A Contingent Model of How Fear of External Security Threats Sparks Insiders' Proactive Information Security Behaviors

Early Research Paper

Feng Xu, Mississippi State University

Carol Hsu, Tongji University

Xin (Robert) Luo, University of New Mexico

Merrill Warkentin, Mississippi State University

Abstract

The experience of fear of external security threats has been considered to be generally associated with organizational insiders' protection motivation and behaviors. The most important theoretical foundation to explain insiders' behavioral reactions to fear is the Protection Motivation Theory (PMT). Based on PMT, previous information systems (IS) security researchers have identified antecedents of insiders' security-related behaviors, such as security policy compliance and noncompliance and the adoption of protective technologies. However, previous research has largely overlooked the possibility that insiders' experience of fear can lead to proactive information security behaviors (ISB) that are self-initiated and future-oriented. Motivated thus, this study focuses on two proactive ISB (*voice and individual innovation*) and aims to identify the underlying motivations. Based on Lebel (2017)'s model, this article identifies can-do (*emotional regulation knowledge*) and reason-to (*felt responsibility for constructive change*) motivational factors under which fear of external security threats can lead to insiders' proactive security behaviors. This article contributes to PMT and information security behavior research by specifying when and why fear of security threats leads to insiders' proactive ISB. This study provides important practical suggestions for organizations to understand insiders' behavioral reactions to emotional experience of fear of external security threats, resulting in improved organizational security protection.

Keywords: Fear, PMT, proactive motivation, voice, individual innovation, information security behaviors

1. Introduction

Safeguarding organizational information assets is the primary goal of organizational IS security (Posey et al. 2013; Siponen and Vance 2010). Organizational insiders have been considered as exerting a significant influence on protection of organizational information assets (Willison and Warkentin 2013). Organizational insiders are "full-time employees, part-time employees, temporary workers, and external consultants who have been given authorized access to organizational information" (Posey et al. 2015, p. 180) and can include part-time or seasonal employees (Sharma and Warkentin, 2019). Insiders' behaviors have been considered as determinants of the success of organizational information security initiatives (Da Veiga and Eloff 2010; Ng et al. 2009).

Organizations have taken extensive efforts in motivating insiders' policy compliance behaviors, such as implementing security education, training, and awareness (SETA) programs (D'Arcy et al. 2009), rewarding protective behaviors (Posey et al. 2015), improving message persuasiveness of fear appeal (Boss et al. 2015), and so on. However, organizations continue to struggle with organizational information security protection from increasing security threats. Cybersecurity Ventures predicts that cybercrime will cost business globally over $6 trillion annually by 2021 even if the cumulative spending on cybersecurity will be more than $1 trillion from 2017 to 2021[1].

More importantly, with the evolving change of information technology and security threats, organizations realize the importance of employees' proactive thinking about security decision making. In order to cope with the evolving security threats, organizations should motivate insiders to not only adopt recommend security solutions but also to take proactive actions to help organizations strengthen their overall information security management. For example, employees might speak up about possible organizational vulnerabilities or foresee potential information security issues in the work processes or even develop measures to address future security concerns. Security magazines report that "organizations should consider rewarding or acknowledging individuals who embrace good cyber strategies"[2]. Thus, in this research, our objective is to theorize about the types of proactive ISB and the factors influencing employees' intention in engaging in proactive ISB.

[1] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[2] https://www.securitymagazine.com/articles/89138-employee-behaviors-have-a-direct-impact-on-corporate-cybersecurity-effectiveness

When employees are proactive, they are likely to take actions in advance rather than react to situational factors. Proactive behavior is individual level, self-initiated, and future-oriented (Parker et al. 2006). Employees conduct proactive behavior to make an impact on the self or the organization. In the organizational literature, various antecedents have been proposed for affecting employees' proactive behavior such as flexible role orientation (Parker et al. 2006), fear (Lebel 2016), and role breadth self-efficacy (Fuller Jr et al. 2012). Interestingly, among these factors, we discovered the scholarly argument on theorizing the linkage between negative emotions, such as fear, and proactive actions (Lebel 2016; Lebel 2017; Sonnentag and Starzyk 2015). In IS security literature, fear has become a well-known construct framed to affect insiders' protection motivation and security-related behavior (Johnston and Warkentin 2010; Boss et al. 2015; Posey et al. 2015). Yet there has been little investigation of the mechanisms underlying the relationship between fear and proactive ISB. Given the increasing attention on employees' proactive security behaviors and the proven role of fear in employees' security behaviors, our research objective is to fill the research gap by exploring the relationship between the fear and employees' proactive ISB. To achieve this, we draw on a contingency model of emotion and proactivity developed by Lebel (2017) to develop and empirically test a theoretical model identifying specific factors that determine when fear of security threat is directed toward proactive ISB.

This paper provides several important theoretical and practical contributions to information security research. First, prior IS security study has investigated the effect of fear on insiders' security-related behavior. This paper develops a more detailed understanding of the effect of fear on insiders' proactive ISB. Second, the effect of fear on insiders' behavior varies (Lebel 2017; Oh and Farh 2017). This paper contributes to PMT in IS security research by specifying when fear of external security threat produces proactive ISB. Third, it is critical to identify potential psychological processes between fear and proactive ISB. The understanding of the psychological process provides important value to organizational information security management. Addressing this question provides practical insight into how the organization can effectively manage insiders' experience of fear and increase organizational information security policy (ISP) effectiveness in the presence of external security threats.

2. Literature Review

2.1 Previous Research on Fear and Security-related Behaviors

Previous IS security research has emphasized the importance of affect (emotions) in influencing employees' security behaviors. For example, D'Arcy and Lowry (2019) investigated the effects of positive and negative affect on employees' daily ISP compliance. Except aggregate emotional experience, there are few IS security studies estimating the effects of discrete emotions. For example, D'Arcy and Teh (2019) found that employees' experience of frustration and fatigue arising from security-related stress might negatively influence employees' ISP compliance and Ormond, et al (2019) similarly showed that frustration can contribute to security policy violation. Burns et al. (2019) investigated effects of four discrete emotions (happiness, interest, sadness, and anxiety) on employees' precaution taking through psychological capital and psychological distancing. Based on appraisal tendency framework (ATF), Xu et al. (2020) compared the effects of two discrete emotions, fear and anger, on employees' computer-related deviant behavior through perceived formal and informal sanctions.

Table 1. Research Summary of Fear and Security-related Behavior

Author	Theory	Mediation variable	Security-related behaviors	Proactive?
Boss et al. (2015)	PMT	Protection motivation	Backup; anti-malware software adoption	No
Posey et al. (2015)	PMT	Protection motivation	Past protection-motivated behaviors	No
Burns et al. (2017)	PMT	Protection motivation	Protection-motivated behaviors	No
Xu et al. (2020)	ATF	Perceived formal and informal sanction	Computer-related deviant behavior	No

Fear, as a negative-valence and high arousal emotion, has been investigated in previous IS security research and has been considered to be able to activate individuals' current or future actions. PMT is the dominant theory to explain employees' security behavioral reactions to fear appeals (Herath and Rao 2009; Hina et al. 2019; Ifinedo 2012; Siponen et al. 2014; Vance et al. 2012; Wall and Warkentin 2019). PMT aims to "persuade people to follow the communicator's recommendations" (Floyd et al. 2000, p. 411). Based on PMT, previous research empirically estimated the positive effect of fear on employees' protection motivation and adoption of recommended security behavior, such as information security policy compliance and protective technologies adoption (Boss et al. 2015; Burns et al. 2017; Posey et al. 2015). Table 1 shows the summary of recent research which has empirically investigated the relationship between fear and security-related behaviors.

Although PMT is the dominant theory to explain insiders' security behavioral reactions to fear, previous research mostly investigated employees' adoption of recommended protective behaviors which can be regarded as *in-role security behaviors*. It is important to emphasize that proactive behavior is different than in-role behavior. Previous research found that "The key criterion for identifying proactive behavior is not whether it is in-role or extra-role, but rather whether the employee anticipates, plans for, and attempts to create a future outcome that has an impact on the self or environment" (Grant and Ashford 2008, p. 9). Proactive behavior focuses on self-initiated action that refers to doing something without being told or without an explicit role requirement (Parker et al. 2006). Thus, we characterize adoption of recommended protective behaviors communicated by the organization to be *non-proactive ISB*. We found no work yet extending the PMT to examine proactive ISB. In particular, there already exists the theoretical foundation that explicates the role of fear in invoking employees' proactivity in organizations (Lebel 2017). This research extends PMT to investigate employees' proactive security behavior with a contingency model of fear and proactivity.

2.2 The Definition of Proactive Information Security Behavior

Proactive behavior comprises "proactive work behavior, proactive strategic behavior, and proactive person-environment fit behavior" (Parker and Collins 2010, p. 633). In this paper, we focus on proactive work behavior which is more related to employees' daily workplace behavior. According to the definition of proactive work behavior (Crant 2000), we define proactive ISB as anticipatory and self-initiated behavior aimed to prevent security threats and improve the situation or the self. We argue that employees who experience fear of external security threats can be motivated to conduct proactive ISB.

In the IS security context, we consider two types of proactive ISB: voice and individual innovation. We select these two behaviors for two reasons. First, previous studies have identified four types of proactive work behaviors, including "taking charge, voice, individual innovation, and problem prevention" (Parker and Collins 2010, p. 636). Taking charge indicates that individuals can take control and change the procedures in the workplace. Problem prevention indicates that individuals try to find the root cause of things. These two types of behaviors require more control and technical capacities and are not appropriate for organizational insiders in the context of information security.

Second, employee voice and individual innovation, regarded as proactive work behavior (Detert and Burris

2007), have been investigated in IS security research (Hsu et al. 2015; Jensen et al. 2017). Voice indicates individuals' actions to propose recommendations or suggestions for making improvements on organizational security protection (Hsu et al. 2015). Individual innovation has not been estimated in prior IS security research. However, Jensen et al. (2017) found that individuals can construct new strategies and mental models to detect phishing messages under mindfulness training programs. It indicates that individuals might be able to generate new ideas or approaches to prevent the reoccurrence of security threats. However, scholars lack a systematic understanding of why and when fear of external security threats leads to these proactive ISB.

3. Theoretical Foundation and Hypotheses

Fear is an unpleasant and high activated discrete negative emotion (Smith and Ellsworth 1985). Individuals experience fear if they appraise the situation or negative events as uncertain and loss of control. The dominant action tendency for fear of security threats is associated with protection motivation and behavior. Following this, previous research suggested that employees who experience fear of security threat will be likely to comply with security policy or adopt protective technologies (Boss et al. 2015; Burns et al. 2017; Posey et al. 2015). However, other research found that fear of external threats can invoke employees' voice when they perceive a high supervisor openness (Lebel 2016). Thus, individuals' behavioral reactions to discrete emotions, such as fear, depend on "the joint occurrence of an emotion and specific external or internal stimulus conditions" (Roseman et al. 1994, p. 216). We integrate PMT and Lebel (2017)'s contingent model to show how fear leads to different behavioral reactions under specific conditions.

3.1 Protection Motivation Theory

The dominant theory to explain individuals' behavioral reactions to the experience of fear is PMT. PMT suggested that individuals make security decisions through two appraisals of the situation: threat appraisal and coping appraisal (Floyd et al. 2000). In the threat appraisal process, individuals' perception of severity of and vulnerability to threats and fear will induce their protection motivation. In the coping appraisal process, individuals will assess their perception of response efficacy, self-efficacy and response cost. When response efficacy and self-efficacy outweigh response cost, individuals will tend to engage in protection motivation.

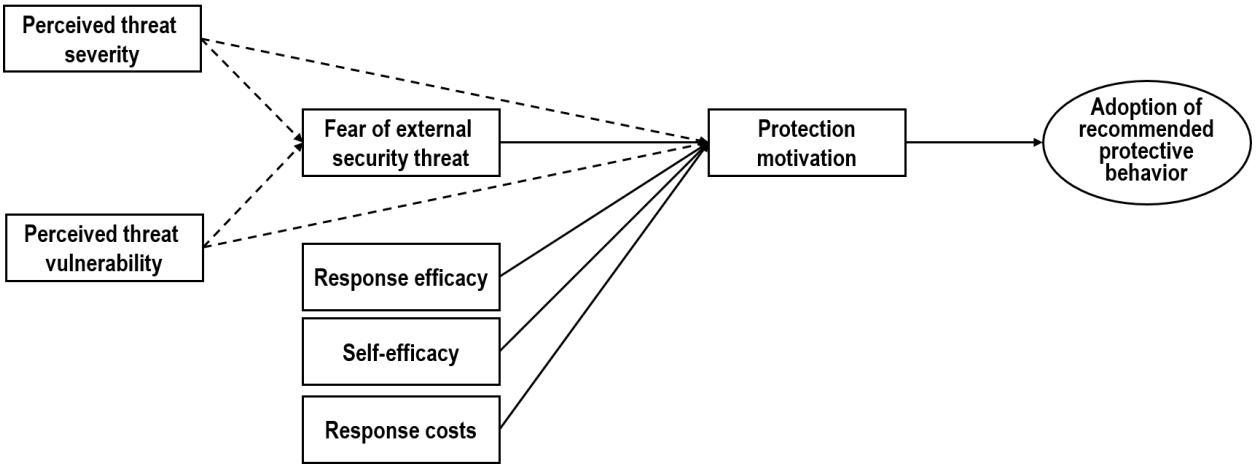

Figure 1. Fundamental PMT Model

In terms of threat appraisal, fear is important and different with fear appeals which are widely used in previous research (Boss et al. 2015; Burns et al. 2017; Posey et al. 2015). Previous research defines fear as "relational construct, aroused in response to a situation that is judged as dangerous and toward which protective action is taken" (Rogers 1975, p. 96). Boss et al. (2015) argued that "measuring fear helps researchers know whether the threat severity and vulnerability generate an appropriate level of fear" (p. 841) and found that the effect of threat appraisals on protection motivation is through fear. So we don't consider perceived threat severity and vulnerability in our model but regard them as the trigger of insiders' experience of fear. According to PMT, individuals' experience of fear and coping appraisal invoke individuals' protection motivation and then individuals transfer their protection motivation to adoption of recommended protective behavior, such as adoption of anti-malware software (Boss et al. 2015). The fundamental PMT model is shown in Figure 1.

3.2 The Contingent Model of Fear and Proactivity

Although PMT provides critical understanding of individuals' behavioral reactions to fear, it is still unknown how individuals can transfer their protection motivation to proactive ISB. Lebel (2017) proposed a framework for understanding individuals' proactive behaviors when they experienced fear. The authors identified specific *energized-to* (fear), *can-do* (emotional regulation knowledge), and *reason-to* (felt responsibility to act) motivation. The framework suggests that fear provides energy for individuals to take protective efforts and can-do motivation and reason-to motivation moderate the relationship between protective efforts and individuals' proactive behavior. The contingent model is shown in Figure 2.

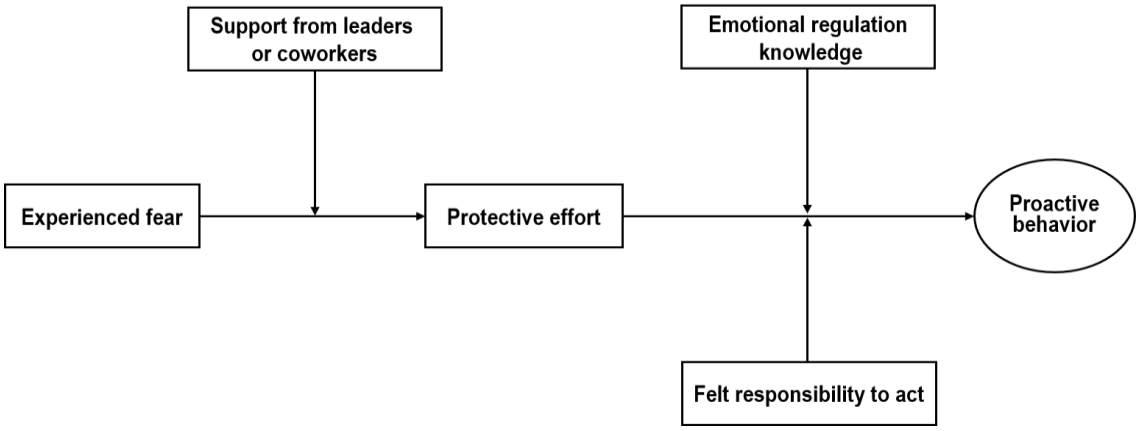

Figure 2. Contingent Model in Lebel (2017)

Table 2. Explanation of Constructs

Lebel (2017)	Explanation	In this study	Sample item
Experienced fear	Negatively valenced and high-arousal emotion	Experienced fear of external security threat	I am worried about the prospect of losing files.
Support from leaders or coworkers	The presence of supportive cues from leaders or coworkers	Supervisor support for security protection	My supervisor praises me when I adopt proper information security practices
Protective effort	Increased focus on a threat or readiness for defensive action	Protection motivation	I intend to expend effort to protect my organization from its information security threats
Emotional regulation knowledge	"One's awareness of the most effective strategies to modify and nurture emotions in particular situations" (Côté et al. 2011, p. 1074)	Emotional regulation knowledge	I control my emotions by changing the way I think about the situation I'm in
Felt responsibility to act	"A psychological state that reflects one's willingness to make improvements, deal with problem, and put extra effort" (Lebel 2017, p. 198)	Felt responsibility for construct change	I feel a personal sense of responsibility to bring about change on security protection
Proactive behavior	"A self-initiated and future-oriented action that aims to change and improve the situation or oneself" (Parker et al. 2006, p. 636)	Proactive ISB -individual innovation - voice	- Search out new security protective software, technologies and/or ideas? - Speak up in the organization with ideas for new strategies or changes in information security policies.

In the context of information security, fear of external security threats can be considered as an energized-to motivation for insiders' proactive security behavior. Fear, as a negative emotion, can activate individuals' protective effort, such as increased attention to the threat (Izard and Ackerman 2000) or readiness for defensive action (Frijda 1986). Readiness for defensive action refers to individuals' readiness to interact with the environment and engage in protective actions (Frijda et al. 1989). Previous IS security research has cast action readiness as individuals' intention to conduct security behavior (Kim et al. 2016). We argue that protection motivation, defined as "an intervening variable that has the typical characteristics of a motive: it arouses, sustains, and directs activity" (Rogers 1983, p. 158), shows individuals' readiness for defensive action. For example, Boss et al. (2015) suggested that fear increases insiders' protective motivation which leads to their protective security behavior, such as security policy compliance. Therefore, we consider that, in fear, the energized-to-motivation takes the form of protective effort, including protection motivation.

Emotional regulation knowledge can be regarded as can-do proactive motivation (Lebel 2017) and felt responsibility for constructive change can be considered as reason-to proactive motivation (Fuller Jr et al. 2012) which direct protective efforts towards proactive behaviors. Emotional regulation knowledge indicates individual differences in "awareness of the most effective strategies to modify and nurture emotions in particular situations" (Côté et al. 2011, p. 1074). Emotional regulation knowledge has been regarded to be related to subordinates' proactive coping - "where subordinates forgo an immediate reaction in favor of strategies that anticipate, avoid, and minimize the impact of future like events" (Oh and Farh 2017, p. 219). Felt responsibility to act is considered as "a psychological state that reflects one's willingness to make improvements, deal with problem, and put extra effort". (Lebel 2017, p. 198). This reason-to proactive motivation emphasizes individuals' responsibility to change the situation. The change-oriented behavior is likely to arise from felt responsibility for constructive change (Fuller Jr et al. 2012).

Based on PMT and Lebel (2017), we assert that fear of external security threats can lead to different security behaviors under different conditions. PMT suggests that experience of fear and coping appraisals influence insiders' protection motivation. Lebel (2017) suggested that support from supervisor moderates the relationship between fear and insiders' protective effort. However, what types of security behaviors individuals will conduct depends on can-do and reason-to motivation. Based on PMT, protection motivation directly influences non-

proactive ISB, such as adoption of anti-malware software. However, whether individuals will transfer their protection motivation to proactive ISB, such as individual innovation and voice, depends on individuals' emotional regulation knowledge and felt responsibility for constructive change. Our resulting research model is shown in Figure 3.

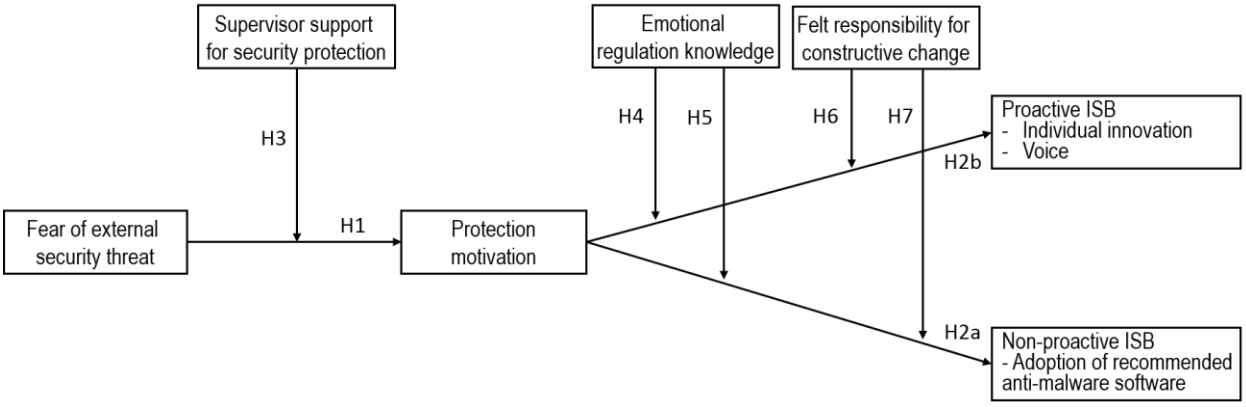

Figure 3. A Research Model of Fear and Security-related Behavior

3.3 Fear and Protection Motivation

PMT suggests that insiders are likely to take protection-motivated behavior when they perceived threats (Johnston and Warkentin 2010; Johnston et al. 2015). There are two appraisal processes from PMT: threat appraisal and coping appraisal. Fear, as a core part of PMT, has been less empirically investigated in previous research. Previous research found that "evaluating the efficacy of a fear appeal without measuring fear itself is problematic" (Boss et al. 2015, p. 859). This paper aims to identify how fear rather than perceived threats invokes proactive security behavior. Considering fear as a core partial mediator between perceived threat and protective motivation (Boss et al. 2015), this paper doesn't consider perceived threat severity and perceived threat vulnerability in the research model.

Lebel (2017) proposed that experienced fear can motivate individuals' protective efforts. Lebel argued that fear, as an unpleasant and high activated negative emotion, can improve individuals' psychological resources to take action (Cosmides and Tooby 2000). This argument is also supported by the affect-as-information theory which suggested that affect influences people's information processing (Carver 2003). Individuals who experienced negative emotions from current situation have the motivation to put effort to work on it. PMT also suggests that fear can lead to individuals' protection motivation which finally influences individuals' adoption of recommended action. Previous research has empirically investigated the positive relationship between fear

and protection motivation, and the predictive effect of protection motivation on non-proactive ISB, such as adoption of recommended anti-malware software (Boss et al. 2015; Burns et al. 2017; Posey et al. 2015). However, we argue that protection motivation has no effect on proactive ISB because individuals will take proactive actions only in the condition in which the emotional regulation knowledge or felt responsibility for constructive change is high. Thus, we hypothesize:

H1*: Fear of external security threats positively influences insiders' protection motivation*

H2a*: Protection motivation positively influences insiders' non-proactive ISB*

H2b*: Protection motivation has no significant effect on insiders' proactive ISB*

Previous research found that employees experiencing fear tend to deal with the uncertainty by seeking support from managers or coworkers about how to respond to the negative events (Gino et al. 2012; Taylor 2006). This organizational support can increase fearful employees' protective efforts (Chan and McAllister 2014). Organizational support can increase employees' efficacy which increases their self-protective efforts (Lebel 2017). When employees get support from organizations or supervisors, they increase their motivation for protecting themselves or others. For example, previous research suggests that fearful individuals are more likely to respond to disease actively when they have a high efficacy to act (Witte and Allen 2000). In the case of fear of external security threats, insiders who have supervisor support for security protection can increase their confidence in dealing with security threats and thereby increase their protection motivation (Puhakainen and Siponen 2010).

H3*: Perceived supervisor support positively moderates the positive relationship between fear of external security threat and protection motivation*

3.4 Protection Motivation and Proactive and Non-proactive ISB

In our context of fear arising from external security threats, individuals might take action proactively if they can do and have the reason to do. According to the notion that individuals' responses to emotions are situationally contingent, we propose a research model explaining when fear sparks proactivity. Proactivity indicates that individuals intend to change the situation and to be constructive (Grant and Ashford 2008). Previous research has investigated a number of proactive behaviors, such as speaking up (Detert and Burris 2007), seeking feedback (Ashford 1986), or new policies introduction (Frese and Fay 2001).

Based on information security literature, this study proposed two proactive ISB, individual innovation and voice. Following the model of Lebel (2017), there are two motivational states turning protective efforts to proactive behavior, including can-do, reason-to motivation. First, "can-do" motivation emphasizes individuals' evaluation of whether it is possible to conduct proactivity (Cai et al. 2019). Second, "reason-to" motivation concentrates on individuals' assessment of whether it is worthwhile for goal achievement (Grant and Rothbard 2013).

3.4.1 Can-do motivation

Although fear and supervisor support for security protection can increase insiders' protection motivation, insiders still need to regulate their negative emotions, such as fear, to act proactively. Lebel (2017) suggested that emotional regulation knowledge can regulate individuals' experience of fear and direct individuals' protective effort toward proactive behavior. Insiders with high emotional regulation knowledge tend to take a proactive approach.

In the context of information security, we argue that insiders with high emotional regulation knowledge might direct their protection motivation toward proactive ISB. Individuals with high emotional regulation knowledge will be more likely to reappraisal the situation and regulate the negative affective experience (Rupp et al. 2008). Emotional regulation knowledge can regulate insiders' negative experiences of fear and motivate insiders to take regulated security behaviors. Insiders with high emotional regulation knowledge will focus more on positive and long-term outcomes (Mayer and Salovey 1995) and take a more adaptive or strategic approach (Oh and Farh 2017) and thus perceive their individual innovation and voice behavior as an adaptive way to mitigate threats to the organization.

Compared with proactive ISB, non-proactive ISB, such as adoption of recommended anti-malware software, is more passive and less related to proactive motivation. Previous studies have empirically tested the positive relationships between protection motivation and insiders' protective behaviors, such as ISP compliance (Hina et al. 2019; Ifinedo 2012; Johnston et al. 2015; Siponen et al. 2014; Vance et al. 2012; Wall and Warkentin 2019), adoption of protective technologies (Johnston et al. 2015; Lee 2011) or implementation of security practice (Burns et al. 2017; Posey et al. 2015). However, previous research has not identified conditional factors in this relationship. Lebel (2017) suggested that the relationship between protective effort and proactive behavior is

negative when individuals' emotional regulation knowledge is low. We argue that individuals with low emotional regulation knowledge are less likely to take proactive approach and more likely to direct protection motivation to non-proactive behavior, such as adopting the recommended anti-malware software.

***H4**: Emotional regulation knowledge moderates the relationship between protection motivation and proactive ISB (individual innovation & voice) such that there is a positive relationship when emotional regulation knowledge is high and there is no relationship when emotional regulation knowledge is low.*

***H5**: Emotional regulation knowledge moderates the relationship between protection motivation and non-proactive ISB (adoption of recommended anti-malware software) such that the positive relationship is enhanced when emotional regulation knowledge is low.*

3.4.2 Reason-to motivation

Lebel (2017) considered felt responsibility to act as a reason-to proactive motivation and suggested that individuals who felt a responsibility to act might direct protective effort to proactive behavior. Although previous IS security research found the effect of personal responsibility on individuals' security behaviors (Anderson and Agarwal 2010; Van Schaik et al. 2017), personal responsibility does not mean that insiders will hold themselves responsible for the change. For example, insiders with a responsibility towards protecting an organization's information security policy may have a reason to conduct ISP compliance behavior (Yazdanmehr and Wang 2016). Felt responsibility for constructive change reflects "the extent to which an individual feels personal responsibility for continually redefining performance (i.e., doing things better), rather than solely performing his or her own task well according to current performance standards (i.e., doing the job right)" (Fuller et al. 2006, p. 1092). Thus, insiders are more likely to direct protective effort to proactive behavior when they felt high responsibility for constructive change.

We argue that felt responsibility for constructive change moderates the relationship between protection motivation and insiders' proactive ISB. Lebel (2017) suggested that individuals need a strong motivational reason to act proactively rather than adopt avoidance behavior. When insiders experienced fear, they might have the willingness to take protective action. However, insiders need reason-to proactive motivation to transfer their willingness to proactive action (Schilpzand et al. 2015). If individuals perceive that it is their responsibility for constructive change, they are likely to explore improvement opportunities (Fuller et al. 2006). We suggest that

insiders will have a powerful reason to take proactive ISB when they feel high responsibility for constructive change. Insiders are likely to view individual innovation and voice behaviors as necessary to change their current situation and improve organizational security protection. In contrast, when individuals perceive low felt responsibility to act, the relationship between protective effort and proactive behavior is negative (Lebel 2017). That is to say, under low felt responsibility for construct change, individuals' protection motivation is more likely to cause non-proactive behavior. Individuals are likely to direct protection motivation to non-proactive ISB when they have a low responsibility for constructive change. Thus, we hypothesize that:

H6*: Felt responsibility for constructive change moderates the relationship between protection motivation and proactive ISB (individual innovation & voice) such that there is a positive relationship when insiders' felt responsibility for constructive change is high and there is no relationship when insiders' felt responsibility for constructive change is low.*

H7*: Felt responsibility for constructive change moderates the relationship between protection motivation and non-proactive ISB (adoption of recommended anti-malware software) such that the positive relationship is enhanced when insiders' felt responsibility for constructive change is low.*

4. Proposed Research Method

We propose using the survey method to collect data from individual subjects. The survey instrument will be pretested and refined based on the guidelines in the literature. To reach general organizational insiders, Amazon Mechanical Turk will be used to recruit the respondents by giving them a small incentive. All respondents will be presented a security-related scenario that describes a security threat event occurred in an organization. For example:

> *You are an employee of a large corporation. Recently, something happened to your organization. "An attack, which started on Friday, locked people out of their computers and encrypts their files, demanding they pay up to $300 in bitcoin -- a price that doubles after three days -- to receive a decryption key or risk losing their important files forever. What's worse is the malware also behaves like a worm, potentially infecting computers and servers on the same network."*

– From https://www.cnet.com/how-to/wannacry-ransomware-how-to-protect-your-pc/

After reading the scenario, the respondents will be asked to answer questions regarding the extent to which they felt fearful, protection motivation, perceptions of supervisor support for security protection, emotional regulation knowledge, and responsibility for constructive change, along with intention to engage in proactive and non-proactive ISB and demographic information.

References

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp. 613-643.

Ashford, S. J. 1986. "Feedback-Seeking in Individual Adaptation: A Resource Perspective," *Academy of Management Journal* (29:3), pp. 465-487.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837-864.

Burns, A., Posey, C., Roberts, T. L., and Lowry, P. B. 2017. "Examining the Relationship of Organizational Insiders' Psychological Capital with Information Security Threat and Coping Appraisals," *Computers in Human Behavior* (68), pp. 190-209.

Burns, A., Roberts, T. L., Posey, C., and Lowry, P. B. 2019. "The Adaptive Roles of Positive and Negative Emotions in Organizational Insiders' Security-Based Precaution Taking," *Information Systems Research* (30:4), pp. 1228-1247.

Cai, Z., Parker, S. K., Chen, Z., and Lam, W. 2019. "How Does the Social Context Fuel the Proactive Fire? A Multilevel Review and Theoretical Synthesis," *Journal of Organizational Behavior* (40:2), pp. 209-230.

Carver, C. 2003. "Pleasure as a Sign You Can Attend to Something Else: Placing Positive Feelings within a General Model of Affect," *Cognition and Emotion* (17:2), pp. 241-261.

Chan, M. E., and McAllister, D. J. 2014. "Abusive Supervision through the Lens of Employee State Paranoia," *Academy of Management Review* (39:1), pp. 44-66.

Cosmides, L., and Tooby, J. 2000. "Evolutionary Psychology and the Emotions," in *Handbook of Emotions (2nd Ed.),* M. Lewis, and J. M. Haviland-Jones (eds.), New York: Guilford Press, pp. 91-115.

Côté, S., Decelles, K. A., Mccarthy, J. M., Van Kleef, G. A., and Hideg, I. 2011. "The Jekyll and Hyde of Emotional Intelligence: Emotion-Regulation Knowledge Facilitates Both Prosocial and Interpersonally Deviant Behavior," *Psychological Science* (22:8), pp. 1073-1080.

Crant, J. M. 2000. "Proactive Behavior in Organizations," *Journal of Management* (26:3), pp. 435–462.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

D'Arcy, J., and Lowry, P. B. 2019. "Cognitiv-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study," *Information Systems Journal* (29:1), pp. 43-69.

D'Arcy, J., and Teh, P.-L. 2019. "Predicting Employee Information Security Policy Compliance on a Daily Basis: The Interplay of Security-Related Stress, Emotions, and Neutralization," *Information & Management* (56:7), Article 103151.

Da Veiga, A., and Eloff, J. H. 2010. "A Framework and Assessment Instrument for Information Security Culture," *Computers & Security* (29:2), pp. 196-207.

Detert, J. R., and Burris, E. R. 2007. "Leadership Behavior and Employee Voice: Is the Door Really Open?," *Academy of Management Journal* (50:4), pp. 869-884.

Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. 2000. "A Meta-Analysis of Research on Protection

Motivation Theory," *Journal of Applied Social Psychology* (30:2), pp. 407-429.

Frese, M., and Fay, D. 2001. "Personal Initiative: An Active Performance Concept for Work in the 21st Century," *Research in Organizational Behavior* (23), pp. 133-187.

Frijda, N. H. 1986. *The Emotions*, Cambridge, England: Cambridge University Press.

Frijda, N. H., Kuipers, P., and Ter Schure, E. 1989. "Relations among Emotion, Appraisal, and Emotional Action Readiness," *Journal of Personality and Social Psychology* (57:2), pp. 212-228.

Fuller, J. B., Marler, L. E., and Hester, K. 2006. "Promoting Felt Responsibility for Constructive Change and Proactive Behavior: Exploring Aspects of an Elaborated Model of Work Design," *Journal of Organizational Behavior* (27:8), pp. 1089–1120.

Fuller Jr, J. B., Marler, L. E., and Hester, K. 2012. "Bridge Building within the Province of Proactivity," *Journal of Organizational Behavior* (33:8), pp. 1053-1070.

Gino, F., Brooks, A. W., and Schweitzer, M. E. 2012. "Anxiety, Advice, and the Ability to Discern: Feeling Anxious Motivates Individuals to Seek and Use Advice," *Journal of Personality and Social Psychology* (102:3), pp. 497-512.

Grant, A. M., and Ashford, S. J. 2008. "The Dynamics of Proactivity at Work," *Research in Organizational Behavior* (28), pp. 3-34.

Grant, A. M., and Rothbard, N. P. 2013. "When in Doubt, Seize the Day? Security Values, Prosocial Values, and Proactivity under Ambiguity," *Journal of Applied Psychology* (98:5), pp. 810-819.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Hina, S., Selvam, D. D. D. P., and Lowry, P. B. 2019. "Institutional Governance and Protection Motivation: Theoretical Insights into Shaping Employees' Security Compliance Behavior in Higher Education Institutions in the Developing World," *Computers & Security* (87: November), Article 101594.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., and Lowry, P. B. 2015. "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness," *Information Systems Research* (26:2), pp. 282-300.

Ifinedo, P. 2012. "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security* (31:1), pp. 83-95.

Izard, C. E., and Ackerman, B. P. 2000. "Motivational, Organizational, and Regulatory Functions of Discrete Emotions," in *Handbook of Emotions (2nd Ed.),* M. Lewis, and J. M. Haviland-Jones (eds.), New York: Guilford Press, pp. 253-264.

Jensen, M. L., Dinger, M., Wright, R. T., and Thatcher, J. B. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *Journal of Management Information Systems* (34:2), pp. 597-626.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Johnston, A. C., Warkentin, M., and Siponen, M. T. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.

Kim, J. J., Park, E. H. E., and Baskerville, R. L. 2016. "A Model of Emotion and Computer Abuse," *Information & Management* (53:1), pp. 91-108.

Lebel, R. D. 2016. "Overcoming the Fear Factor: How Perceptions of Supervisor Openness Lead Employees to

Speak up When Fearing External Threat," *Organizational Behavior & Human Decision Processes* (135), pp. 10-21.

Lebel, R. D. 2017. "Moving Beyond Fight and Flight: A Contingent Model of How Anger and Fear Spark Proactivity," *Academy of Management Review* (42:2), pp. 190-206.

Lee, Y. 2011. "Understanding Anti-Plagiarism Software Adoption: An Extended Protection Motivation Theory Perspective," *Decision Support Systems* (50:2), pp. 361-369.

Mayer, J. D., and Salovey, P. 1995. "Emotional Intelligence and the Construction and Regulation of Feelings," *Applied and Preventive Psychology* (4:3), pp. 197-208.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. C. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (46:4), pp. 815-825.

Oh, J., and Farh, C. 2017. "An Emotional Process Theory of How Subordinates Appraise, Experience, and Respond to Abusive Supervision over Time," *Academy of Management Review* (42:2), pp. 207-232.

Ormond, D., Warkentin, M., and Crossler, R. E. 2019. "Integrating Cognition with an Affective Lens to Better Understand Information Security Policy Compliance," *Journal of the Association for Information Systems* (20:12), pp. 1794-1843.

Parker, S. K., and Collins, C. G. 2010. "Taking Stock: Integrating and Differentiating Multiple Proactive Behaviors," *Journal of Management* (36:3), pp. 633-662.

Parker, S. K., Williams, H. M., and Turner, N. 2006. "Modeling the Antecedents of Proactive Behavior at Work," *Journal of Applied Psychology* (91:3), pp. 636-652.

Posey, C., Roberts, T., Lowry, P. B., Bennett, B., and Courtney, J. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS Quarterly* (37:4), pp. 1189-1210.

Posey, C., Roberts, T. L., and Lowry, P. B. 2015. "The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets," *Journal of Management Information Systems* (32:4), pp. 179-214.

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757-778.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91:1), pp. 93-114.

Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in *Social Psychophysiology: A Sourcebook,* J. T. Cacioppo, and R. E. Petty (eds.), New York: Guilford, pp. 153-176.

Roseman, I. J., Wiest, C., and Swartz, T. S. 1994. "Phenomenology, Behaviors, and Goals Differentiate Discrete Emotions," *Journal of Personality and Social Psychology* (67:2), pp. 206-221.

Rupp, D. E., McCance, A. S., Spencer, S., and Sonntag, K. 2008. "Customer (in) Justice and Emotional Labor: The Role of Perspective Taking, Anger, and Emotional Regulation," *Journal of Management* (34:5), pp. 903-924.

Schilpzand, P., Hekman, D. R., and Mitchell, T. R. 2015. "An Inductively Generated Typology and Process Model of Workplace Courage," *Organization Science* (26:1), pp. 52-77.

Sharma, S., and Warkentin, M. 2019. "Do I Really Belong?: Impact of Employment Status on Information Security Policy Compliance," *Computers & Security*, (87), paper 101397.

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

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487-502.

Smith, C. A., and Ellsworth, P. C. 1985. "Patterns of Cognitive Appraisal in Emotion," *Journal of Personality and Social Psychology* (48:4), pp. 813-838.

Sonnentag, S., and Starzyk, A. 2015. "Perceived Prosocial Impact, Perceived Situational Constraints, and Proactive Work Behavior: Looking at Two Distinct Affective Pathways," *Journal of Organizational Behavior* (36:6), pp. 806-824.

Taylor, S. E. 2006. "Tend and Befriend: Biobehavioral Bases of Affiliation under Stress," *Current Directions in Psychological Science* (15:6), pp. 273-277.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., and Kusev, P. 2017. "Risk Perceptions of Cyber-Security and Precautionary Behaviour," *Computers in Human Behavior* (75), pp. 547-559.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3-4), pp. 190-198.

Wall, J. D., and Warkentin, M. 2019. "Perceived Argument Quality's Effect on Threat and Coping Appraisals in Fear Appeals: An Experiment and Exploration of Realism Check Heuristics," *Information & Management* (56:8), Article 103157.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1-20.

Witte, K., and Allen, M. 2000. "A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns," *Health Education & Behavior* (27:5), pp. 591-615.

Xu, F., Luo, X. R., and Hsu, C. 2020. "Anger or Fear? Effects of Discrete Emotions on Employee's Computer-Related Deviant Behavior," *Information & Management* (57:3), Article 103180.

Yazdanmehr, A., and Wang, J. 2016. "Employees' Information Security Policy Compliance: A Norm Activation Perspective," *Decision Support Systems* (92), pp. 36-46.