthy behavior. The model shows that the total amount of threat experienced equals to the summation of severity and vulnerability, minus with rewards. For coping appraisal, three factors are used to evaluate the responsive result: (1) the efficacy of the recommended preventive behavior or response efficacy, the effectiveness of the recommended behavior in removing or preventing possible harm; (2) the perceived self-efficacy, the belief that one can successfully enact the recommended behavior (Roger, 1975)[2]; and (3) response costs which are associated with the recommended behavior. Lastly, the total amount of coping ability that a person can experience is the summation of response effectiveness and self-efficacy, minus the response costs. The PMT model proposed by Roger (1983)[1] is shown in Figure 1.

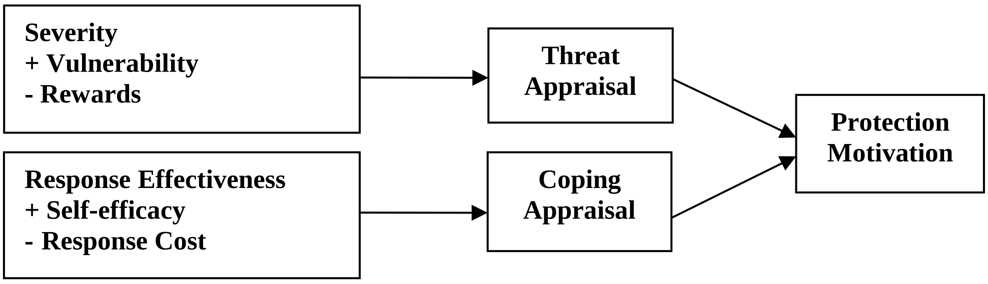

Figure 1 Cognitive Process of Protection Motivation Theory

Redrawn from Rogers (1983)

3. Related Studies

3.1 The Study of Liang & Xue (2009)

Liang & Xue (2009),[10] the authors of "Avoidance of Information Technology Threats: A Theoretical Perspective," proposed the Technology Threat Avoidance Theory (TTAT) which explains the preventing behaviors of the computer and internet users from cyber threats. They contended that there are two cognitive processes that motivate users to protect themselves from threats, they are: threat appraisal and coping appraisal. By integrating models from three studies: the PMT of Rogers

(1975 & 1983);[2][1] Health Belief Model of Janz and Becker (1984)[11] and Rosen stock (1974);[12] and Risk Analysis Research of Baskerville (1991 & 1991),[13][14] Liang & Xue proposed the variance theory view of TTAT (shown in Figure 2) which consists of three main parts, they are: (1) Threat Appraisal; (2) Coping Appraisal; and (3) Coping. Threat Appraisal consists of three constructs including perceived susceptibility, perceived severity and perceived threat. Coping Appraisal consists of four constructs, they are: Perceived Effectiveness, Perceived Costs, Self-efficacy, and Perceived Availability. Coping consists of three constructs, they are: Avoidance Motivation, Avoidance Behavior, and Emotion-focused Coping. In addition, there are two social environment factors that affect the model, they are: Risk Tolerance and Social Influence.

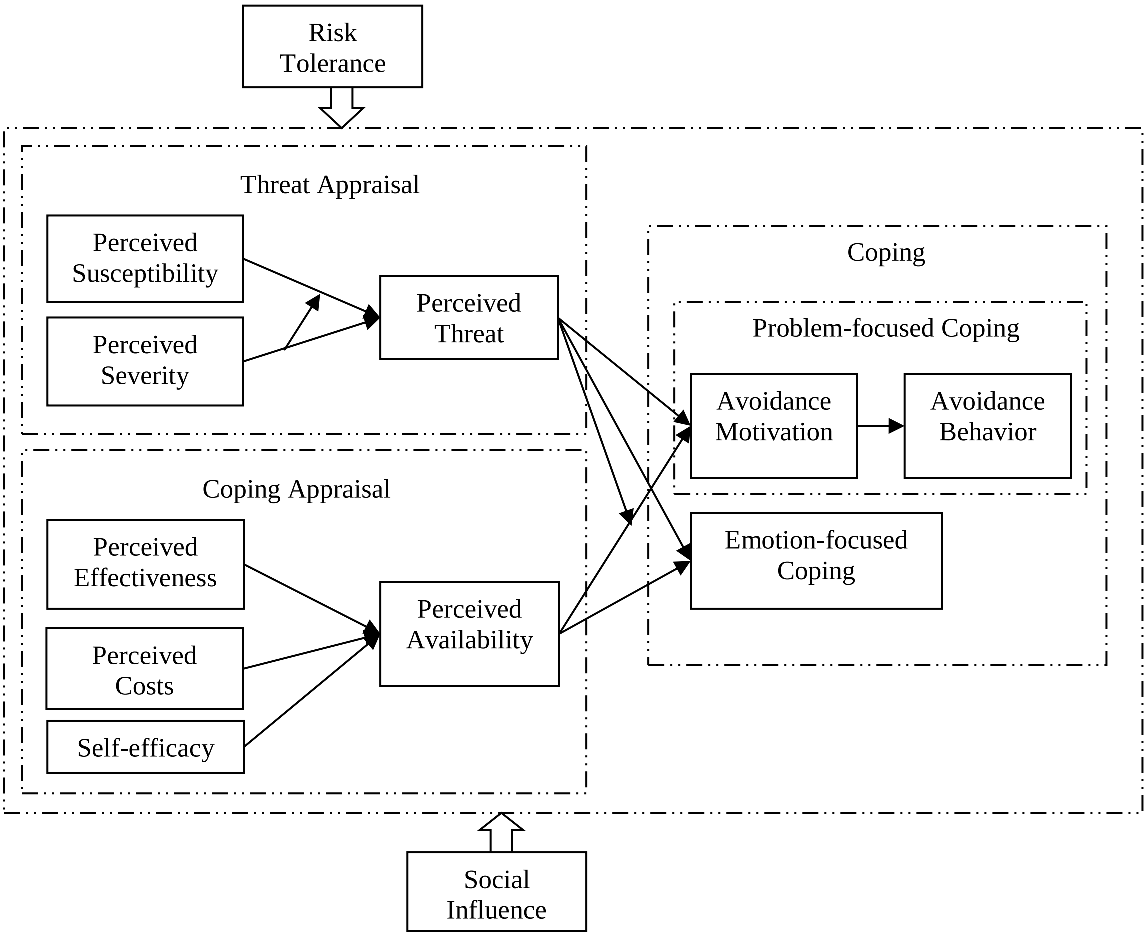

Figure 2 The Variance Theory View of TTAT

Redrawn from Liang & Xue (2009)[10]

3.2 The Study of Srisawang, Thongmak & Ngarmyarn (2015)

Srisawang, Thongmak & Ngarmyarn (2015)[6] wrote the authors of "Factors Affecting Computer Protection Behavior" which is based on PMT model. They proposed factors that affect computer crime protection behavior (shown in Figure 3), including: (1) Conscientious Personality, individuals' traits of being painstaking and careful; (2) Perceived Value of Data, individuals' perceptions on the value of data in term of monetary value and emotional value; (3) Prior Experience, the past experiences of individuals; (4) Subjective Norm, individual perception on social pressures to perform or not to perform some things; (5) Security Knowledge, individuals' knowledge of computer security; and (6) Safeguard Costs, costs in performing the recommended behavior. The model was tested with 600 empirical data that were the people who used personal computers at homes and at the workplaces in Thailand. The results showed that all the factor variables had significant effects on the computer crime protection behavior.

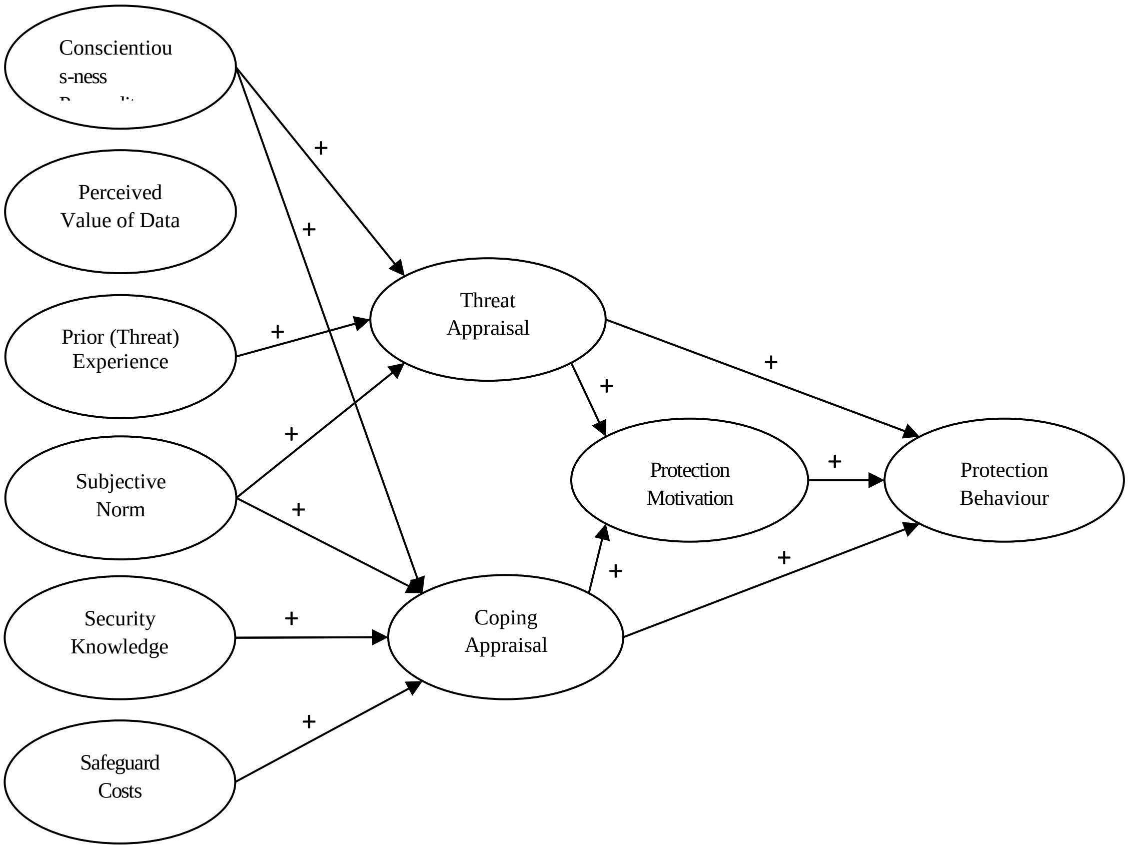

Figure 3 The Proposed Research Model of Srisawang, Thongmak & Ngarmyarn (2015)

Redrawn from Srisawang, Thongmak & Ngarmyarn (2015)[6]

3.3 The Study of Tu, Z.L. & Yuan, Y.F. (2012)

The study of Tu, Z.L. & Yuan, Y.F. (2012)[15] wrote "Understanding User's Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft" which is about the potential risks of mobile devices being loss and theft, and the countermeasures to cope with these risks. Their study adopted the PMT as core of the study. They presented a framework for analyzing behaviors of mobile device users in coping with the risk of mobile devices loss and theft (shown in Figure 4) which consists of five constructs, they are: Threat Appraisal, Coping Appraisal, Social Influence, Coping Intention of Mobile Devices Loss and Theft, and Coping Behavior of Loss and Theft Threat. Threat Appraisal has two sub-constructs, they are: Perceived Vulnerability and Perceived Severity, while Coping Appraisal has four sub-constructs: Locus of Control, Self-efficacy, Perceived cost, and Perceived Effectiveness.

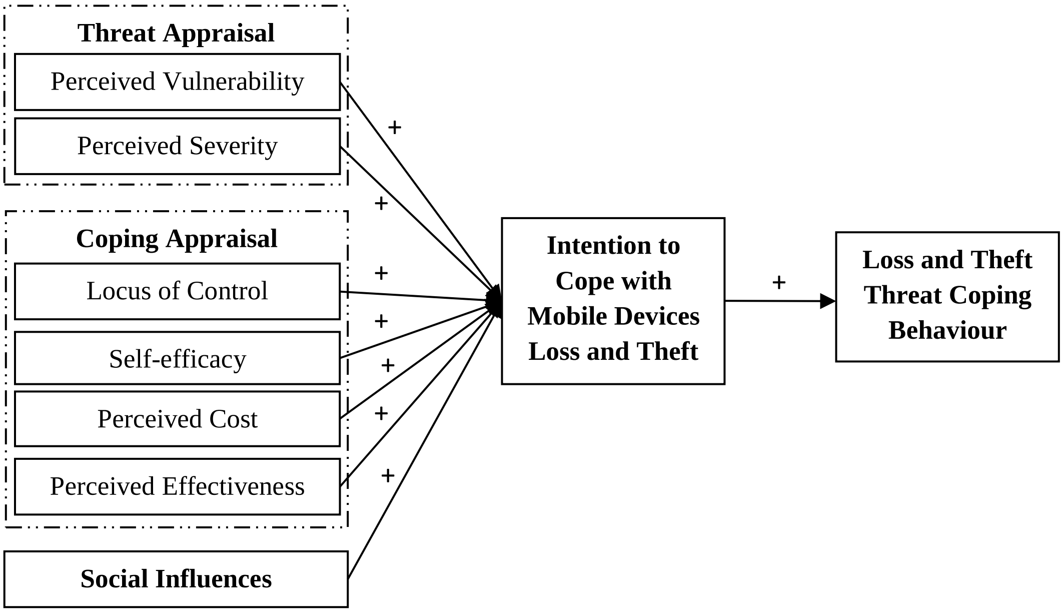

Figure 4 The Proposed Research Framework of Tu, Z.L. & Yuan, Y.F. (2012)

Redrawn form Tu, Z.L. & Yuan, Y.F. (2012)[15]

4. Proposed Theoretical Model

4.1 Selected Constructs

In selecting variables for this study, the researcher gives precedence to exogenous and endogenous variables that basically comply with the PMT, and also impact the appraising abilities of the smartphone users in coping with cyber threats. The selected constructs for this study consist of: (1) five exogenous variables, they are: Perceived Severity, Perceived Vulnerability, Social Influence, Self-efficacy, and Response Effectiveness; and (2) four endogenous variables including: Threat Appraisal, Coping Appraisal, Protection Motivation, and Protection Behavior. Details of these constructs and their supported scholars are shown in Table 1.

Table 1 Selected Constructs and Supported Scholars

Selected Constructs	Supported Scholars			
	Rogers (1983)[1]	**Liang & Xue (2009)[10]**	**Srisawang, Thongmak, Ngarmyarn (2015)[6]**	**Tu, Z.L. & Yuan, Y.F., (2012)[15]**
Perceived Severity / Prior (Threat) Experience	✓	✓	✓	✓
Perceived Vulnerability / Perceived Susceptibility	✓	✓		✓
Social Influence / Subjective Norm		✓	✓	✓
Response Effectiveness / Perceived Effectiveness	✓	✓		✓
Self-efficacy / Security Knowledge	✓	✓	✓	✓
Threat Appraisal / Perceived Threat	✓	✓	✓	✓
Coping Appraisal / Perceived Availability	✓	✓	✓	✓
Protection Motivation / Avoidance Motivation / Coping Intention	✓	✓	✓	✓
Protection Behavior / Avoidance Behavior / Coping Behavior		✓	✓	✓

4.2 Determine the Relationships between Constructs

Next, the relationships between the selected constructs are determined according to the PMT and the related studies. Details are shown in Table 3.

Table 3 Relationships between Constructs and the Supported Scholars

Relationships (Positive Impact)	**Supported Theory or Related Studies**			
	Rogers (1983)[1]	**Liang & Xue (2009)[10]**	**Srisawang, Thongmak, Ngarmyarn (2015)[6]**	**Tu, Z.L. & Yuan, Y.F., (2012)[15]**
Perceived Severity → Threat Appraisal	✓	✓	✓	✓
Perceived Vulnerability →Threat Appraisal	✓	✓		✓
Social Influence → Threat Appraisal		✓	✓	
Social Influence → Coping Appraisal		✓	✓	
Response Effectiveness → Coping Appraisal	✓	✓		✓
Self-efficacy → Coping Appraisal	✓	✓	✓	✓
Threat Appraisal → Protection Motivation	✓	✓	✓	✓
Threat Appraisal → Protection Behavior			✓	
Coping Appraisal → Protection Motivation	✓	✓	✓	✓
Coping Appraisal → Protection Behavior			✓	
Protection Motivation → Protection Behavior		✓	✓	✓

4.3 The Proposed Model and Hypotheses

Based on the selected constructs and their relationships found in the previous section, the researcher depicts them as a diagram the shows the constructs, their descriptions, and the relationships between them. Details are shown in Figure 5.

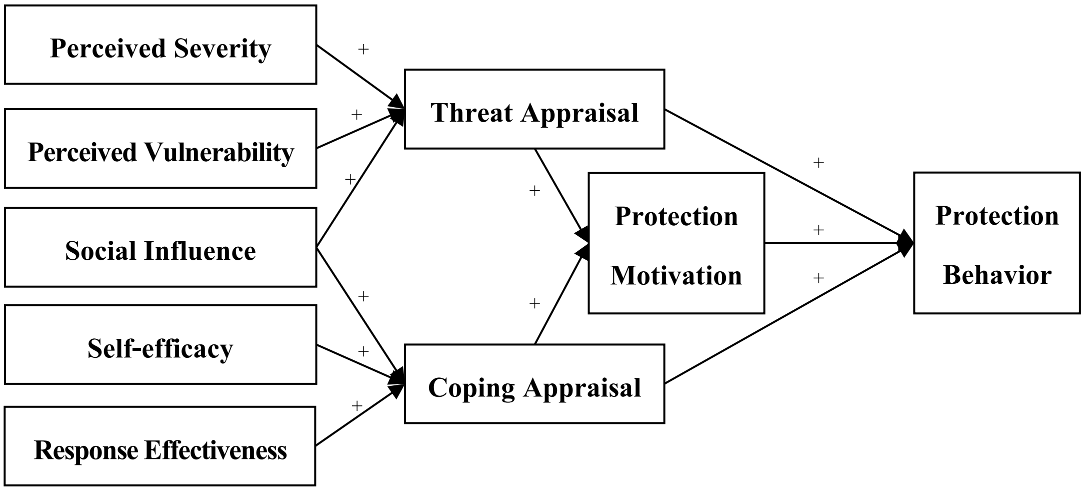

Figure 5 The Proposed Model

5. Conclusion

Objective of this study was to create a model for learning protection behaviors of smartphone users from cyber threats. In this study, the PMT theory was adopted and the related literatures were reviewed in order to identify essential model's constructs and their relationships. Result of this study is useful as it proposed a protection behaviors model of smartphone users which, so far, has not been studied in the literature. The analysis results from testing the proposed model with the empirical data will give us a better understanding of the behaviors of smartphone users in protecting themselves from cyber threats.

References

[1] Rogers, R.W. (1983). **Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation**. In J. Cacioppo & R. Petty (Eds.), Social Psychophysiology. New York: Guilford Press.

[2] Rogers, R.W. **A Protection Motivation Theory of Fear Appeals and Attitude Change**. Journal of Psychology, 1975, 91, pp. 93-114.

[3] Rippetoe, P. and Rogers, R. W. (1987) **Effects of components of protection motivation theory on adaptive and maladaptive coping with a health threat**. Journal of Personality and Social Psychology*, 52, 596–604.*

[4] Anderson, C. L., and Agarwal, R. (2010). **Practicing safe computing: a multi-method empirical examination of home computer user security behavioral intentions.** MIS Quarterly, 34.

[5] Humaidi, N., and Balakrishnan, V. (2012). **The Influence of Security Awareness and Security Technology on Users' Behavior towards the Implementation of Health Information System: A Conceptual Framework**. 2nd International Conference on Management and Artificial Intelligence, 35.

[6] Srisawang, Sirirat; Thongmak, Mathupayas; and Ngarmyarn, Atcharawan.(2015). **Factors Affecting Computer Crime Protection Behavior**. PACIS 2015, pp. 3.

[7] Maddux, J. E.; Rogers, R. W. (1983). **Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change.** Journal of Experimental Social Psychology. **19** (5): 469–479.

[8] Woon, I., Tan, G.-W., and Low, R. (2005). **A Protection Motivation Theory Approach to Home Wireless Security.** ICIS 2005 Proceedings, 31.

[9] Boer, Henk and Seydel, Erwin R. (1996) **Protection Motivation Theory. In: Predicting Health Behaviour: Research and Practice with Social Cognition Models.** Open University Press, Buckingham, pp. 95-120.

[10] Liang, H. and Xue, Y. (2009). **Avoidane of Information Technology Threats: A Theoretical Perspective.** MIS Quarterly, 2009, 33(1), pp. 71 - 90.

[11] Janz, N. K., and Becker, M. H. 1984. **The Health Belief Model: A Decade Later**, Health Education Quarterly (11:1), pp. 1-45.

[12] Rosen stock, I. M. 1974. **The Health Belief Model and Preventive Health Behavior**, Health education Monographs (2), pp. 354-386.

[13] Baskerville, R. 1991a. **Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security**, European Journal of Information Systems (1:2), pp. 121-130.

[14] Baskerville, **R. 1991b. Risk Analysis as a Source of Professional Knowledge**, Computer & Security (10:8), pp. 749-764.

[15] Tu, Z.L. and Yuan, Y.F. (2012). **Understanding User Behavior in Coping with Security Threats of Mobile Device Loss and Theft**. 45th Hawaii International Conference on System Sciences 978-0-7695-4525-7/12.