Identifying the Neural Correlates of Protection Motivation for Secure IT Behaviors

Merrill Warkentin, Eric A. Walden, Allen C. Johnston, Detmar W. Straub

Corresponding author: m.warkentin@msstate.edu

A central goal of managing information systems is the assurance of the information's security – its confidentiality, integrity, and accessibility – which comprises a plethora of activities to, among other things, implement and maintain technical, behavioral, and economic controls to prevent and deter threats arising from internal and external sources which may originate from human or nonhuman sources. Extensive research has pointed to the insider, typically the employee, as a primary source of threat to the information system's security. Employee actions that threaten the security of organizational information resources may be accidental or they may be volitional but not malicious. (Willison & Warkentin, 2012).

Straub (2009) called for more creative research approaches to understanding the cognitive and affective processes of both so-called "white hat" and "black hat" IS security policy violators. The focus of the present study is the "white hat" insider (employee, student, contractor, agent, customer) who is expected by the organization to comply with various IT security policies and procedures, including engaging in protective behaviors such as backing up important data, avoiding suspect emails and websites, scanning for malware, selecting strong passwords that cannot be easily guessed, maintaining up-to-date software (patch management), encrypting mobile data, and other activities. Insiders are typically influenced to engage in these activities by managers through the use of security education, training, and awareness (SETA) campaigns and by the use of persuasive communications, including fear appeals (Johnston & Warkentin, 2010). Fear appeals seek to increase the message recipient's perceptions of a specific threat's severity and one's susceptibility or vulnerability to it (known as "threat appraisal"), while also seeking to boost the recipient's efficacy levels by recommending a response (response efficacy) that is said to be easy to perform (self-efficacy). The latter mediating process is termed "coping appraisal." This complex cognitive and affective process, depicted in Figure 1, is the focus of our investigation.

For fear appeals to be effective, the message must manipulate the neural regions responsible for cognitively processing perceptions of threat and efficacy. Threat appraisal is a cognitive assessment of vulnerability which may or may not be associated with the intense affective response to immediate danger (the "fight or flight" response that is activated by neural activity in the amygdala, and which is characterized by a massive release of adrenaline). Coping appraisal is a parallel cognitive mediating process in which the message recipient engages in an assessment of his or her own ability to cope with the threat (self-efficacy) and of the efficacy of the recommended response. The theory, supported by extensive research in several domains, suggests that in order for the message recipient to form the intention to engage in the recommended protective behavior(s), he or she must believe that "it is bad, it can happen to me, but this response works, and I can do it," while also determining that the response costs do not impose a prohibitive constraint. We seek to establish the first efforts at understanding the neural activities associated with each of these cognitive mediating processes.

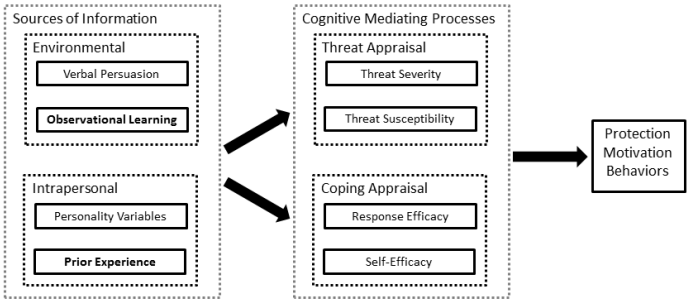

FIG 1: PROTECTION MOTIVATION PROCESS
(Adapted from Floyd, et al. 2000)

In order to understand the proximal biological sources of these cognitive mediating processes in the context of individual assessment of IS security threats and the recommended responses, we adopt a functional magnetic resonance imaging (fMRI) design to isolate and assess the individual neural processes associated with exposure to the stimuli components of IS security fear appeals. Subjects will be exposed to stimuli consisting of ten sets of five screens. After fixation is presented, a general IT statement is displayed (e.g. "Computer cases are sometimes made of plastic."). Third is an IT threat (e.g. "USB drives have recently been stolen.") and fourth is a recommended IT response (e.g. "Encrypting USB drives keep data safe"). On the fifth screen, subjects indicate their intention to engage in the response behavior. We then investigate whether there are neural correlates of IT threats and IT responses, as compared to the reaction to simply reading general IT statements (the baseline). Further, we investigate whether fear appeals really invoke *fear* in the sense of activating known fear areas of the brain such as the amygdala and hypothalamus, or whether the threat appraisal process activates other centers of activity. We expect this initial knowledge will enable deeper understanding of IT user decision making in the context of protection motivation.

REFERENCES

- Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. 2000. "A Meta-Analysis of Research on Protection Motivation Theory," *Journal of Applied Psychology* (30:2), pp. 407-429.
- Johnston, A.C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.
- Straub, D. W. 2009. "Black Hat, White Hat Studies in Information Security," Keynote Address, The Dewald Roode Workshop on Information Systems Security Research, Cape Town, South Africa.
- Willison, R., and Warkentin, M. 2012. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly*, forthcoming.