Spring 2010

Protection-motivated behaviors of organizational insiders

Michael C. Posey
Louisiana Tech University

PROTECTION-MOTIVATED BEHAVIORS OF ORGANIZATIONAL INSIDERS

by

Michael C. Posey, B.A., M.B.A.

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree of
Doctor of Business Administration

COLLEGE OF BUSINESS
LOUISIANA TECH UNIVERSITY

May, 2010

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

LOUISIANA TECH UNIVERSITY

THE GRADUATE SCHOOL

March 31, 2010
Date

We hereby recommend that the dissertation prepared under our supervision by Michael C. Posey entitled "Protection-Motivated Behaviors of Organizational Insiders." be accepted in partial fulfillment of the requirements for the Degree of Doctor of Business Administration - Computer Information Systems

Supervisor of Dissertation Research

Head of Department

Management and Information Systems
Department

Recommendation concurred in:

Advisory Committee

Approved:

Director of Graduate Studies

Approved:

Dean of the Graduate School

Dean of the College

GS Form 13a
(6/07)

ABSTRACT

Protecting information from a wide variety of security threats is an important and sometimes daunting organizational activity. Instead of solely relying on technological advancements to help solve human problems, managers within firms must recognize and understand the roles that organizational insiders have in the protection of information. The systematic study of human influences on organizational information security is termed behavioral information security (Fagnot 2008; Stanton, Stam, Mastrangelo, and Jolton 2006), and it affirms that the protection of organizational information assets is best achieved when the detrimental behaviors of organizational insiders are effectively deterred *and* the beneficial activities of these individuals are appropriately encouraged. Relative to the former, the latter facet has received little attention in the academic literature.

Given this opportunity, this dissertation explicitly focuses upon protective behaviors that help promote the protection of organizational information resources. These behaviors are termed *protection-motivated behaviors* (PMBs) and are defined as the volitional behaviors organizational insiders can enact that protect (1) organizationally-relevant information within their firms and (2) the computer-based information systems in which that information is stored, collected, disseminated, and/or manipulated from information-security threats. Each of the chapters herein is dedicated to fostering

knowledge about these beneficial behaviors and acts as a complement to existing research in order to more fully support the entire scope of behavioral information security.

Chapter 2 focuses upon the development of a formal typology of PMBs and relies on the complementary classification techniques of Multidimensional Scaling (MDS), Property Fitting (ProFit) analysis, and cluster analysis. 67 individual PMBs were discovered, and the above classification techniques uncovered a three-dimensional perceptual space common among organizational insiders regarding PMBs. This space verifies that insiders differentiate PMBs according to whether the behaviors (1) require minor or continual level of improvements within organizations, (2) are widely or narrowly standardized and applied throughout various organizations, and (3) are a reasonable or unreasonable request of organizations to make of their insiders. 14 unique clusters were also discovered during this process, which finding further assists information security researchers in their understanding of how organizational insiders perceive the behaviors that help protect information assets.

Chapter 3 uses the findings from Chapter 2 to develop a self-report measure of insiders' engagement in PMBs within their organizations. PMBs are modeled as a multiple indicators and multiple causes (MIMIC) structure (Joreskog and Goldberger 1975) with the clusters found in Chapter 2 being first-order, formative constructs of the overall, second-order PMB measure. These clusters explain over 70% of the variance in overall PMB activity. The nomological validity of the newly constructed measure is also empirically examined in this chapter, and the results largely support the conceptualization of PMBs.

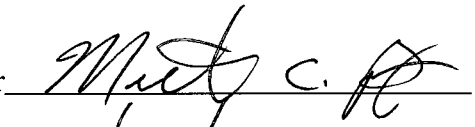
Chapter 4 places the measure developed in the previous chapter in a motivational model founded on Protection Motivation Theory (PMT) (Rogers 1975, 1983). The findings from covariance-based structural equation modeling show that insiders' motivation to engage in PMBs is largely influenced by the perceived efficacy of protective responses and potential adaptive response costs—both components of the coping appraisal process. Fear, however, is shown to have little influence on these motivational levels. In addition to the PMT components, several rival explanations are examined. Job satisfaction and management support are found to significantly explain variance in organizational insiders' motivation to engage in PMBs.

In summary, this dissertation comprises a significant work in the field of behavioral information security by conducting 33 semi-structured interviews, eliciting the participation of 13 subject matter experts, and issuing 6 individual data collections. When these efforts are combined, the results of this dissertation are based on the responses of more than 1,700 organizational insiders. The findings help both information security researchers and managers within organizations more fully understand the protective role that organizational insiders play in the protection of information resources.

APPROVAL FOR SCHOLARLY DISSEMINATION

The author grants to the Prescott Memorial Library of Louisiana Tech University the right to reproduce, by appropriate methods, upon request, any or all portions of this Thesis/Dissertation. It is understood that "proper request" consists of the agreement, on the part of the requesting party, that said reproduction is for his personal use and that subsequent reproduction will not occur without written approval of the author of this Thesis/Dissertation. Further, any portions of the Thesis/Dissertation used in books, papers, and other works must be appropriately referenced to this Thesis/Dissertation.

Finally, the author of this Thesis/Dissertation reserves the right to publish freely, in the literature, at any time, any or all portions of this Thesis/Dissertation.

Author 

Date 04/15/2010

GS Form 14
(5/03)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

I often receive the question "Clay, was getting your doctorate a difficult thing to do?" Obtaining my doctorate certainly has not been easy, and the process has required much dedication, perseverance, and the ability to prioritize time appropriately. Unfortunately, there were many times when I had to devote my attention to my doctoral studies and research at the expense of those who assisted me while on my journey. To those individuals who have ever felt disappointed because of my absence—whether physical or mental—I thank them for their continued love and support. Further, I apologize if my efforts to explain exactly what it was that I was going through and trying to accomplish during the last five years were not as helpful as I had intended.

Several individuals deserve specific mention for their role in providing outstanding support. First, I must mention my wife Leslie. Her willingness to endure my many complaints and late nights on the computer has been greatly appreciated. The completion of this dissertation marks a new beginning for us as it is the culmination of all of our sacrifices since the fall of 2005. Not only does the work herein make me proud, but I hope that somehow she shares the same feeling of accomplishment, because I could not have gone through this process without her. *IILWY.*

To my two beautiful children, Kennedy and Grayson. Those who are close to me understand that my little ones mean the world to me, and it has truly been an experience with both of them being born during my doctoral program. They are still young, so I hope

they do not have many lingering memories of Daddy being too busy to take a nap or to play on the floor with them. Trust me, Daddy always wanted to be there.

To Mom, for always giving me unconditional love though times were not always easy for her. To Dad, for instilling in me a love for music and learning and for making sure that I had the best educational opportunities. To Mamaw and Papaw Britt, for being what grandparents should be. To Ronnie and Charlene, for always being a second home.

I must also not forget the academicians who have become my colleagues and friends over the years and who helped make this and other endeavors a success. To my dissertation chair, Dr. Tom Roberts, for giving me the opportunity to work with him and for making me a better scholar—though it often meant being "timed out" to get where I am at today! To Dr. Becky Bennett, for guiding me in my many questions and for taking a sympathetic interest in the well being of her students. To Dr. James Courtney, for his many years of dedicated service to the field and for showing us that everything does not have to be quantitatively driven. To Dr. Paul B. Lowry, for always offering words of encouragement and for joining me in my journey despite being many miles away. And to the many others (e.g., Dr. Jim Cochran, Dr. Barry Babin, Dr. Marcia Simmering-Dickerson, and Dr. Hani Mesak) whose efforts have touched my life in a positive way, I am extremely grateful.

Last but definitely not least, I am indebted to the individuals at PERSEREC for believing in me and my research enough to fund this dissertation effort. Without the support of this center and its employees, I am certain that my research would not have achieved its desired goal. I hope that this dissertation and its findings are worthy of their confidence.

CHAPTER 1

INTRODUCTION

Protecting information from a wide variety of security threats is an important and sometimes daunting organizational activity. Firms increasingly devote considerable resources to ensure the confidentiality, integrity, and availability of information contained within their walls. These efforts have most often concentrated on the acquisition and implementation of technological solutions such as firewalls, monitoring systems, and intrusion prevention and detection systems.

Despite these large investments in sophisticated technological advancements, technology cannot solve human problems. Information security researchers have recently shifted their attention to the systematic study of individuals who are given control of this information in their daily work environments (i.e., organizational insiders). This discipline has been termed behavioral information security and focuses extensively on the human aspect of organizational information security (Stanton, Stam, Mastrangelo, and Jolton 2006). One of the major tenets of behavioral information security asserts that the protection of organizational information assets is best achieved when the detrimental behaviors of organizational insiders are effectively deterred *and* the beneficial activities of these individuals are appropriately encouraged. Research examining the negative behaviors of insiders began in the late 1980s and early 1990s—

research on the more positive activities of individuals internal to organizations, however, is still in its infancy.

Given this opportunity, this dissertation explicitly focuses upon protective behaviors that help promote rather than hinder the protection of organizational information resources. These behaviors are termed *protection-motivated behaviors* (PMBs) and are defined as the volitional behaviors organizational insiders can enact that protect (1) organizationally-relevant information within their firms and (2) the computer-based information systems in which that information is stored, collected, disseminated, and/or manipulated from information-security threats. Each of the chapters herein is dedicated to fostering knowledge about these beneficial behaviors and acts as a complement to existing research in order to more fully support the entire scope of behavioral information security.

This dissertation is structured in the following manner. Chapter 2 focuses upon the development of a formal typology of PMBs. This typology is necessary to make a determination of whether and how PMBs are differentiated from one another in the minds of organizational insiders. Following semi-structured interviews to elicit individual PMBs, insiders employed in various positions by organizations from a wide variety of industries in the United States were surveyed regarding their perceptions about these individual behaviors. This data is used as input to the classification technique of multidimensional scaling (MDS) (Kruskal and Wish 1978). MDS is utilized to provide a graphical representation of the insider mindset in regard to the individual PMBs. A second data collection is issued and a property fitting (ProFit) analysis is conducted to make an objective determination of the individual dimension labels of the multi-

dimensional solution uncovered by MDS. Finally, cluster analysis is performed to identify PMBs that are more closely related in the perceptual space of PMBs. All of these components comprise the steps taken to develop the formal typology of PMBs.

Chapter 3 uses the typology discovered in Chapter 2 and two separate data collections to develop a self-report measure of insiders' engagement in PMBs within their organizations. PMBs are modeled as a multiple indicators and multiple causes (MIMIC) structure (Joreskog and Goldberger 1975) with the clusters found in Chapter 2 being first-order, formative constructs of the overall, second-order PMB measure. Following these efforts, the nomological validity of the new PMB measure will be explored for the first time with data collected from a third set of organizational insiders. Antecedents, correlates, and a consequence of PMBs are included in this examination, which provides an empirical assessment of where PMBs fit in the nomological network of other important organizational behaviors.

Chapter 4 attempts to discover ways organizational insiders become motivated to engage in the behavioral structure discovered in previous chapters. The research conducted in this chapter places the newly formed PMB measure in a structural model derived from Protection Motivation Theory (PMT) (Rogers 1975, 1983). In addition to the individual components suggested by PMT, several rival explanations elicited from the semi-structured interviews will be tested for their potential influence on motivating PMBs within organizations. This structure will be examined via covariance-based structural equation modeling (i.e., AMOS) to assess these motivating influences on PMBs.

Finally, Chapter 5 will conclude this dissertation. This chapter will provide a brief review of the overall contributions of this dissertation to the discipline of Information Systems generally and to the field of behavioral information security specifically. The contributions of the research efforts conducted in Chapters 2, 3, and 4 will also be individually discussed.

CHAPTER 2

INSIDERS' PROTECTION OF ORGANIZATIONAL INFORMATION ASSETS: A MULTIDIMENSIONAL SCALING STUDY OF PROTECTION-MOTIVATED BEHAVIORS

The primary goal in managing a firm's information systems (IS) security is to protect information resources of the firm (Dhillon and Torkzadeh 2006). For this purpose, organizations worldwide dedicate an increasing amount of financial resources to the protection of their information from both external and internal threats (Cavusoglu, Cavusoglu, and Raghunathan 2004; Richardson 2007). As examples, companies in the United Kingdom spent over $7 billion on IT security in 2008 (IT Security Market Report 2009 2009), the 2009 spending by the United States' Federal Government reached almost $8 billion (Defining the Federal Information Security Mission: 2009 – 2014 Market Forecast 2009), with the global IT security market projected to increase 15.5% growth rate from 2008 to 2012 (Global IT Security Market Forecast to 2012 2008). These spending habits are no doubt a result of the general public and investors' reactions to security-breach announcements, which lead to a decrease in public trust and in market value to the extent of $1.65 billion per breach within just two days of the declaration (Cavusoglu, Mishra, and Raghunathan 2004). Clearly, organizations and their stakeholders view information as a resource that must be protected even at considerable costs because the costs of not doing so are exponentially greater.

Despite the literature's early focus on traditional, technical methods to achieve this protection, researchers now recognize that security efforts must adequately account for individual, social, and organizational influences (Choobineh et al. 2007; Dhillon and Backhouse 2000; Vroom and von Solms 2004). In particular, researchers are interested in the impact of organizational insiders' behavior on information security within firms (D'Arcy and Hovav 2007; Moore, Cappelli, and Trzeciak 2008; Whitman 2003). These individuals' actions, whether accidental or intentional, exert significant influence on the organizational information security chain (Im and Baskerville 2005; Vroom and von Solms 2004).

While individuals within organizations can have detrimental effects on organizational information (Straub 1990; Whitman 2003), they also have the potential to help protect organizational information and information systems (Stanton and Stam 2006; Stanton et al. 2005). Moreover, recent research underscores the need for security practitioners and researchers to expand their belief systems about organizational insiders rather than continue to view them from a singular, unfavorable perspective. Specifically, organizational information protection can be achieved with a simultaneous understanding of (1) how to deter detrimental human behavior *and* (2) how to motivate the beneficial activities of organizational insiders (Stanton et al. 2005). These latter, benevolent activities are extremely desirable as the timely detection of security attacks against an organization is highly dependent upon the awareness and actions of authorized organizational insiders (Hamill, Deckro, and Kloeber 2005).

Despite the importance of protecting organizational information from insiders, few studies have expanded on the knowledge proffered by the field's initial investigations

of these protective behaviors. Some of these protective-based behaviors have been examined under the guise of "safe computing practices" (Aytes and Connolly 2004) and behaviors requiring general caution when using email (Ng, Kankanhalli, and Xu 2009); however, research defining, eliciting, and further classifying the wide range of beneficial behaviors in which organizational insiders can engage is limited. Such exploratory efforts would prove beneficial to guide future research efforts to more effectively complement the findings already established by researchers investigating the negative behaviors of organizational insiders.

Given these opportunities, this research focuses on *protection-motivated behaviors* (PMBs), which are defined as the volitional behaviors organizational insiders can enact that protect (1) organizationally-relevant information within their firms and (2) the computer-based information systems in which that information is stored, collected, disseminated, and/or manipulated from information-security threats. *Organizational insiders* refers to all individuals such as full-time employees, part-time workers, temporary employees, or contracted individuals who have access to organizationally-relevant information while fulfilling their organizational duties (Shaw, Ruby, and Post 1998). These behaviors, however, represent an individual's attempt to protect their organization from information security threats but do not guarantee that such threats would be fully prevented. This chapter proposes a typology of PMBs through the use of multidimensional scaling (MDS) (Kruskal and Wish 1978), a classification technique that has greatly benefitted a wide variety of other disciplines, such as organizational deviance (Robinson and Bennett 1995), acoustics recognition (Grey 1977), individual power strategies (Falbo 1977), ecology (Kenkel and Orloci 1986), and market segmentation

(DeSarbo, Grewal, and Scott 2008). The findings reveal that a wide range of PMBs exist and are best represented along three dimensions: (1) whether the behaviors (1) required minor or continual level of improvements within organizations; (2) were widely or narrowly standardized and applied throughout various organizations; and (3) were an reasonable or unreasonable request of organizations to make of their insiders.

The remainder of the chapter is structured as follows: after a review of the relevant literature, the qualitative and quantitative methodological approaches used to develop and explain the classification of 67 protection-motivated behaviors is explained; finally, the findings of the study and its contributions to academia and practice are discussed.

Literature Review

The information and computer security literature has traditionally favored the technical methods of ensuring organizational information protection, which are derived heavily from fields such as electrical engineering and computer science (Choobineh et al. 2007). For example, physical access controls, network security, and the design of secure information systems have played a major role in the literature's development (Siponen and Oinas-Kukkonen 2007). Other important technical matters such as biometrics (Jain, Ross, and Pankanti 2006), data perturbation techniques (Muralidhar and Sarathy 2005), and various access management and intrusion prevention and detection methods (Hansen et al. 2007; Yue and Cakanyildirim 2007) have also been addressed. A recent assessment of organizational security by security professionals also describes a handful of technical measures firms can adopt to help protect organizational information (Whitman 2003).

Notwithstanding the importance of the above technical approaches, the IS discipline recognizes that information security is as much a managerial and human-behavior issue as it is a technical matter (D'Arcy and Hovav 2009, 2007; Im and Baskerville 2005; von Solms 2000). Sole reliance on technical methods is an ineffective approach to achieve organizational information protection as it fails to incorporate the "softer" approaches to IS security (Siponen 2001) such as examining the influences produced by individual, organizational, and social factors or best management practices to appropriately handle threats to information security (Dhillon and Backhouse 2000; Dhillon and Torkzadeh 2006; Hitchings 1995; Trompeter and Eloff 2001). Hence, research should foster an understanding of technical methods and managerial and behavioral controls of IS security in a simultaneous fashion (D'Arcy and Hovav 2007; Stanton and Stam 2006).

Fagnot (2008) refers to the study of these human influences as behavioral information security. *Behavioral information security* research encompasses all of the complexities of human activity that influence the confidentiality, integrity, and availability of information and information systems (Stanton et al. 2006). This research stream is composed of two general areas in regard to organizational insiders. The first area focuses on individuals as the weakest link in the security chain (Dhillon 2001; Vroom and von Solms 2004) and how these individuals can be successfully deterred from committing detrimental acts against organizational information and information systems (Lee, Lee, and Yoo 2004; Straub 1990). Studies have concentrated on how individuals can be deterred from committing costly internal computer abuses (Backhouse and Dhillon 1995; Dhillon 2001; Harrington 1996), most often using the foundation of

general deterrence theory (Lee, Lee, and Yoo 2004; Straub 1990; Straub and Welke 1998; Siponen and Willison 2007; Theoharidou et al. 2005). This focus on deterrence stems from the commonly held belief that organizational insiders are the most significant risk to organizational information security because of either unintentional errors (Im and Baskerville 2005; Loch, Carr, and Warkentin 1992) or purposeful malfeasance (Cronan, Foltz, and Jones 2006; D'Arcy and Hovav 2007; Dhillon and Backhouse 2000; Magklaras and Furnell 2005; Willison and Backhouse 2006).

The second and significantly smaller behavioral information security area leverages organizational insiders as a positive solution to information-security problems (Ng, Kankanhalli, and Xu 2009; Stanton et al. 2005; Stanton and Stam 2006). This research area attempts to determine how these individuals can be motivated to engage in behaviors that increase organizational information security by including such human principles as responsibility, integrity, trust, and ethicality (Dhillon and Backhouse 2000). Despite long-held knowledge of the obligations of certain employees—especially IS practitioners—to protect the privacy and confidentiality of organizational information (Oz 1992; Walsham 1996), the responsibility of all individuals within firms to protect organizational information has been overwhelmingly overlooked and under investigated (Stanton and Stam 2006). This lack of interest in these defensive actions of organizational insiders is particularly troubling as even honest individuals might harm organizational security efforts by unknowingly becoming victim to external threats (Choobineh et al. 2007). This deficiency in knowledge is also surprising given the increased number of hierarchically flattened organizations, which attempt to disseminate more rather than less

organizational information to employees within their structures (Dhillon and Backhouse 2000).

Researchers have explored individuals' motivation to adopt *technologies* to aid in *personal* protection (Dinev et al. 2009; Dinev and Hu 2007; Lee and Kozar 2008), though limited research efforts have addressed the *behaviors* individuals engage in to protect their respective *organizations*. Researchers have, however, specified that humans have a responsibility to act with integrity (Whitman 2003) and can become protective agents of information within their respective organizations (Stanton et al. 2005; Stanton and Stam 2006). Getting these organizational insiders to take ownership of this responsibility while being focused on their daily work tasks, however, is made much more difficult as these individuals endure significant economic downturns, corporate downsizing, and sizeable outsourcing efforts of their respective firms (Stanton and Stam 2006). Previous studies in behavioral information security have argued that specific individuals should be held responsible for information liability, and that this responsibility should be formally delegated by organizational management (Backhouse and Dhillon 1995; Straub and Collins 1990). Current governmental mandates (e.g., Sarbanes-Oxley, Graham-Leach-Bliley, HIPAA) place extreme pressure on upper-level organizational members to conform to accepted standards for organization information security. Expanding on this belief, this research posits that *all* insiders have a responsibility to protect information relevant to their organization due to their expansive roles and involvement with organizational information. To quote from Stanton and Stam (2006):

> As a group, employees have access to most or all of the organization's most valuable information assets. Their actions have a profound influence on the safety and protection of those assets, even in situations in which information technology professionals have put monumental efforts into

> imposing mechanical controls on what users are allowed to do with the company's computers and networks (p. 38).

Individuals within organizations have immense control over the protection of organizational information where technical methods of IS security fail to exert their intended influence or cannot extend. All insiders, rather than a selected few, are ultimately responsible for the protection of information assets within their firms. Now more than ever, organizations have significant need of employees who are willing to take an expansive, active role as protection-motivated stewards of organizational information (Straub and Collins 1990; Van Niekerk and von Solms 2010; Ng, Kankanhalli, and Xu 2009). The difference between employees knowing what to do and actually performing that behavior, however, concerns even the most prepared of managers in organizations (Workman, Bommer, and Straub 2008) and should remain a focus of behavioral information security researchers.

Out of the variety of security countermeasures or mechanisms available to employees (Ng, Kankanhalli, and Xu 2009; Workman, Bommer, and Straub 2008), only a few have been formally specified and/or investigated. "Safe computing practices" studies have highlighted individuals' regular backing up of data, scanning email attachments for viruses, voluntarily changing of passwords, refusing to share passwords (Aytes and Connolly 2004), and exercising general caution when receiving emails (Ng, Kankanhalli, and Xu 2009). Such defensive behaviors are fundamental for organizational informational security, hence, it is surprising that a mere 20% and 40% of respondents report volitionally changing passwords and backing-up data files, respectively, on a frequent basis (Aytes and Connolly 2004).

Several authors have attempted to understand the motivation which prompts employees to engage in such protective behaviors. Siponen, Pahnila, and Mahmood (2007) examined employees' general behavior of adherence to organizational information security policies. Workman et al. (2008) explored employee engagement in three precautionary measures: (1) updating and protecting passwords, (2) keeping security and antivirus software up to date, and (3) keeping systems backed up. Both studies provide empirical evidence that employees can be motivated to protect organizational information assets. These studies further suggest that individuals assess both the threats to their organizations and their ability to cope with those threats effectively prior to their engagement in the above behaviors (Workman, Bommer, and Straub 2008; Siponen, Pahnila, and Mahmood 2007).

Despite the importance of the aforementioned studies and their view of insiders as stewards of organizational information (Stanton and Stam 2006), the behaviors of organizational insiders and their interrelationships are not yet fully understood. In fact, the majority of the protective behaviors are likely only to be found within security certification training texts (Price 2007). Some protective-based behaviors have also been studied in academic research but in isolation or in very small subsets (Aytes and Connolly 2004; Workman, Bommer, and Straub 2008; Ng, Kankanhalli, and Xu 2009; Siponen, Pahnila, and Mahmood 2007). Methodologists have suggested, however, that studying behaviors as an aggregate rather than as isolated events offers researchers the opportunity to better understand complex psychological processes surrounding the human behavior (Hanisch, Hulin, and Roznowski 1998; Hanisch and Hulin 1991) In summary,

the domain space of PMBs has yet to be defined and examined by a targeted study. Accordingly, the first question addressed by this research is:

RQ1. What protection-motivated behaviors (PMBs) do organizational insiders perform within organizations?

Once the domain space of PMBs is defined, a determination can be made as to how the individual PMBs are differentiated from one another relative to the collective perceptual space of organizational insiders. Determining whether different perceptual dimensions exist will be important for theoretical advancement in the field of PMBs as a formal typology of these behaviors can be developed. This typology will allow researchers to focus on the individual components of the PMB structure and determine the motivations for the various facets. Findings from these studies will make vital contributions to the practitioners trying to increase their occurrence within organizations. Therefore, the second question addressed by this research is:

RQ2. What cognitive dimensions do organizational insiders use to categorize PMBs?

In the following sections, steps are taken to explain how a formal typology can direct research on PMBs. A brief review of the chosen theoretical basis upon which this typology is derived (i.e., Protection Motivation Theory) and a discussion of the chosen methodology is provided.

Implicit Assumptions and Theoretical Foundation

The formation of a sound typology should be preceded by an exposition of the grand assumptions underlying its development (Doty and Glick 1994). In this regard, it is posited that organizational insiders can be motivated by various factors to engage in

PMBs to help protect their respective organizations from information security threats. Just as employees can become motivated to engage in both in-role and extra-role behaviors within organizations (MacKenzie, Podsakoff, and Ahearne 1998; McNeely and Meglino 1994; Organ, Podsakoff, and MacKenzie 2006), techniques can likely be leveraged to motivate individuals to attempt to defend their organization in the security domain. These PMBs represent insiders' attempts to maintain the confidentiality, integrity, and availability of information and computerized information systems within their firms. These behaviors are meant to protect the organization from both external and internal security threats. It is further posited that a set of these behaviors exists, which is generally applicable to a wide variety of organizations and occupations. Behaviors within this set, however, are likely to vary according to several factors or dimensions (Ng, Kankanhalli, and Xu 2009); therefore, all PMBs are not expected to be the same in the minds of insiders. Some PMBs may be more beneficial to the overall protection of organizational information and information systems than others.

The theoretical foundation guiding the above assumptions is Protection Motivation Theory (PMT) (Rogers 1975, 1983). Briefly, PMT specifies the cognitive processes that individuals undergo following the reception of threat information. These processes result in the individual being motivated to engage in either adaptive or maladaptive behaviors (Rogers and Prentice-Dunn 1997). *Adaptive responses* are those which effectively minimize the threat (Rogers 1983), whereas *maladaptive responses* are those responses which assist in reducing the fear an individual may feel in regard to a danger but fail to reduce the occurrence and/or effects of the actual danger (Rippetoe and Rogers 1987).

Two appraisal processes are central to the theory: threat appraisal and coping appraisal. *Threat appraisal* is the process by which an individual analyzes the perceived vulnerability to a threat, the perceived severity of a threat, and any perceived intrinsic and/or extrinsic rewards for engaging in a maladaptive manner. *Coping appraisal,* is the process by which an individual evaluates the efficacy of potential adaptive responses to a threat, the individual's perceived ability of successfully carrying out the recommended responses (i.e., self-efficacy expectancy; (Bandura 1977), and any response costs associated with the adaptive coping strategy (Maddux and Rogers 1983; Rogers 1983). Both strengthening and weakening forces act upon the individual in their decision to engage in both adaptive and maladaptive responses to dangers. It is important to note that PMT does not assume that the decision maker is rational (Rogers and Prentice-Dunn 1997).

The outcome of the PMT model is a motivational force termed protection motivation. *Protection motivation* is "an intervening variable that has the typical characteristics of a motive: it arouses, sustains, and directs activity" (Rogers 1983, p. 158). Therefore, protection motivation drives behavior change (Rogers and Prentice-Dunn 1997).

While PMT's vast background is largely rooted within the field of personal preventive medicine (Floyd, Prentice-Dunn, and Rogers 2000; Milne, Sheeran, and Orbell 2000), PMT may be applied to any situation involving a threat (Rogers 1983). In fact, any source of information about a threat, especially a fear appeal, initiates a threat appraisal and a coping appraisal process. PMT can also be applied to incidents that do not arouse one's fear (Rogers 1975) and to situations entailing multiple adaptive and/or

maladaptive response possibilities (Rogers and Prentice-Dunn 1997). PMT may therefore be used to understand reactions to threat phenomenon outside of personal health communications and experimental settings (Beck 1984; Maddux and Rogers 1983; Rogers and Prentice-Dunn 1997) to include social problems (Tanner, Day, and Crask 1989) as well as individuals' protection of other individuals (Beck and Feldman 1983; Flynn, Lyman, and Prentice-Dunn 1995) and even organizations (Beck 1984).

To this end, PMT has also recently been applied in IS security research. The most extensive integration of PMT is provided in the technology threat avoidance theory (Liang and Xue 2009) wherein technology adoption models are described as being inadequate to completely understand users information-security behaviors. This theoretical contribution enlarges researchers' awareness of the mediating cognitive factors suggested by PMT when individuals perceive personal, information-security threats (Liang and Xue 2009).

Empirical findings showing general support this integration have been proffered. Siponen, Pahnila, and Mahmood (2007) investigated organizational protection of information through employees' intention to comply with IS security policies. The threat appraisal process, response efficacy, and self-efficacy all significantly predicted intention to comply with information security policies. These intentions, which represent a single protection-motivated behavior, also significantly predicted actual compliance behaviors of the employees surveyed (Siponen, Pahnila, and Mahmood 2007). Very similar results in general compliance behaviors have recently been found (Herath and Rao 2009). Likewise, significant links from the components of PMT to the behaviors of home wireless security technology adoption (Woon, Low, and Tan 2005), the updating and

protection of passwords, the updating of security and virus software, and the backing up of systems' files (Workman, Bommer, and Straub 2008) have also been found.

As more organizations are engaged in educating and training their employees in regard to information security principles, techniques, and threats (Richardson 2007), PMT can help explain why individuals choose to protect their organization's information resources by engaging in PMBs. The PMT theory can also assist in highlighting the potential maladaptive behaviors organizational insiders enact (e.g., avoidance, hopelessness, and fatalism) following receipt of threat communication within organizations.PMT is thus suitable to frame researchers' understanding of individuals' security-related activities and how those behaviors affect the security of organizational rather than just personal information assets.

Methodology

Multidimensional scaling (MDS) (Kruskal and Wish 1978) was the chosen technique to derive the typology of PMBs. MDS is a powerful classification methodology, which allows a set of objects or behaviors to be differentiated without much foreknowledge of such differences or researcher-introduced bias (Hair et al. 2006). Further, the technique is an iterative attempt to physically map the latent psychological distances between a set of objects or behaviors that exist collectively in the minds of the respondents (Rabinowitz 1975; Tan and Hunter 2002). This approach is important as the respondents' perceived dimensions are the relevant dimensions (Green and Carmone 1970). Other disciplines have shown significant benefits from the use of this methodological process in their formative years (Robinson and Bennett 1995).

Multidimensional scaling refers to a group of data classification techniques that allow researchers to position similar objects or behaviors within their respective perceptual dimensions (Kruskal and Wish 1978). The technique recovers underlying structure, usually in two or three dimensions, among stimuli which are masked in a dataset (Schiffman, Reynolds, and Young 1981; Huang et al. 2006) and is similar to both factor and cluster analyses but does not rely on a specified variate, which often introduces researcher bias into studies of an exploratory nature (Hair et al. 2006). Further, MDS techniques normally provide "more readily interpretable solutions of lower dimensionality" than do factor analysis techniques (Schiffman, Reynolds, and Young 1981, p.13) and are more effective at recovering the structure among myriad interest points when dimensionality, both in number and context, is relatively unknown to the researcher than cluster analysis (Kruskal 1977).

PROXSCAL, which is based on the previous work of de Leeuw and colleagues on the SMACOF approach (de Leeuw and Heiser 1980, 1977; de Leeuw and Mair 2008) was the MDS technique used in this study. While there are various methods of obtaining a spatial representation of similarity data with MDS, PROXSCAL is superior to other popular methods such as ALSCAL in that it does not tend to exaggerate large distances and understate small distances among objects (Groenen and van de Velden 2004). The SMACOF approach, which focuses on what is termed a majorization algorithm, determines the spatial representation that is most representative of the similarities by minimizing a badness-of-fit measure called a stress function. *Stress* is a multivariate function of the distances between the objects and is analogous to the sum of the Euclidean distances between the objects in a spatial configuration relative to the

difference between the objects in the input matrix (Kruskal and Wish 1978). (ALSCAL uses SSTRESS, which represents the sum of the *squared* Euclidean distances). The PROXSCAL approach iteratively attempts to find the position of each individual object relative to all other objects that effectively minimizes the stress index of the overall graphical representation (Groenen and van de Velden 2004; de Leeuw and Mair 2008). The technique is decompositional in nature as the number of dimensions best representing PMBs were not known beforehand (Hair et al. 2006).

Despite the fact that IS researchers have explained the importance of using the MDS technique (Byrd, Cossick, and Zmud 1992; Tan and Hunter 2002), few have heeded the call. Of these, researchers have used the technique to graphically relate types of business-to-business e-marketplace activities (Matook and Vessey 2008), users in the e-mail network space (Rice 1994), and variations among different system development methodologies (Sircar, Nerur, and Mahapatra 2001). This chapter presents one of the first examples in the IS literature in using MDS to empirically determine the mindset of a population of individuals regarding their behaviors in the workplace.

Data Collection

The MDS technique requires researchers to conduct three preliminary activities: (1) behavior elicitation; (2) removal of redundant behaviors; and, (3) acquisition of similarity ratings, which form the data matrix for use in an MDS program. Behavior elicitation requires an initial in-depth review of the protective behaviors listed in previous literature. Since the protective-based, organizational-insider literature is currently in a developmental stage, few sources (Ng, Kankanhalli, and Xu 2009; Stanton and Stam 2006; Stanton et al. 2005) have cited such information.

To bridge this gap, semi-structured interviews with 11 information security professionals and 22 organizational insiders were conducted to obtain a more complete view of these behaviors. Table 2.1 highlights the qualifications of the interviewees who were employed in various roles in a multiple industries. These interviews were vital to the purposes of the study as MDS techniques are dependent upon the inclusion of only relevant behaviors or objects of interest (Hair et al. 2006; Priem, Love, and Shaffer 2002). A professional transcription service was hired to transcribe the interviews, and QSR International's NVivo 8 software was utilized during content analysis to help elicit the individual behaviors mentioned during the 33 interviews. In total, 160 protection-motivated behaviors were elicited from the interviews.

Table 2.1 Interviewee Qualification

Position	**Industry**	**Manager**	**Years of Experience**
*Information Security Professionals**			
IT Security Architect	Computer Hardware and Services	No	10
Assistant Vice President / IT Manager	Banking	Yes	9
Network Administrator	Retail / Financial Services	No	10
IT Security Supervisor	Utilities	Yes	9
Senior Network Administrator	United States' Armed Forces	No	30
Manager of IT Governance and Compliance	Insurance	Yes	1
Chief Information Security Officer	Logistics	Yes	10
Network Administration Supervisor	Medical	Yes	12
Director of Cyber Security Program	United States' Armed Forces	Yes	2
Information Security Engineer	Defense Contractor	No	9
Vice President of Information Security	Retail	Yes	11

Table 2.1 (Continued)

Organizational Insiders			
Regional Sales Manager	Wholesale - Food	Yes	6
Regional Sales Manager	Retail Sales - Medical Equipment	Yes	22
Radiology Technician	Medical	No	14
Printed Circuit Board Technician	Engineering / Production	No	21
Administrative Assistant	Higher Education	No	40
Customer Service Representative	Telecommunications	Yes	27
Collections Agent	Financial Services	No	45
Customer Service / Quality Engineer	Engineering / Production	No	2
Assistant Branch Manager	Banking	Yes	11
Finance Officer	Higher Education	No	4
Supervisor	United States' Postal Service	Yes	7
Auditor	State Government	No	14
Probation officer	Federal Government	No	21
Technical Assistant / Chemical Engineer	Engineering / Production	No	6
Finance Manager	Automobile Sales	Yes	9
Loan Secretary	Banking	No	32
Pilot	United States' Armed Forces	No	11
Court Reporter	Legal Transcription Services	No	14
Project Manager	Technology Services	Yes	14
Financial Analyst	Financial Services	No	19
Air Traffic Controller	Aviation	No	7
Rating Chart Specialist	Insurance	No	2

* Collectively, the information security professionals held the following certifications: CISSP (5); CEH (2); Security+; CISM; SANS GIAC; NSA IAM and IEM; MCSE; CCNA; MCP+I; Net+; A+; and, PMP.

This set of behaviors was then subjected to several external reviews. First, a senior doctoral candidate in information systems assessed the behaviors to remove potential redundancies. This review left 92 unique behaviors, which were then subjected to a more rigorous assessment. Ten subject-matter experts (SMEs) (three professors of information systems, two professors of management, and five graduate information systems students with significant professional experience) rated each of the unique

behaviors along a 7-point Likert-like scale on three factors: (1) the behavior's fit with the definition of PMBs; (2) the clarity of the behavior's wording; and, (3) the behavior's applicability to a wide range of occupations and industries. The SMEs' ratings were averaged and behaviors receiving a four or less on any of the three above factors were given consideration for minor alterations or exclusion from further assessment. Following this second review, 67 behaviors emerged as the unique set of PMBs to undergo assessment with the MDS technique (see Appendix A).

To obtain data for the MDS similarity matrix, an online panel provider was hired. Online panels provide the diversity (e.g., work experience and professional background) of sample respondents requisite for the development of a generalizable typology of PMBs. In total, 492 panelists from a wide variety of industries participated. As in other studies (Robinson and Bennett 1995), similarity ratings could not be obtained for all behavior pairs from each respondent due to the overall set size; therefore, each respondent was issued a single behavior to compare against the other 66 behaviors in the behavior set. These judgments were averaged across all respondents thereby making the technique an aggregate MDS approach (Hair et al. 2006). In addition to rating each behavior-pair comparison on a 9-point bipolar scale (*not at all similar – very similar),* respondents were asked to comment as to how they arrived at each of their comparison decisions.

Analysis and Results

The first step in running the MDS technique was to determine the number of dimensions that best represents the structure of the respondents' ratings in a parsimonious manner. Configurations of 2 to 10 dimensions were run with various preliminary

configurations (i.e., Simplex, random, and Torgerson), and their stress amounts were plotted against the number of dimensions to conduct a Scree test (Cattell 1966; Robinson and Bennett 1995). The traditional Torgerson approach consistently produced a better fit to the data with all Scree plots indicating a three-dimensional solution. Three other criteria were also used to select the appropriate number of dimensions: (1) Normalized Raw Stress levels; (2) Percentage of dispersion accounted for (DAF; similar to variance explained); and, (3) Tucker's Coefficient of Congruence. The combination of both badness-of-fit (i.e., stress) and goodness-of-fit (i.e., DAF and Coefficient of Congruence) indices is important in assessing the overall configuration (Hair et al. 2006). Again, a three-dimensional solution represented acceptable statistics while maintaining parsimony (Normalized Raw Stress = 0.067; DAF = 0.933; Tucker's Coefficient of Congruence = 0.966).

Labeling the Dimensions

Once the dimensionality of the respondents' perceptual space has been determined, the dimensions need to be labeled. As a more objective method of making this determination, the recommendations of MDS researchers (Kruskal and Wish 1978; Robinson and Bennett 1995; Padgett and Mulvey 2007) were followed by conducting a property fitting (ProFit) analysis. A ProFit analysis regresses respondents' ratings of several possible dimension labels on the behaviors' position in the three-dimensional coordinate space indicated by the MDS coordinate space. Variance explained, calculated *F* values, standardized regression weights, and correlations among the ratings are used in combination to determine the appropriate dimension labels (Robinson and Bennett 1995; Padgett and Mulvey 2007).

Possible dimension labels were elicited from the comments provided by the first set of panelists, and those mentioned most frequently were used in the ProFit analysis. A new set of panelists (n=235) rated each of the behaviors on 7-point bipolar scales on the following eight possible dimension labels on whether or not the behavior: (1) is an adopted standard or protocol; (2) should be performed by all insiders; (3) made common sense; (4) placed a significant burden on the insider to perform; (5) required much training to perform appropriately; (6) should always be performed; (7) is always an issue; and, (8) the need for the behavior was rather obvious. The results of the ProFit analysis are shown in Table 2.2.

Cluster Analysis

While MDS techniques are appropriate for determining the dimensionality of the structure best representing the configuration of similarities among a large number of items, objects, or behaviors, cluster analysis techniques are better utilized when attempting to classify the smaller structures or types within a pre-specified configuration—such as one suggested by MDS (Padgett and Mulvey 2007; Kruskal 1977). For this reason, a cluster analysis was conducted to determine whether subgroups of PMBs exist within the perceptual space of the respondents. The cluster analysis utilized a two-step approach (Hair et al. 2006). First, a series of hierarchical cluster analyses with agglomerate schedules and various algorithms (i.e., minimum distance, maximum distance, Ward's method, and centroid method) was conducted to determine the number of clusters present within the configuration. All of the elbow analyses (similar to Scree plots) from these hierarchical methods suggested that 14 clusters exist within the recovered structure. Following this determination, a K-means cluster analysis constrained

Table 2.2 Property Fitting (ProFit) Analysis Results

Derivation of Labels for the Dimensions													
						Correlations							
Attributes	R^2	F	Dimension 1	Dimension 2	Dimension 3	1	2	3	4	5	6	7
1. Adopted Standard or Protocol	0.140	3.428*		0.338**								
2. Should Be Performed by All	0.117	2.787*		0.262*		0.706***						
3. Common Sense	0.096	2.231+			0.296*	0.644***	0.759***					
4. Burdensome	0.113	2.688+	0.265*			-0.138	-0.170	-0.120				
5. Training Required	0.115	2.732+	0.284*			0.239+	0.230+	0.243*	0.602***			
6. Should Always Be Performed	0.084	1.936		0.265*		0.551***	0.634***	0.527***	-0.377**	-0.008		
7. Always an Issue	0.165	4.157**	0.332**			0.256*	0.246*	0.302*	0.366**	0.440***	0.176	
8. Need is Obvious	0.113	2.688+		0.335**		0.578***	0.623***	0.488***	-0.196	0.260*	0.656***	0.326**

+ $p < 0.100$
* $p < 0.050$
** $p < 0.010$
*** $p < 0.001$

to 14 total clusters was utilized to establish the membership of each cluster of PMBs. Figures 1, 2, and 3 graphically display the clusters within the three-dimensional space suggested by the MDS technique. It is important to note that the classification techniques used in this study (i.e., multidimensional scaling and cluster analysis) are not immune to error, and that the findings from these techniques—just like those of other methods—should be used as a guide for interpretation rather than as a basis to claim of absolute proof.

Discussion

Summary of Results

The MDS technique, which used the similarity matrix derived from the responses of 492 organizational insiders, demonstrates that PMBs are best classified within a three-dimensional solution. Further, ProFit analysis (n=235) shows that these three dimensions are delineated on (1) the degree to which improvement efforts are needed, (2) the level of standardization and applicability across organizations and insiders, and (3) the level of reasonableness upon which the behavior is founded. Post-hoc cluster analysis also suggests that various clusters exist within the above structure. A discussion of these results in given in more detail below.

Typological Findings

The quantitative techniques used in this study (i.e., MDS, ProFit analysis, and cluster analysis) indicate that PMBs are classified according to several major types in the minds of organizational insiders (see Table 2.3).

Table 2.3 Major Types of Protection-Motivated Behaviors

Level of Improvement Required	Level of Standardization and Applicability	Level of Reasonableness	Description
Continual	Wide	Reasonable	Behaviors having a wide applicability across organizations and their insiders whose demands are reasonable yet require continual, formal measures of improvement to conduct appropriately
		Unreasonable	Behaviors having a wide applicability across organizations and their insiders whose demands are unreasonable and would require continual, formal measures of improvement to conduct appropriately
	Narrow	Reasonable	Behaviors having a narrow applicability across organizations and their insiders whose demands are reasonable yet require continual, formal measures of improvement to conduct appropriately
		Unreasonable	Behaviors having a narrow applicability across organizations and their insiders whose demands are unreasonable and would require continual, formal measures of improvement to conduct appropriately
Minor	Wide	Reasonable	Behaviors having a wide applicability across organizations and their insiders whose demands are reasonable and should not require much improvement efforts to conduct appropriately
		Unreasonable	Behaviors having a wide applicability across organizations and their insiders whose demands are unreasonable and should not require much improvement efforts to conduct appropriately
	Narrow	Reasonable	Behaviors having a narrow applicability across organizations and their insiders whose demands are reasonable and should not require much improvement efforts to conduct appropriately
		Unreasonable	Behaviors having a narrow applicability across organizations and their insiders whose demands are unreasonable and should not require much improvement efforts to conduct appropriately

As the first line of demarcation, insiders separate PMBs on whether these activities are always an issue within their organization and require much training to conduct appropriately. This factor was labeled as *level of improvement required.*

PMBs classified as *continual* are those behaviors that organizational insiders believe should remain a steady focus of the organization either because they are more difficult to perform or that these are the PMBs best suited to successfully prevent a frequently occurring information security threat. These PMBs place more of a burden on the insider to perform than others while requiring more formal training to ensure the behaviors' efficacy. These PMBs require continual emphasis within organizations and include the behaviors of double checking work completed to ensure accuracy (behavior 20) and backing up data on a regular basis (behavior 65). *Minor* PMBs on the other hand are those PMBs that insiders believe require little to no formal training or continual awareness programs. Reasons for this characteristic are because they (1) either do not encumber the insider during engagement and are more easily performed than those behaviors in the continual classification or (2) they are already being performed to a degree that only minimal awareness efforts should be dedicated to them. Examples of such behaviors include the locking of the workstation upon insiders' physical leave of the workspace (behavior 66) or the immediate informing of proper authorities upon physical theft of computing equipment (behavior 35).

Level of Standardization and Application is the second part of the classification scheme identified by the MDS and ProFit procedures. PMBs having a *wide* standardization and application should be performed by all insiders, regardless of occupation, status, or organization. These behaviors are likely included as part of adopted

company protocol and are a general expectation of and are generally accepted by all organizational insiders. Behaviors such as discussing sensitive information with authorized individuals only (behavior 17), logging out of a computer system as soon as he/she is done with it (behavior 23), and changing passwords according to organizational guidelines (behavior 28) fit into this category. *Narrowly* standardized and applicable PMBs are considered by insiders as having a more limited scope. These behaviors do not necessarily need to be performed by everyone or at all times within the organization. This characteristic is due in part that insiders do not view many of these behaviors as having been formally adopted within their organizations as protocol or as every individual's responsibility to conduct. Setting the permissions of computer files to prevent unauthorized access (behavior 2), keeping the electronic devices assigned to them by the organization with them at all times (behavior 32), and adequately documenting any changes he/she makes in the computer system (behavior 21) are placed within this narrow classification. One notable difference in the mindset of insiders regarding behaviors in the wide and narrow types is the perceptual distance between behaviors 67 (i.e., reminding a co-worker of information security guidelines) and 43 (i.e., reporting a co-worker who breaks those guidelines to proper authorities). The former is positioned in the narrow level of standardization, whereas the latter is positioned in the wide. Interestingly, insiders as a collective unit believe it is everyone's responsibility to report an internal deviant, while only some should give friendly reminders.

The third general factor in the formal typology is best represented as *level of reasonableness*. The behaviors that are considered as *reasonable* in the collective minds of organizational insiders are thought of as having been based on common sense and

clear logic. Many insiders commented on these activities as being "commonly held knowledge by everyone" or by the more colloquial terms such as "of course." Examples of such commonsensical behaviors are working at a steady but cautious pace (behavior 53) or immediately reporting a lost physical access card to management (behavior 36). *Unreasonable* PMBs refer to actions whose founding logic may be unclear to the insiders and whose expectations exceed what is a reasonable expectation of the insider given other workplace activities. For example, the behavior of not opening emails that "just do not look right" (behavior 14) is seen as more unreasonable than reasonable because many insiders cannot make an adequate assessment of what constitutes legitimate business communication. Surprisingly, some respondents commented that *all* emails that make it to them through their organizations' networks should be treated as valid communication attempts and deserve a reply. Insiders also believe that disallowing access to the Internet for non-work related material (behavior 52) and disallowing use of corporate email for personal matters (behavior 51) are too restrictive. Perhaps this finding can help explain why so many insiders choose to deviate from corporate policy on Internet and email usage.

Cluster Findings

In addition to the typology, this research shows that various clusters of similar PMBs exist. Cluster analysis identified 14 unique clusters within the MDS structure; however, a few of the clusters had only one or two members. While all of the behaviors are PMBs, some of them are not considered similar enough to be grouped with others. For example, the behaviors of gaining approval before setting up a wireless network within the organization and the act of keeping the physical electronic equipment assigned

to insiders by the organization with them at all times when away from the organization do not have enough similarity with the other behaviors and are hence each considered to be a single cluster. Likewise, due to the wide array of behaviors in the perceptual space, some PMBs are assigned to a cluster whose other behaviors may not appear similar to them. In these cases, clusters have been defined according to the majority of behaviors making up their composition.

The following paragraphs explain these clusters in detail. The actual comments of respondents are utilized to help obtain a more holistic understanding of PMBs' assignments in the perceptual space of organizational insiders. Table 2.4 displays the clusters' position with the typology, and Appendix B displays the cluster assignments in detail. Figures 2.1, 2.2, and 2.3 graphically display the individual clusters in two- and three-dimensional space.

Table 2.4 Cluster Memberships and Centroid Positions

Cluster Memberships		**Position of Cluster Centroids within Typology**		
		Level of Improvement Required	Level of Standardization and Application	Level of Reasonableness
Cluster ID	**Behavior IDs**			
1	7, 21, 34, 47	Continual	Narrow	Unreasonable
2	9,12,26,64,66	Minor	Wide	Reasonable
3	16,25,28,30,41,54,61	Continual	Wide	Unreasonable
4	19,20,53,65	Continual	Wide	Reasonable
5	24,40	Minor	Narrow	Reasonable
6	13,31,39,46,51,52	Continual	Narrow	Unreasonable
7	17,22,37,44,49	Minor	Wide	Reasonable
8	8	Continual	Wide	Unreasonable
9	3,5,23,29,55,57	Minor	Wide	Reasonable
10	1,2,4,6,10,11,27,33,36,38,45,56,63	Minor	Narrow	Reasonable
11	14,18,58,62,67	Continual	Narrow	Reasonable
12	35,42,50,59,60	Minor	Wide	Unreasonable
13	15,43,48	Continual	Narrow	Reasonable
14	32	Minor	Narrow	Unreasonable

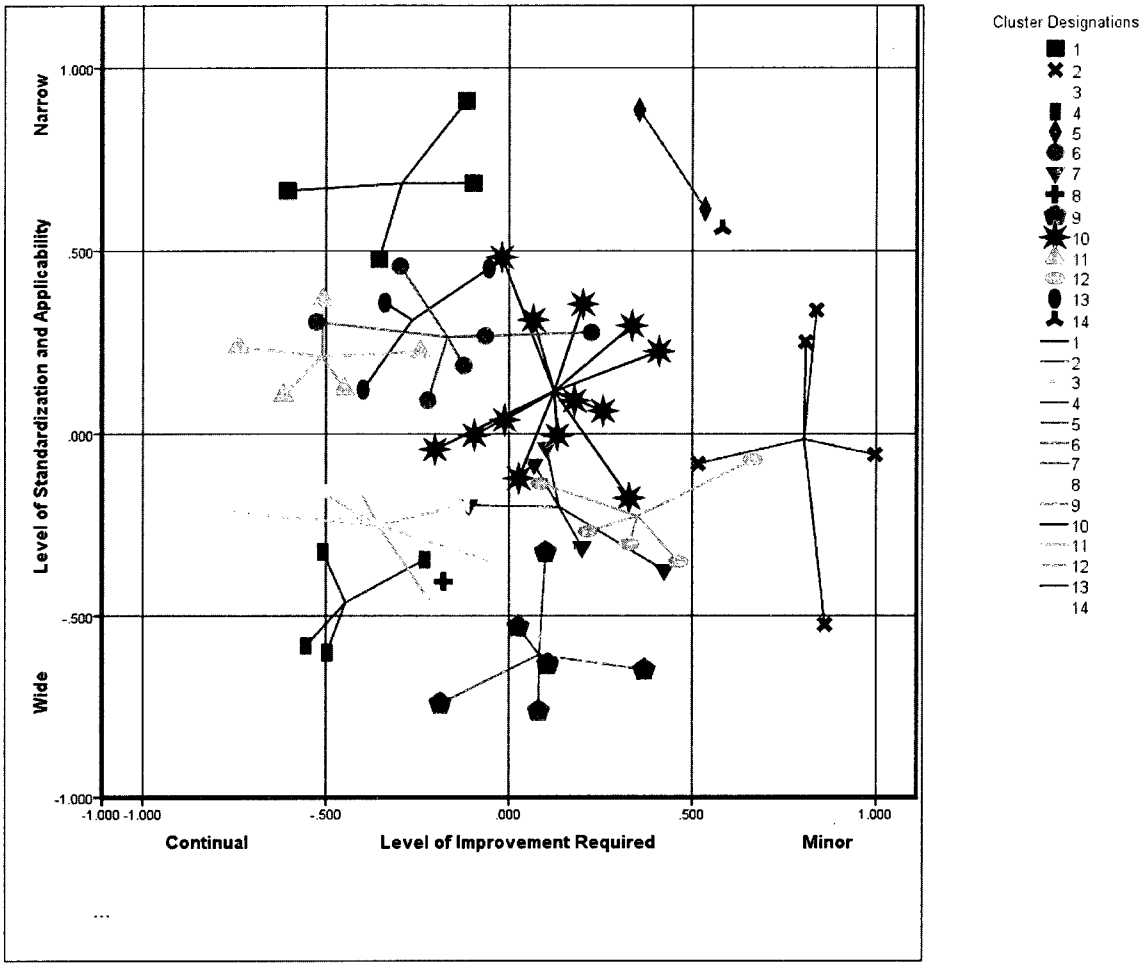


Figure 2.1 Clusters Positioned within Dimensions 1 and 2 of MDS Space

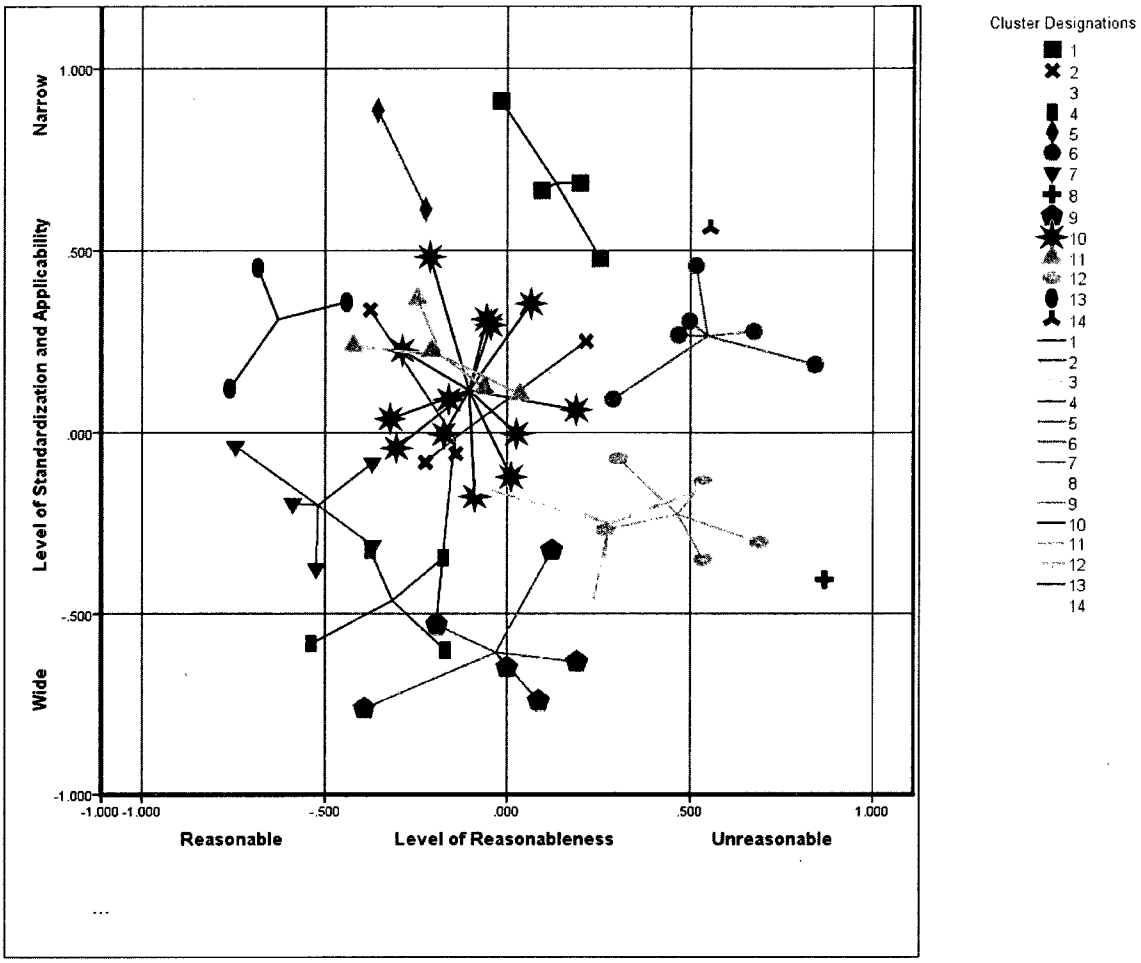


Figure 2.2 Clusters Positioned within Dimensions 2 and 3 of MDS Space

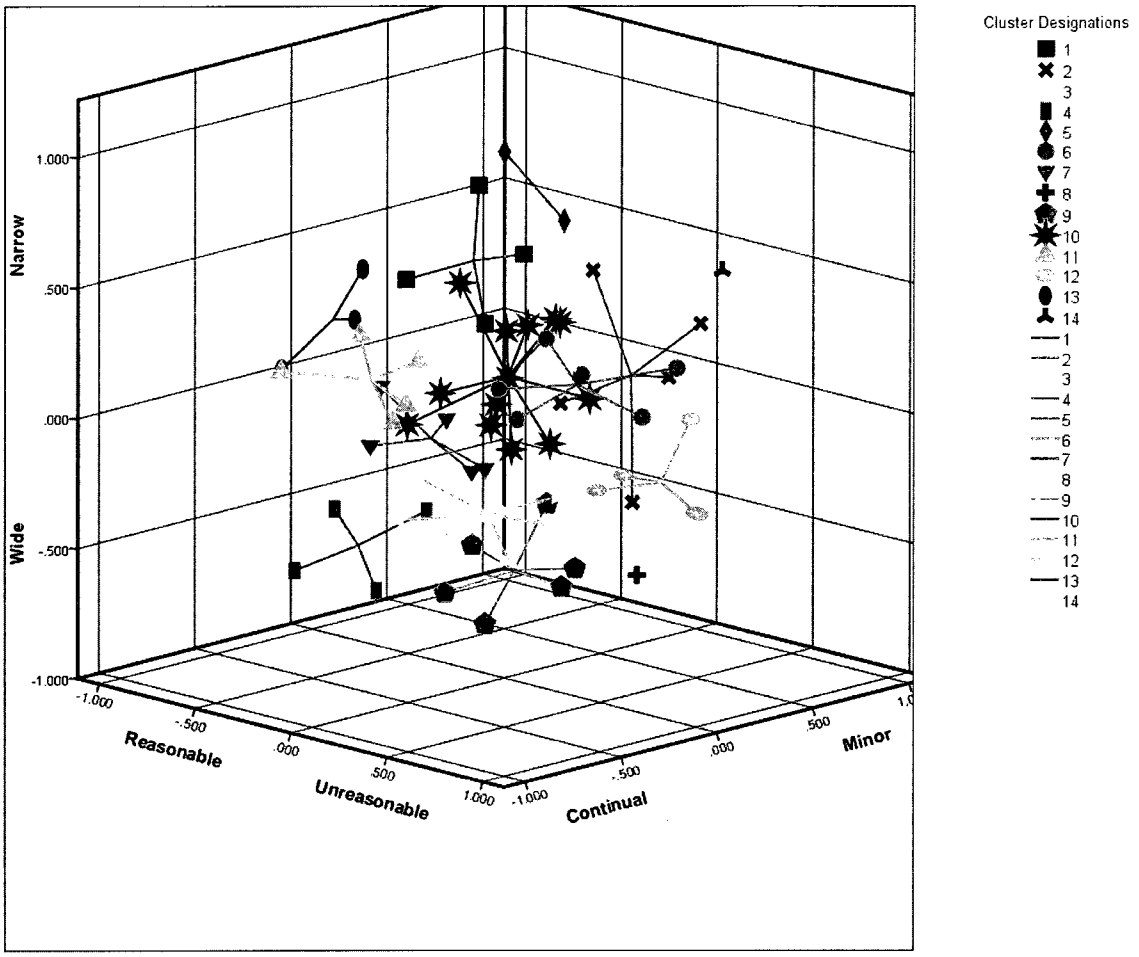


Figure 2.3 Clusters Positioned within All 3 Dimensions of MDS Space

Cluster 1: Legitimate Email Handling
(4 Behaviors: Continual, Narrow, Unreasonable)

The majority of PMBs assigned to cluster 1 deal specifically with insiders' use and handling of corporate email. Respondents continually mentioned that they have difficulty in making a determination as to what specifies "legitimate" electronic communication. Some respondents mentioned that "all emails deserve a response" due to their inability to make this determination. Other comments indicate that many insiders believe that their follow-up to an inadvertent email is necessary only if that email

contained sensitive information, while other individuals believe that they "don't send information that is *THAT* private. [They] would just send it again to the correct address" (emphasis original). Accordingly, legitimate email handling activities require more of an organizational focus to assist insiders in making appropriate determinations of "legitimate" communication attempts and that these behaviors apply to everyone.

Cluster 2: Protection against Unauthorized Exposure (5 Behaviors: Minor, Wide, Reasonable)

The behaviors in cluster 2 are those PMBs that insiders perform to specifically limit the amount of sensitive information unauthorized (both internal and external) individuals are exposed to. PMBs in this cluster describe how insiders manipulate their personal and/or shared workstations to accomplish this goal. Setting a workstation's screen saver to password protect, locking a workstation prior to leaving one's workspace, and logging other individuals out of a shared workstation prior to using it belong in this cluster. These activities are labeled as "most obvious", "follow good business practice", and are "always the best thing to do for everyone." To further protect against unauthorized individuals being exposed to sensitive organizational information, insiders must be careful not to verbally discuss sensitive information in proximity to areas where unauthorized persons are located and to never allow other individuals to do work for which they are responsible as this activity would violate "professional codes of conduct" or "HIPAA regulations."

Cluster 3: Policy-Driven Awareness and Action (7 Behaviors: Continual, Wide, Unreasonable)

Awareness and behaviors rooted in formal corporate policy are assigned to cluster 3. This set of behaviors includes the storing of information and the changing of passwords according to accepted internal security protocol. Further, this behavioral group also includes an insider not using system shortcuts, which use would be against corporate policy. Despite being against corporate policy, individuals responded that "as long as [the shortcut] does not compromise the integrity of my work or the computer system, I will use [it]," "sometimes you need to meet a deadline," and "it depends on how effective [the shortcut] is."

Other behaviors in cluster 3 include not emailing spam to co-workers, notifying those in authority of anything that appears out of the ordinary, and not bringing a laptop from home and attaching it to the corporate network without prior authorization. While these behaviors tend to be heavily documented within many organizations and are widely applicable, the general mindset of insiders indicates that organizations may need to further explain why these activities are important.

Cluster 4: Appropriate Data Entry and Management (4 Behaviors: Continual, Wide, Reasonable)

Cluster 4 is composed of PMBs related to insiders' care for data entry and data management such as the proper disposal of all unneeded sensitive documents and the regular backing up of data and documents. The other two PMBs assigned to this cluster deal directly with the accuracy of data-entry activities (e.g., double checking one's work and working at a cautious but steady pace). Respondents mentioned that they "take pride

in doing [their] job right" and that it is "always wise to have a backup in case something happens to the original documents."

Cluster 5: Document Conversion (2 Behaviors: Minor, Narrow, Reasonable)

Cluster 5 is one of the few clusters whose assigned behaviors appear to be quite dissimilar (i.e., not writing passwords down and converting sensitive documents to PDF to increase security). In this case, the pairing is likely a result of error in the original similarity matrix, and that the former behavior should reside in a cluster closer to the perceptual space axis origin (e.g., cluster 10). The latter behavior of converting sensitive documents to PDF should actually stand alone. In regard to the activity itself, insiders believe that this conversion process is fairly straightforward, does not need to be continually emphasized, and is a reasonable request—especially for "tax related filings," "legal documents whose wording cannot be allowed to be changed," and official corporate documents to be placed on a website—but that it is not normally the requirement of all insiders. The activity of document conversion is different to many of the other behaviors as "PDFs are made to be sent to others."

Cluster 6: Secure Software, Email, and Internet Use (6 Behaviors: Continual, Narrow, Unreasonable)

PMBs located in cluster 6 require insiders to slow their work pace and adjust their normal routine to accommodate organizational information security efforts. For example, immediately applying software updates to one's individual workstation upon receipt of notification is seen as somewhat burdensome. Insiders believe that this activity should be done "as soon as is reasonably possible but not if one is in the middle of a project", while

others see it as "not essential to security" as other actions. Pausing before responding to an email also tends to slow down the workflow, and insiders may only do this if the email is believed to request sensitive information. Further, insiders may be likely to install software on their workstations without prior authorization if they believe the software is useful to their daily tasks. Getting authorization for such a task appears to be a waste of time for both the insider and authorized person(s)—according to the mindset of the insider.

Other PMBs placed in this cluster restrict insiders' use of the Internet and email while at work. Some believe "these are important but often not followed" and see it as an impossibility for them to wholly conform to such restrictions. Insiders justify their actions with statements like "some personal email on a limited basis can be acceptable," "inevitably everyone gets some personal email once in a while," "there are some needs and times for an organizational insider to get personal business done," and should be "allowed as long as they don't distract from getting business tasks done quickly."

Cluster 7: Verbal and Electronic Sensitive-Information Protection (5 Behaviors: Minor, Wide, Reasonable)

Clusters 2 and 7 are in close proximity to each other in the perceptual space of PMBs, and their centroids reside in the same type within the formal typology. As such, some of their behaviors are quite similar. The PMBs in cluster 7 deal with insiders' control of their verbal communication to limit unneeded release of sensitive information. Verbally discussing sensitive information with authorized individuals only and not discussing sensitive corporate information with the media without prior approval reside in this cluster. Not limiting verbal transmission (i.e., "fraternizing") of sensitive

information could cause an insider or organization "to suffer legal issues." In reference to an old U.S. military adage from World War II, several insiders repeated the comment that "loose lips sink ships."

Individuals within organizations must also attempt to limit the exposure of electronic communication and documentation. PMBs stipulating that insiders not allow anyone to look over their shoulder while working on sensitive documents (e.g., using a laptop in a crowded area such as a airport or airplane) and double checking all potential recipients of an email prior to submission decrease the chance that sensitive electronic documentation falls into the wrong hands. Insiders mentioned that they minimize their computer screen if they find someone other than their boss looking over their shoulder. Others stated that they were a bit more cautious and always refrained from working on sensitive material on airplanes.

Cluster 8: Wireless Installation (1 Behavior: Continual, Wide, Unreasonable)

The first of two single-behavior clusters, cluster 8 is comprised by the PMB, which refers to an insider's seeking permission prior to setting up a wireless network access point within the organization. Overall, insiders responded that this activity would be "grounds for dismissal" if prior authorization was not given. However, most respondents stated that they would "have no idea how to set up a wireless access point" and would require training on how to do so. Others mentioned that the installation of wireless access points within the organization is a responsibility of managers or the IT group and to place this responsibility on all insiders to install access points would be unreasonable as they "don't need to worry about this" with everything else they are responsible for.

Cluster 9: Widely Applicable Security Etiquette (6 Behaviors: Minor, Wide, Reasonable)

Clusters 9 and 10 contain behaviors, which are fairly general rules of professional conduct within organizations in regard to the protection of information assets. The key difference between these two sets of behavioral groups is that insiders believe that one set (i.e., cluster 9) is widely applicable to various insiders and positions, whereas the other (i.e., cluster 10) is should be much more restricted to a smaller body of individuals and/or organizations. For example, logging in and out of systems immediately upon completion of job tasks and fully reading and paying attention to organizational security newsletters or other forms of communication should be performed by everyone. However, setting the permissions of files to restrict unauthorized access, while a good general protective behavior, does not appear to be the responsibility of many insiders. Further, all organizations may not issue access cards or give everyone access to important information-security information such as breaches and litigation both of which are necessary to perform behaviors 36 and 63.

Cluster 10: Distinctive Security Etiquette (13 Behaviors: Minor, Narrow, Reasonable)

Admittedly, the behaviors assigned to clusters 9 and 10 span a wide variety of PMBs. It could be argued that some of these activities would be better positioned in one of the other clusters. Despite this possibility, the variety of general behaviors assists researchers in better understanding the delineation between insider behaviors termed "basic hygiene" and "aware assurance" by previous research (Stanton et al. 2005) where

both sets of behaviors are benevolent, but the latter requires more knowledge or expertise on part of the insider to perform.

Cluster 11: Co-worker Reliance (5 Behaviors: Continual, Narrow, Reasonable)

Cluster 11 contains behaviors related to insiders relying on each other for important information-security information and activities within organizations. These behaviors state that insiders have the ability to remind their fellow co-workers of information-security guidelines and policies as well as informing them if they believe they are acting in a manner that would violate these rules. Despite this capability, insiders sometimes feel uneasy or hesitant about approaching one of their fellow employees if there is a chance that they could be incorrect. Some insiders mentioned that these activities require them "to take a leadership role to ensure that others adopt [policy]" and "keeping others out of trouble" even as a simple reminder of the guidelines can avert disaster, while others leave this responsibility to management or the IT security group. Realistically, insiders must use caution in these approaches as they do not want to appear to "support Big Brother" to too large of an extent. However, "call[ing] someone out if they are compromising security" is "a definite must."

Cluster 12: Account Protection (5 Behaviors: Minor, Wide, Unreasonable).

Insiders must protect their system account information, as well as the resources they are able to access under their individual accounts. Accordingly, the PMBs of not allowing anyone else to use a workstation under an insider's personal account and an insider not using another co-worker's account fit into this behavioral group in cluster 12. Moreover, insiders should be concerned with the information resources they access when

properly logged on under their own account. Some respondents mentioned, however, that "if it saves time and won't affect anything, [they] will use another account" and the act largely "depends on the situation" and occurs "only under certain circumstances." Others stated that "it depends on the [insider's] ethics, but if he wants to be treated the same way, he respects the co-worker's privacy" and will do it sometimes if they receive the other insider's permission to access their system.

Cluster 13: Immediate Reporting of Suspicious Behavior (3 Behaviors: Continual, Narrow, Reasonable)

As a major line of defense, organizations rely on insiders to report suspicious physical or electronic activity to minimize potential security threats. Behaviors of this nature are assigned to cluster 13. An example behavior is immediately notifying a co-worker's negligent security-related behavior to the proper internal authorities. Respondents state that while it is an accepted protocol in most organizations, the behavior of blowing the whistle on fellow co-workers should be taken seriously—especially if the co-worker is not looking out for the company's best interest. Individuals also felt the need to first notify the individual, and then if not corrected, go to the higher authorities for notification purposes.

Cluster 14: Equipment Location and Storage (1 behavior: Minor, Narrow, Unreasonable)

Cluster 14 is solely comprised of a PMB that specifies that insiders should always keep electronic devices (e.g., laptops, personal digital assistants) issued to them by their organization with them at all times. While considered a worthy expectation, many insiders stated that always keeping these devices with them "just isn't sensible" because

it "can be under [their] control but not with [them] at all times." This control is accomplished by devices being "locked up at home or hotel room, but they can't be beside you all of the time." While all insiders are not issued portable electronic devices by their organization, respondents mentioned individuals that always have these devices on their person when away from their office were "obsessing with following rules."

Contributions

Contributions to Theory

First and foremost, this research represents the most extensive work to date on the protective role that organizational insiders have in the protection of information and information systems within their firms. These behaviors were defined as protection-motivated behaviors, and both qualitative and quantitative methods were extensively utilized to define the conceptual space of PMBs—until now tasks not found in the academic literature. In doing so, the findings confirm previous suggestions (Ng, Kankanhalli, and Xu 2009) that the positive security-related behaviors organizational insiders can engage in are indeed of a multidimensional nature and have many incarnations.

Second, this chapter appears to be the first work in the IS literature to integrate the multidimensional scaling, property fitting, and cluster analysis techniques to determine the general mindset of subjects of interest. The combination of these techniques provides a much needed rigorous and unique method (Choobineh et al. 2007) to quantitatively define and explain the perceptual space of an entire group of individuals. In this chapter, these techniques (1) have led to the formal development of a typology of PMBs that explains those previously undetermined dimensions and (2) provided a much focused

view of the behaviors clustered together within that typology. With this information, other IS researchers can be made aware of the powerful combination these techniques are and can integrate them into their particular field.

Third, the identification of similarities among various activities within the entire PMB set would likely have been impossible if the behaviors had continued to be studied in isolation or in small subsets (Ng, Kankanhalli, and Xu 2009; Herath and Rao 2009; Workman, Bommer, and Straub 2008; Siponen, Pahnila, and Mahmood 2007; Aytes and Connolly 2004). For example, while seeking to understand why individuals comply with internal security policies is an important endeavor, this research shows that that single activity alone may be much more multifaceted than once believed. The research community now has the opportunity to direct its attention to PMBs in their entirety rather than doing so in a piecemeal fashion.

Fourth, the findings provide the basic foundation from which sound survey instruments measuring PMBs can be developed. Within such development efforts, researchers can determine the nomological network of each type of PMBs as well as the correlates among them. Should the correlates between each of the subsets of PMBs with other related constructs differ, then it is highly likely that the motivational forces for one type of PMBs will not be synonymous with those of another. These findings will be important precursors to the integration and development of theories in the realm of behavioral information security—something that has been lacking in the information-security literature in general (Siponen and Willison 2007).

Finally, this chapter proposes that Protection Motivation Theory (Rogers 1983) is an essential foundation for understanding how and why individuals become motivated to

protect their organizations—not just themselves—from information-security threats. As other researchers posit (Liang and Xue 2009), PMT is a much more appropriate theory from which to study protective behaviors than other foundations, which have flourished for years in the IS literature. Notwithstanding the importance of PMT, it is only a *single* foundational element. The IS community should also continue to embrace and integrate relevant theories and frameworks from such fields as criminology, human communication, organizational and occupational health psychology, and safety. These theoretically derived findings will be vital in recommending solutions to more effectively close the "knowing-doing gap" (Workman, Bommer, and Straub 2008) experienced in many organizations.

Contributions to Practice

It is important to note again that the findings presented in this chapter represent the collective mind of organizational insiders from a wide variety of occupations and industries. Rather than focus only on what information security professionals believe, this research shows that insiders perceive differences among the activities which protect organizations' information and information systems from information-security threats. These findings alone should assist practitioners in (1) determining if they are covering all of the facets of protective behaviors in their individual organizations and (2) approaching employees about their engagement in behaviors from various perspectives depending upon the subset of PMBs under consideration.

For example, security professionals and managers wanting to promote PMBs residing in the narrow level of standardization and applicability might focus much of their efforts in explaining why those behaviors—in regard to that organization—should

be considered the role of everyone within the organization and not just a select few. Likewise, individuals attempting to encourage participation in PMBs framed within the wide level of standardization and applicability are likely to find that many if not all of their insiders already perceive these behaviors as their responsibility. These individuals would then need to ascertain why participation in these behaviors is low given that the insiders already believe in their wide application and are directed to review the other areas of the typology in which those PMBs are situated. Of course, much of the effectiveness of these approaches can be determined through continued academic investigation of the variety of PMBs that were unearthed in this chapter.

Limitations

As with any quantitative technique, MDS and cluster analysis are sensitive to error. As stated in the cluster findings, some of the behaviors assigned to a particular cluster may better fit under the scope of another behavioral grouping. These imperfections are due in large part to the quite sizable number of behaviors being mapped in the MDS perceptual space—often two to three times more than comparable studies (Matook and Vessey 2008; Sircar, Nerur, and Mahapatra 2001)—as well as the number of clusters identified by the initial hierarchical clustering technique. Where possible, multiple configurations and algorithms were used to make decisions for both the MDS and clustering techniques to reduce the potential of being misled by any one approach.

Also due to the number of behaviors being examined, several attempts were made to decrease the error occurring from the data collection efforts. First, respondent fatigue can be a considerable concern when collecting the paired-similarity ratings to be used by the MDS technique. The number of total behavior-pair comparisons to be conducted

follows the formula [n (n+1)] / 2. The reader should clearly be able to understand why an aggregate approach was used, and respondents only received a single behavior to make the paired comparisons between it and the other 66 behaviors. This limitation prohibits us from using other MDS techniques (e.g., INDSCAL), which provide comparisons of the perceptual space between individual respondents.

Second, MDS requires only relevant objects or behaviors to generate a solution of reasonable accuracy. The initial qualitative interviews and subsequent analyses by subject matter experts attempted to ensure that only widely applicable behaviors fitting the definition of PMBs were used. These efforts represent a best attempt to minimize the irrelevant behaviors entering the quantitative analyses; however, it is possible that a few of the initial behaviors were eliminated prematurely from analysis. Despite this possibility, the elimination of irrelevant behaviors is much more important than the inclusion of all relevant ones (Hair et al. 2006; Priem, Love, and Shaffer 2002).

As a final limitation of the study, some of the statistics generated by the ProFit analysis were unexpectedly low upon initial review. For example, the R^2 values were smaller in respect to the findings of other MDS studies (Padgett and Mulvey 2007; Robinson and Bennett 1995). These values are the result of the univariate linear regression technique and are therefore influenced to a large degree by non-linearity of the coordinate points within their dimensions. Figures 2.1, 2.2, and 2.3 display the dispersion patterns of behaviors in the perceptual space and indicate the presence of non-linear relationships. In addition, the number of behaviors in the data set is significantly larger than referent others, thereby making it more difficult to obtain extraordinarily high statistical values.

Conclusion

Organizational insiders play an important role in the information-security efforts of their firms. This chapter reviews these individuals from a more positive perspective than previous research—one that suggests insiders can be motivated to engage in activities that protect rather than solely harm sensitive organizational information and information systems. Further, these behaviors are defined as protection-motivated behaviors (PMBs), and both qualitative (i.e., semi-structured interviews) and quantitative (i.e., multidimensional scaling, property fitting, and cluster analysis) approaches were taken to determine the construct space of PMBs. A series of 67 unique PMBs were found to compose 14 clusters in a three-dimensional solution defined by whether the behaviors (1) required minor or continual level of improvements within organizations, (2) were widely or narrowly standardized and applied throughout various organizations, and (3) were an reasonable or unreasonable request of organizations to make of their insiders. These findings offer significant benefits to the research targeting behavioral information security matters and practitioners who are given the responsibility of overseeing such protective efforts within their organizations.

CHAPTER 3

PROTECTION-MOTIVATED BEHAVIORS OF ORGANIZATIONAL INSIDERS: CONCEPTUALIZATION, MEASUREMENT, AND NOMOLOGICAL VALIDITY

Introduction

Organizations expend a significant amount of financial resources to protect information from security threats. Institutions worldwide continue to enlarge their budgets on information-security initiatives despite the recent fluctuations of many national economies (Gartner 2009; van Kessel 2009). For example, a recent study using responses of more than 7,000 upper-level managers in over 130 countries provides evidence that the majority of organizations remain willing to support information security efforts despite difficult economic times (CIOMagazine, CSOMagazine, and PricewaterhouseCoopers 2009). This support, however, comes with increased scrutiny on the performance of security initiatives as they are receiving the funds other worthwhile organizational programs are being denied (CIOMagazine, CSOMagazine, and PricewaterhouseCoopers 2009).

In this quest to protect information, practitioners and researchers have traditionally focused their efforts on the acquisition and capabilities of new technologies. Notwithstanding the importance of these advancements, information-security efforts must also be concerned with human behavior–in particular, the behaviors of those within organizational walls. These individuals often get branded as the "weakest link" in the

information-security chain (Mitnick 2003; Dhillon 2001; Vroom and von Solms 2004) and are subjected to formal security education, training, and awareness programs that attempt to deter them from engaging in detrimental behaviors (D'Arcy and Hovav 2007).

What many managers within these organizations fail to acknowledge, however, is that employees can also be utilized as the best line of defense against information-security threats. Only recently have researchers fostered the perspective that organizational insiders can be a significant weapon in the war against security threats (Stanton and Stam 2006; Stanton et al. 2005). These organizational insiders—resources already acquired by the organization—have immense control over the sensitive information that is gathered, maintained, and disseminated by their firms. Organizational information protection can only be achieved when a simultaneous understanding of (1) how to deter detrimental human behavior *and* (2) how to motivate the beneficial activities of organizational insiders is obtained (Stanton et al. 2005). Relative to the former, the latter facet of this axiom remains largely unexplored.

This research has two main goals. First, I explore these positive insider behaviors in interviews with 33 working professionals and information-security experts. I term these activities *protection-motivated behaviors (PMBs)*, which are the volitional behaviors organizational insiders can enact that protect (1) organizationally-relevant information within their firms and (2) the computer-based information systems in which that information is stored, collected, disseminated, and/or manipulated. The findings from the interviews coupled with data from several end-user surveys provide the necessary steps to not only define the criterion space but to also develop and validate a self-report measure of PMBs.

Second, once a new construct is defined and developed, it is important to determine how it relates with other variables of interest in the organizational literature. Therefore, the nomological network of PMBs is investigated for the first time. From PMBs' associations with various insider traits, perceptions, and activities, I offer suggestions about how organizations can promote the positive, security-oriented behaviors of organizational insiders. I also provide guidance for future theoretical development efforts in the literature on PMBs.

Literature Review

The research stream that focuses on the human element in the protection of information has been termed *behavioral information security* (Fagnot 2008; Stanton et al. 2006). This field emerged as researchers acknowledged that information security is not just a technical concern based on electrical engineering and computer science foundations but a managerial and behavioral one rooted in applied psychology and organizational behavior as well (Dhillon and Torkzadeh 2006; Choobineh et al. 2007). For some time, researchers in this stream have chosen to concentrate on the methods by which organizations can deter individuals from engaging in activities that are detrimental to organizational information security. This deterrence has largely been shown to be a function of employees' perceptions of potential sanctions for their non-compliant behavior (D'Arcy, Hovav, and Galletta 2009; Straub 1990; Lee, Lee, and Yoo 2004; D'Arcy and Hovav 2007; Theoharidou et al. 2005). One of the most studied of these detrimental behaviors is internal computer abuse, which is the intentional act of harming or destroying organizational data, networks, hardware, software, and services by individuals within the organization (Lee, Lee, and Yoo 2004; Straub 1990; Straub and

Nance 1990; Harrington 1996). This perspective of focusing on the negative behaviors of insiders continues to flourish due to the reputational and financial damage these breaches create for organizations and their stakeholders (ITRC 2009).

Recently, researchers have issued calls to incorporate frameworks outside the deterrence-based ones derived from criminological fields with non-deterrent foundations that help explain the motivational forces behind security-related behaviors (Siponen and Oinas-Kukkonen 2007; Im and Baskerville 2005). Studies currently provide evidence that organizational insiders can be used to promote the well being of organizations' information and information systems. For example, basic protective actions of individuals within organizations such as "safe computing practices" (e.g. the regular backing up of data, scanning email attachments for viruses, voluntarily changing of passwords, and refusing to share passwords) (Aytes and Connolly 2004) and behaviors requiring general caution when using email (Ng, Kankanhalli, and Xu 2009) have been explored. Adherence to information-security policies (Siponen, Pahnila, and Mahmood 2007) and other general protective measures (Workman, Bommer, and Straub 2008) have also received some attention.

Previous research in behavioral information security has provided evidence that organizational insiders are not inherently bad and do not necessarily want to engage in detrimental information security behaviors. There is little doubt that organizational insiders do intentionally engage in behaviors that can create great harm to organizations (Straub 1990; D'Arcy, Hovav, and Galletta 2009; Moore, Cappelli, and Trzeciak 2008), but they are just as likely to do so from basic human error or on accident (Im and Baskerville 2005). Conversely, it appears that insiders have largely been overlooked as a

considerable source of behaviors that protect organizational information resources (Albrechtsen and Hovden 2009).

The protective behaviors that have been examined are but a few that exist in the wide variety of security countermeasures available to insiders (Workman, Bommer, and Straub 2008). Researchers have even explicitly stated that the behaviors of interest in their work were but a small subset of a larger, multidimensional structure of protective insider actions (Ng, Kankanhalli, and Xu 2009). Scholarly efforts that focus only on a single activity or a small subset of behaviors that exist as a component of a larger behavioral structure hamper the ability to understand all of the forces that act upon the overall structure of interest (Hanisch and Hulin 1991; Hanisch, Hulin, and Roznowski 1998). The concept of PMBs has not yet been explicitly explored and examined in the framework of similar and dissimilar behaviors of individuals within organizations.

In the next section, I provide an in-depth view of the conceptualization of these protective behaviors, which have been termed PMBs. This emphasis is a mandatory precursor to the development of any new measure. Moreover, it is expected that the formal conceptualization will assist in theoretical advancement in the field of behavioral information security. Following the discussion of the PMB construct, hypotheses in regard to the structure of the nomological network surrounding the new construct are proposed.

Conceptualization

There are many facets to the conceptualization of PMBs that must be considered before they can be measured. First, insiders engaging in PMBs feel a responsibility to protect their organization and its information and computerized information systems from

both external and internal information-security threats. This feeling of responsibility is an important concept in information security (Dhillon and Backhouse 2000; Albrechtsen and Hovden 2009). It may emerge from various sources including but not limited to commitment to the organization and the organization's customers, a feeling of personal pride in the profession or self, job security, or incentives. These actions are insiders' attempts at reducing the potential harm experienced by information-security threats. However, there is no guarantee that these actions will successfully decrease the likelihood of a breakdown of organizational security.

Second, PMBs are referred to as volitional activities on part of the organizational insider. These individuals have immense control over the information they are exposed to in their jobs (Stanton and Stam 2006) yet have a choice of whether to actively protect it or not. Considering the speed with which security threats can inflict harm, the term *volitional* implies that quick and decisive action must be taken by insiders against these threats as they perform their other daily tasks. In some instances, protection against these attacks requires an almost immediate response by the insider once a threat is identified (Hamill, Deckro, and Kloeber 2005). In these cases, organizational insiders must make a prompt decision about their course of action, and choosing not to do so for even a single threat can lead to a significant loss. Decisions that do not successfully inhibit information-security threats may be grounds for formal punishment of employees by organizations; however, it is ultimately up to the insider to actively decide how s/he handles such situations regardless of the end result. Punishment of an insider following a successful security breach that is linked to the inability of the insider to be a protective

steward is a way to deter human error or lapse in judgment rather than to decrease the disturbance caused by the security attack itself.

Third, PMBs differ from other positive sets of behaviors within organizations (e.g., proactive behaviors, taking charge, organizational citizenship behaviors) as they quite possibly consist of both in-role and extra-role behaviors. For example, the failure of insiders to engage in extra-role behaviors does not place the insider at risk for punishment as the behaviors are not stated contractual obligations (Organ 1988). PMBs, on the other hand, represent behaviors likely addressed in formal information security education, training, and awareness (SETA) efforts as well as activities that require insiders to go beyond their explicitly stated duties. As SETA approaches and successes vary significantly from one organization to the next (Whitman and Mattord 2009; Siponen 2000) and as organizations differ in their information security needs (Siponen and Willison 2009), the percentage of PMBs that are in-role and extra-role will not be consistent across firms and situations. Accordingly, organizations do not view information security issues in a standardized form, and insider engagement in PMBs may be formally rewarded in some organizations and not at all in others. All PMBs are geared toward the protection of the organization from security threats, but some manifestations may be more sought after and may be more beneficial in the overall protection efforts than others. In summary, all PMBs may not be created equal.

Fourth, the acquisition of new technological advancements and the exposure of insiders to increasing amounts of organizational information (Dhillon and Backhouse 2000) mandate that insiders perform regular, active scanning for information security issues—both in the physical and the digital domains. These increasing demands may

place constraints on employees with which they are not accustomed. Further, information-security threats take many forms, and the insiders' awareness of these various manifestations can make an already stressful job more demanding (Albrechtsen and Hovden 2009). These adaptations are a crucial component in insiders' ability to protect an organization against security threats.

Finally, insiders may expend more effort to engage in certain PMBs over others. Certain behaviors may require insiders to use their best judgment about what constitutes an information-security threat. For example, properly logging in and out of computer systems in the workplace when completed with job tasks is straightforward. Reporting a fellow co-worker's negligent actions to management, however, requires an insider to make such a call and the insider may feel reluctant to turn the other individual in to the proper authorities. The insider's reluctance in this case likely stems from the possibility that s/he has falsely accused a fellow co-worker of being a security threat who now must endure sanctions or other repercussions. Therefore, organizations cannot assume that their employees' willingness to engage in all of the PMBs will be equal as various dimensions and behavior clusters have been discovered.

Addressing Nomological Validity

The assessment of the nomological validity of any measure is an important step in its overall validation (Bagozzi 1980; Straub, Boudreau, and Gefen 2004). Nomological validity requires an analysis of intercorrelations between a measure and its proposed antecedents, correlates, and/or consequences to determine if they are greater than zero (MacKenzie, Podsakoff, and Jarvis 2005). This section provides the rationale for the inclusion of several antecedents, correlates, and a consequence to be tested in the

nomological validity assessment of the newly derived measure of PMBs. Figure 3.1 displays the suggested framework for assessing the nomological validity of PMBs.

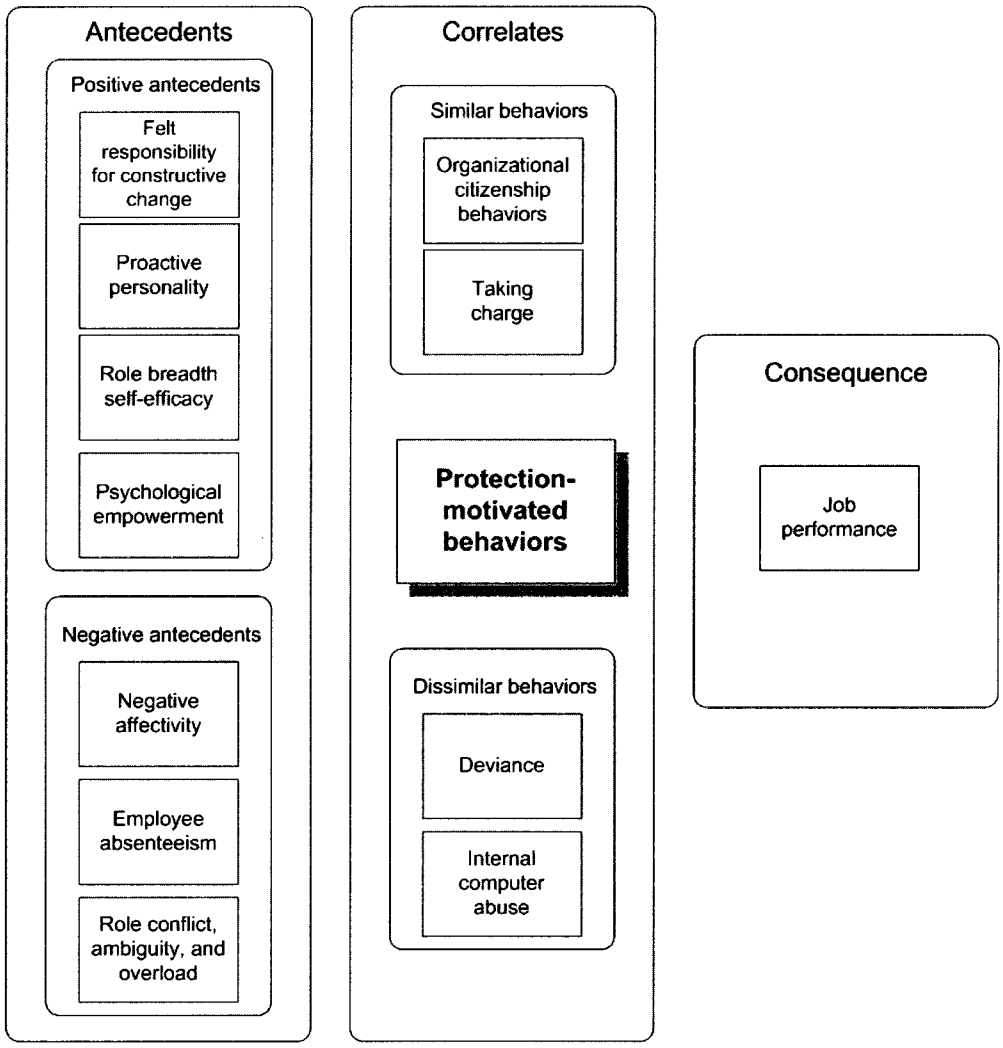


Figure 3.1 Structure Used to Assess the Nomological Validity of PMBs

Antecedents

Positive Correlations

Felt responsibility for constructive change (FRCC)

FRCC represents "an individual's belief that he or she is personally obligated to bring about constructive change" (Morrison and Phelps 1999, p. 407). Individuals who feel responsible for their work are more likely to produce higher quality outputs (Hackman and Oldham 1975) and are more likely to engage in positive behaviors such as continuous improvement and extra-role efforts (Fuller, Marler, and Hester 2006; Morrison and Phelps 1999; Pearce and Gregersen 1991). Likewise, individuals who engage in PMBs do so because they believe they have a personal responsibility to protect their organization's information and computerized information systems from security threats. Therefore, it is expected that FRCC will be positively associated with PMBs.

Hypothesis 1: PMBs are positively correlated with FRCC.

Proactive personality

Proactive personality represents an individual's relatively stable drive to effect change in the workplace (Bateman and Crant 1993). More specifically, individuals exhibiting a proactive personality "scan for opportunities, show initiative, take action, and persevere until they reach closure by bringing change" (Bateman and Crant 1993, p. 105). This perseverance leads individuals of a proactive demeanor to achieve higher levels of job performance (Thompson 2005; Crant 1995) and career success (Seibert, Crant, and Kraimer 1999) than those who do not have a proactive personality.

Individuals engaging in PMBs must remain aware of the many ways that information-security threats attack their organization's information and computer

systems. This active scanning and endurance under the stresses of daily organizational life appears closely in line with individuals maintaining a proactive personality. Further, it is possible for organizational insiders to be rewarded for their active efforts to protect their organizations from significant security threats through higher performance appraisals and promotions. Therefore, a significant positive correlation should exist between proactive personality and PMBs.

Hypothesis 2: PMBs are positively correlated with proactive personality.

Role breadth self efficacy (RBSE)

RBSE "refers to employees' perceived capability of carrying out a broader and more proactive set of work tasks that extend beyond prescribed technical requirements" (Parker 1998, p. 835). These individual perceptions of being capable of effectively handling a variety of workplace situations is important as modern work environments encourage diversified employee activity (Parker 2000; Judge et al. 2007). As organizations continually invest in technologies and other methods of dealing with information-security threats, employees must be able to quickly adapt to a diverse set of circumstances and job requirements. PMBs represent a wide variety of protective behaviors, and it is expected that individuals exhibiting high levels of RBSE will exhibit an increased positive association with the PMB measure.

Hypothesis 3: PMBs are positively correlated with RBSE.

Psychological empowerment

Psychological empowerment represents an active rather than passive orientation to one's work role and is composed of four unique components (Thomas and Velthouse 1990): (1) *meaning*—the degree to which the work role and the individual's beliefs,

values, and behaviors mesh; (2) *competence*—synonymous with self-efficacy, it represents an individual's belief of capability of performing a specified task; (3) *self-determination*—the degree to which individuals believe they have choice in their engagement of organizational behaviors; and, (4) *impact*—the degree to which individuals perceive that their efforts in the workplace have the ability to influence the overall outcomes of their organization (Spreitzer 1995). Research has shown that empowered individuals are more committed to their organizations (Avolio et al. 2004), are seen as having more innovative leadership characteristics (Spreitzer, de Janasz, and Quinn 1999), and are more likely to perform creatively and engage in organizational citizenship behaviors (Alge et al. 2006).

First, in regard to PMBs, if organizational insiders do not feel connected to their work (i.e., meaning), they are less likely to engage in behaviors that potentially go beyond their stated job roles and as such require more effort on their part. Second, similar to the argument about RBSE, individuals who are confident and believe in their abilities (i.e., competence) to effectively protect their organization from information-security threats will engage in more PMB activity. Third, much control over organizational information is given to insiders during their daily tasks. The more likely these individuals perceive that their organization trusts them and believes that they will engage in proper behavioral choices, the more likely insiders will appropriately utilize their right to choose (i.e., self-determination). Finally, information-security threats, if successful, can cause a myriad of problems for organizations, employees, consumers, and essentially any other stakeholder group. Unless organizational insiders believe that their efforts to protect their institutions from these harmful attacks are influential (i.e., impact), they cannot

realistically be expected to engage in PMBs, which require an active and widespread approach to information security on a daily basis.

Hypothesis 4a: PMBs are positively correlated with meaning.

Hypothesis 4b: PMBs are positively correlated with competence.

Hypothesis 4c: PMBs are positively correlated with self-determination.

Hypothesis 4d: PMBs are positively correlated with impact.

Negative Correlations

Negative affectivity (NA)

The disposition to experience negative emotions independent of contextual stressors has been defined as negative affectivity (Watson and Clark 1984; Watson and Pennebaker 1989). Individuals high in NA tend to concentrate on the negative characteristics of themselves and the world around them (Watson and Clark 1984). These individuals experience decreased satisfaction in their jobs (Connolly and Viswesvaran 2000), more issues of stress (Moyle 1995) and work-family conflict (Stoeva, Chiu, and Greenhaus 2002), and engage in more deviant behaviors than their low-NA counterparts (Aquino, Lewis, and Bradfield 1999). Conversely, research shows negative relationships between NA and organizational citizenship (Hui, Law, and Chen 1999) and prosocial behaviors (George 1990). It is expected, then, that individuals who are prone to dwell on negative aspects of themselves and their environment are not likely to expend effort in protecting their organizations from information-security threats.

Hypothesis 5: PMBs are negatively correlated with negative affectivity.

Employee absenteeism

Employee absenteeism has been shown to lead to decreased employee performance, increased turnover, and significant organizational expense (Harrison and Martocchio 1998). Individuals who are not committed to their organizations often engage in absenteeism (Somers 1995; Luchak and Gellatly 2007). Of particular importance for information-security research is that absenteeism can lead individuals in dangerous environments to become unfamiliar with safety procedures of their organizations, thereby increasing the occurrences of workplace accidents (Goodman and Garber 1988). As almost all organizations experience information-security threats of some kind, it seems reasonable to surmise that individuals who are frequently present in their organizations would become more familiar with security policies and procedures, which hopefully translates into more PMB activities within organizations. Further, formal SETA activities may help increase an individual's sense of personal responsibility to protect the organization, thereby also increasing PMBs within firms.

Hypothesis 6: PMBs are negatively correlated with employee absenteeism.

Role conflict, ambiguity, and overload

Individuals assume various roles within organizations for their firms' basic functioning (Katz and Kahn 1978). Unfortunately, organizational members experience (1) conflict between various tasks that each require employees' attention (i.e., role conflict), (2) uncertainties in regard to what is believed to be expected of employees (i.e., role ambiguity), and (3) potential burden with being given too many tasks and demands at a single time (i.e., role overload). These issues regarding individuals' role have been linked with decreased member satisfaction, organizational commitment, and job

involvement, and increased anxiety and turnover intentions among others (Bedeian and Armenakis 1981; Rizzo, House, and Lirtzman 1970; Tubre and Collins 2000).

In today's fast-paced, technology-driven environments, individuals may be more prone to experience such negative aspects of their roles. These environments push more organizational information to their members (Dhillon and Backhouse 2000)—thereby inundating them with increasing chances to make errors in their tasks while also requiring them to be adept in business activities in both the physical and electronic realms. Further, as these systems expand, organizations will struggle to thoroughly assign all of the roles which the organizational members are expected to fill. Therefore, individuals experiencing role conflict, ambiguity, and overload will do so because they are told to quickly accomplish their tasks yet they must slow their pace to do so in a secure manner, they are not completely aware of what is expected of them, and they are overloaded with ever increasing demands.

Hypothesis 7a: PMBs are negatively correlated with role conflict.

Hypothesis 7b: PMBs are negatively correlated with role ambiguity.

Hypothesis 7c: PMBs are negatively correlated with role overload.

Correlates

Similar Behaviors

Organizational citizenship behaviors (OCBs)

OCBs are defined as "individual behavior that is discretionary, not directly or explicitly recognized by the formal reward system, and in the aggregate promotes the efficient and effective functioning of the organization" (Organ, Podsakoff, and MacKenzie 2006, p. 3). Forms of OCBs have been shown to increase performance

quantity and quality (Podsakoff, Ahearne, and MacKenzie 1997) and general organizational effectiveness (Podsakoff et al. 2000). Despite being originally conceptualized as composed of several individual components (Organ 1988), researchers frequently examine OCBs along two dimensions: OCBs directed towards individuals (i.e., OCBIs) and OCBs directed at the organization (i.e., OCBOs) (Lee and Allen 2002; Williams and Anderson 1991; Aryee, Budhwar, and Chen 2002; Podsakoff et al. 2009).

Because both OCBs and PMBs are activities designed to promote the effectiveness of the organization, it is expected that a positive correlation will exist between these two sets of behaviors. Furthermore, PMBs contain protective behaviors that require interactions with co-workers. This multifaceted characteristic of PMBs should result in positive associations of PMBs with both the individual and organizational components of OCBs.

Hypothesis 8a: PMBs are positively correlated with OCBOs.

Hypothesis 8b: PMBs are positively correlated with OCBIs.

Taking charge

Taking charge represents the volitional, extra-role behaviors of employees to bring about positive change in the workplace through modifications to work execution (Morrison and Phelps 1999). These activities along with other proactive behaviors have been expanded by researchers into the domains of proactive idea implementation and proactive problem solving (Parker, Williams, and Turner 2006). Further, such efforts are focused on changing the status quo by bringing about increased organizational effectiveness rather than personal gain and are experienced within organizations when

individuals feel they have a duty or obligation to watch out for the welfare of the organization (Moon et al. 2008).

Similar to taking charge, PMBs are conceptualized as being fostered by feelings of personal responsibility for an organization's (and an organization's customer's) sensitive information from their information-security threats. Individuals may find certain aspects of their job, which they feel may need to be redesigned in order to facilitate such protective efforts. Therefore, individuals who take charge are likely to also engage in PMBs.

Hypothesis 9: PMBs are positively correlated with taking charge.

Dissimilar Behaviors

Deviance

Individuals within organizations may engage in behaviors that bring harm to the organization, its members, or both (Bennett and Robinson 2003; Robinson and O'Leary-Kelly 1998). These activities are detrimental to the mission and goals of organizations and exhibit significant negative correlations with OCBs (Berry, Ones, and Sackett 2007). Accordingly, individuals who engage in OCBs are less likely to engage in counterproductive work behaviors regardless of the target (Dalal 2005). Likewise, PMBs should have a negative association with both interpersonal and organizational deviance.

Hypothesis 10a: PMBs are negatively correlated with organizational deviance.

Hypothesis 10b: PMBs are negatively correlated with interpersonal deviance.

Internal computer abuse

As a more specialized and technologically based form of deviance, internal computer abuse is defined as "the unauthorized and deliberate misuse of assets of the

local organizational information system by individuals" (Straub 1990, p. 257). This insider threat has recently become the focus of information-security researchers (Theoharidou et al. 2005; Willison and Backhouse 2006; Dhillon and Moores 2001) as many organizations experience costly abuses from their employees (Moore, Cappelli, and Trzeciak 2008). Individuals engaging in PMBs, however, certainly do not want to harm their organizations; rather, they are attempting to protect organizations from both external and internal security threats.

Hypothesis 11: PMBs are negatively correlated with internal computer abuse.

Consequence

Job Performance

Individuals who exhibit positive behaviors in their organizations (e.g., OCBs) are given higher performance evaluations and rewards for achievement than those who do not (Podsakoff et al. 2009; Organ, Podsakoff, and MacKenzie 2006). In similar fashion, individuals who actively protect an organization from information-security threats would likely be seen by management as more effective performers. Therefore, individuals who make considerable efforts to protect sensitive information from being breached are more likely to be viewed as a vital resource, which should translate into higher performance evaluations than those received by individuals who are less protection oriented.

Hypothesis 12: PMBs are positively correlated with job performance evaluations.

Methodology

Data Collection

Study 1: Instrument Development

Phase 1: Item generation

The initial step in item generation is to conduct a thorough review of the literature relating to individuals within organizations protecting the organizations from information-security threats. Limited research cited such behaviors (Ng, Kankanhalli, and Xu 2009; Stanton and Stam 2006; Workman, Bommer, and Straub 2008), and most of the existing behaviors that I did find were discovered in a professional certification text. In order to generate additional behaviors, I conducted interviews with 22 working professionals and 11 information-security experts. Table 1 displays the qualifications of the interviewees. Following professional transcription efforts, QSR International's NVivo 8 software was used during content analysis to help elicit the individual behaviors mentioned during the 33 interviews. Two raters not associated with the research independently assessed the elicitation and raised only a few concerns, which were discussed with me. A total of 160 protection-motivated behaviors were elicited from both the interviews and the literature search.

To ensure that the vast majority of PMBs were gathered from the literature review and the interviews, 100 panelists from panel provider Zoomerang were asked to list one or two ways in which they could protect their organization's information and/or computerized information systems from security threats. The use of external panels has received increasing attention in academic literature often as a way to target participants of a specific population or to attain responses from a generalizable spectrum of individuals

(Gibney, Zagenczyk, and Masters 2009; Awad and Ragowsky 2008; Shang, Basil, and Wymer 2010; Posey, Lowry et al. 2010). No new behaviors were added to the original set, and it was reasonably concluded that the wide set of behaviors making up PMBs were ready for review. This sample from a wide variety of industries and job positions was 51.5% female, 80.8% full-time employed, and 41.4% in a managerial role within their firms. The average respondent was 43.2 years (SD = 13.82) of age and had been employed by their current organization for 9.4 years (SD = 7.78). Respondents estimated their time spent on their organization's computer systems during the average work day to be 64.5% (SD = 30.76%).

Phase 2: Item review

Two steps were taken to review the 160 behaviors in order to make inclusion / exclusion decisions. First, one rater with significant professional experience assisted in the removal of behaviors having significant redundancy. This review left 92 unique behaviors.

Second, a more rigorous assessment was performed on the 92 unique behaviors by ten subject-matter experts (SMEs) (three professors of computer information systems, two professors of management, and five graduate information systems students with significant professional experience). Each behavior was rated by the SMEs along a 7-point Likert scale on three factors: (1) the behavior's fit to the definition of PMBs; (2) the clarity of the behavior's wording; and, (3) the behavior's applicability to a wide range of occupations and industries. The SMEs' ratings were averaged, and behaviors receiving a four or less on any of the three above factors were considered for either minor alterations

or elimination. Sixty-seven behaviors emerged as the unique set of PMBs to undergo further analyses.

Study 2: Instrument Refinement

Phase 1: Item selection process

PMBs represent a wide variety of protective behaviors. As such, if an individual within an organization performs at least one of these activities, the individual has engaged in PMB activity. Constructs composed of items such as these form a formative measure rather than a reflective measure and require different validation techniques (Diamantopoulos and Winklhofer 2001; MacKenzie, Podsakoff, and Jarvis 2005). For example, items in a formative construct need not exhibit significant covariance with each other—a requisite condition for classical reflective measures (Diamantopoulos and Siguaw 2006; Wilcox, Howell, and Breivik 2008). Moreover, because the development of a formative measure requires the inclusion of as many if not all of the relevant factors composing a construct, the validation process should not solely rely on statistical information. One of the main purposes of this research is to develop the PMB measure that is widely applicable to many individuals within various industries. Therefore, the exclusion of behaviors at this point in the analysis requires a careful tradeoff between limiting the generalizability of the measure while making certain that the entire criterion space remains intact.

Several steps were taken to assess the formative measure of PMBs. First, another 200 Zoomerang panelists from a wide variety of industries indicated the frequency of their engagement in each of the 67 behaviors within the last year on a 7-point Likert scale (*1=Never; 7=Always*). Very similar to the previous sample of respondents, this sample

was 48.3% female, and 76.1% of the respondents were employed full time within their firms. Further, 36.3% of the respondents were managers, and the average age and organizational tenure were 43.9 years (*SD* = 14.28) and 9.7 years (*SD* = 8.82), respectively. The estimated percentage of time spent on organizational computer systems was 67.6% (*SD* = 29.08). Respondents were also given the option to indicate whether the individual behaviors were not applicable in their workplace. Because the PMB measure must be generalizable to a wide variety of occupations and industries, a behavior that received 25% or more "not applicable" responses were excluded from the set of PMBs. Eleven behaviors—mostly requiring a highly technical aptitude to perform—met this exclusion criterion, leaving 56 behaviors for further analysis.

Second, individual behavior correlations with a measure external but related to the formative construct should be assessed for an initial determination of internal validity (Diamantopoulos and Winklhofer 2001). Items not exhibiting a significant association should be considered for removal. The items developed for this process included five reflective indicators that captured the overall definition of PMBs (see Appendix A). These items were also used for identification purposes of structural equation models to counter the degrees of freedom consumed by formative measurement in structural equation models (Diamantopoulos and Winklhofer 2001; Hair et al. 2006). This reflective measure of PMBs exhibited adequate internal consistency (Cronbach's $\alpha = 0.84$; Average Variance Extracted = 0.53) (Nunnally 1978; Fornell and Larcker 1981). All but 9 of the 55 behaviors exhibited significant associations with this global measure at the 0.05 level of significance. Therefore, the majority of the items in the formative PMB measure

exhibited satisfactory initial internal validity. Items not significantly correlated with the reflective measure were evaluated for potential wording alterations.

Third, inter-item correlational and collinearity analyses were performed to assess high correlations and multicollinearity levels, both of which weaken formative measures. The inter-item correlations were assessed, and those behaviors showing strong associations with others were placed under scrutiny for removal. Six behaviors were deemed to be replicas of others and were discarded from the PMB set, which now contained 50 widely applicable behaviors. The summated formative measure was then regressed on the 50 independent behaviors to check the collinearity statistics. While variance inflation factors (VIFs) less than 10 are traditionally justified as lacking multicollinearity, methodologists have recently called for a more stringent cutoff of 3.3 (Diamantopoulos and Siguaw 2006; Petter, Straub, and Rai 2007). While none of the VIFs quite reached the 3.3 cutoff, nearly one-third of the individual regression coefficients exhibited a negative sign—a counterintuitive finding that suggests multicollinearity might be present. Similar results were also obtained when using the global reflective measure as the dependent variable in the regression equation.

Since deleting any behaviors risked eliminating important behavioral information, suggestions of research methodologists (Petter, Straub, and Rai 2007) were followed, and the PMB construct was modeled as a second-order construct with multiple first-order subconstructs also formative in nature. This modeling of the PMB measure is in line with mainstream PMB research, which suggests that the nature of protective security behaviors is multidimensional (Ng, Kankanhalli, and Xu 2009). Findings from the second chapter of this dissertation shows that these first-order clusters are: (1) account

protection; (2) co-worker reliance; (3) data entry and management; (4) distinct security etiquette; (5) general security etiquette; (6) immediate reporting of suspicious activity; (7) legitimate email handling; (8) policy-driven awareness and action; (9) protection against unauthorized exposure; (10) secure software, Internet, and email use; (11) verbal and electronic sensitive-information protection; and (12) wireless installation. Two of the original clusters (i.e., document conversion and equipment location and storage)—both composed of only one or two behaviors—were removed during the quantitative tests stated above.

To determine the composition of each first-order cluster, the behaviors were examined using principal components analysis (PCA) rather than exploratory factor analysis (EFA). PCA is similar to regression in that individual indicators (i.e., independent variables) explain variance in a construct (i.e., dependent variable) whereas EFA is used to show how a construct explains variance in its indicators (Petter, Straub, and Rai 2007). The findings from PCA were used in conjunction with the assignments represented in Chapter 2.

Study 3: Exploring the Nomological Validity of PMBs

To empirically assess the nomological validity of the newly formed PMB construct as defined by the formal hypotheses, other validated measures in the academic literature were used to capture the other constructs of interest. Where possible, the individual instruments were shortened in their number of items to reduce the overall length of the survey. Factor loadings published in the original developmental pieces were used to make these decisions, and the highest loading items were included.

Responses to this survey were acquired via another independent sample from Zoomerang's panel. Respondents (n = 365) averaged 44.7 years of age (SD = 14.36) with 9.4 years of organizational tenure (SD = 8.99). The 52.9%-female sample consisted of 32.6% managers and 78.9% full-time employed individuals who use their organization's computers systems 65.6% (SD = 32.24) of the time during their daily work schedules.

Revising the PMB Structure

Prior to performing the correlational analysis, it was necessary to check the structure of the PMBs from an empirical standpoint. This structure of PMBs (i.e., PMBs being formed by the 12 individual behavior clusters) was placed in the structural equation modeling program AMOS. The originally proposed structure exhibited the following statistics: χ^2 = 113.72, df = 53; CFI = 0.977; RMSEA = 0.056.

While these statistics indicate the structure's adequate fit to the data (Hair et al. 2006), a review of the inter-cluster correlations showed several high correlations that required attention because multicollinearity in formative measures is detrimental. The correlation between Co-worker Reliance and Immediate Reporting of Suspicious Activity was 0.684. These clusters were combined into a single measure, and the PMB structure was reassessed (χ^2 = 104.01 df = 49; CFI = 0.977; RMSEA = 0.056). Using the chi-square distribution table, a $\Delta\chi^2$ = 9.71, Δdf = 4 represents a significant change at the 0.05 level of significance. Therefore, the combination of the two clusters into a single cluster is warranted quantitatively. From a qualitative perspective, all of these behaviors are active reporting activities by organizational insider in regard to security issues within the firm. This new cluster was named Identification and Reporting of Security Matters.

A similar but smaller correlation between the Data Entry and Management and Policy-Driven Awareness and Action clusters was found (r = 0.617). These clusters were combined, and the steps listed above were followed. The change in fit statistics (i.e., $\Delta\chi^2$ = 10.54, Δdf = 4) again indicate that the combination of these two clusters produces a better fit to the data (χ^2 = 93.47, df = 45; CFI = 0.978; RMSEA = 0.054). The behaviors combined in this cluster (e.g., backing up of data on a regular basis, the changing of password, etc.) are likely derived from policies within organizations. This new cluster was assigned the same name as one of the two original clusters, Policy-Driven Awareness and Action.

In addition to the combination of four clusters into two, the Wireless Installation single-item cluster failed to significantly help form the overall PMB construct. A correlation between this item and the PMB construct also displayed a non-significant association (r = 0.098). Upon reviewing the statistics from the second data collection wherein organizational insiders indicated the applicability of individual behaviors, the wireless installation item received 18% "not applicable" ratings. Because of these reasons, the Wireless Cluster was dropped from further analysis.

The final revision to the PMB structure in AMOS produced the following statistics χ^2 = 86.3, df = 41; CFI = 0.978; RMSEA = 0.055. The squared multiple correlation for PMBs was 0.711, which indicates that the clusters explain considerable variance in the main dependent variable. This finalized structure is displayed in Figure 3.2, and the items composing the first order factors of the revised PMB structure are shown in Appendix C.

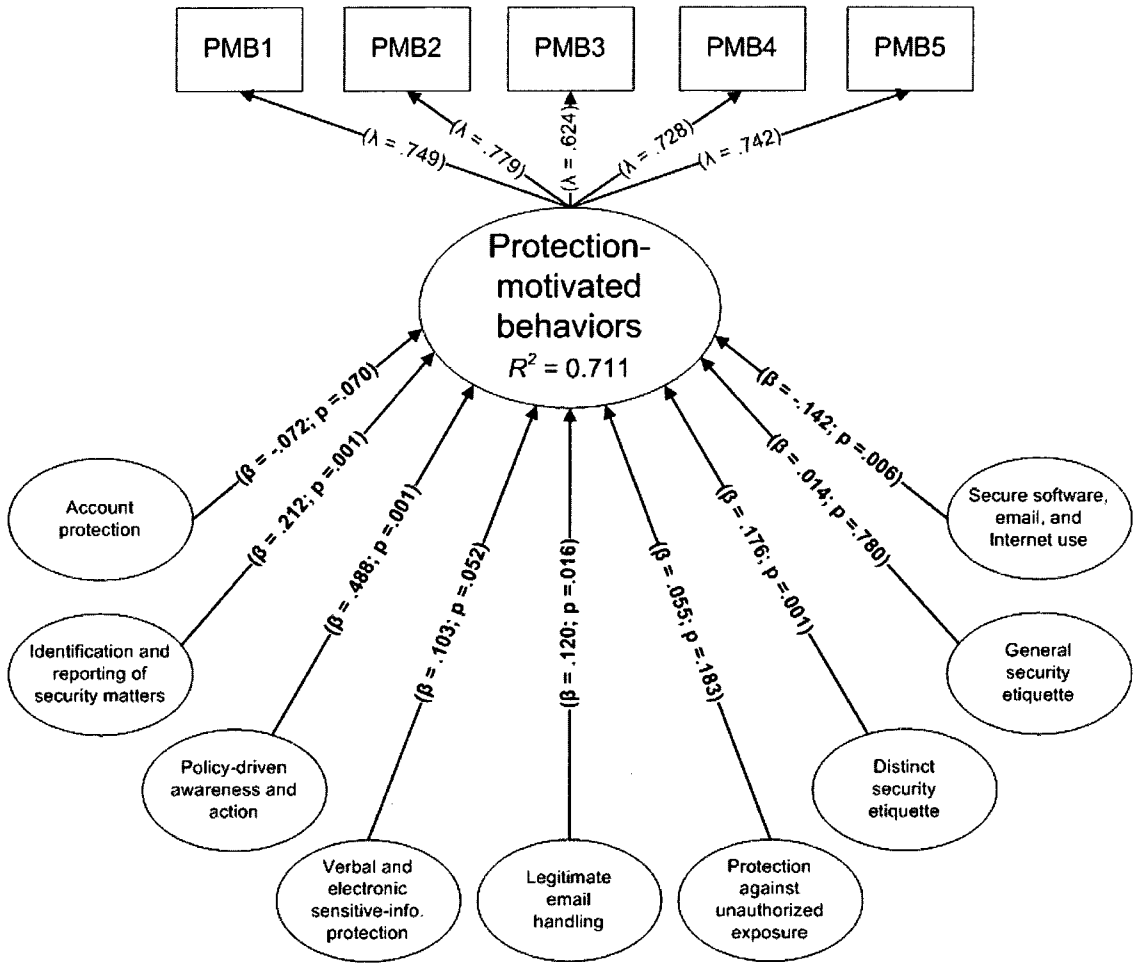


Figure 3.2 PMB Structure

A few points need to be addressed about the finalized structure. Despite the fact that many of the clusters were significantly related to the second-order PMB construct, two of them were in the opposite direction than expected. Both *account protection* and *secure software, email, and Internet use* clusters exhibited negative standardized regression weights on the PMB structure. Upon closer inspection, both of these clusters contain an item that demonstrates negative correlations with the overall reflective measure of PMBs. These individual items were AP1 (i.e., I wrote my system login information down) and SEIU4 (i.e., I used corporate email for non work-related

activities). It is likely that the inclusion of these behaviors influence the model in negative ways; however, removal of these behaviors at this point would mean that the PMB structure would be void of these behaviors—behaviors of insiders that information security professionals consider to be highly salient.

A few clusters exhibited the expected positive weights in the structure but were non-significant at the 0.05 level of significance (*verbal and electronic sensitive-information protection* exhibited a standardized beta weight with a p-value of 0.052, which was justified to be close enough to the chosen cut-off value of 0.05). These clusters were *protection against unauthorized exposure* and *general security etiquette.* Originally it was believed that multicollinearity could be a cause of these insignificant relationships; however, other combinations of clusters exhibiting moderately high correlations with each other (i.e., *secure software, email, and Internet use* combined with *legitimate email handling* and *general security etiquette* combined with *distinct security etiquette*) failed to produce significant $\Delta\chi^2$ tests. Again, formative development efforts must not solely rely on quantitative results (Diamantopoulos, Riefler, and Roth 2008), and the deletion of these clusters would leave only a partial view of PMBs. Therefore, these clusters should be kept as first-order constructs of the second-order PMB model.

Analysis and Results

Once the structure of PMBs had been more properly configured, the proposed constructs were checked for internal consistency. Unfortunately, the items used to capture organizational citizenship behaviors targeted at organizations failed to meet an acceptable level of internal consistency and could not be utilized in further analyses. Table 2.2 displays the means, standard deviations, Cronbach alphas, and inter-construct correlations

of the other constructs hypothesized to exhibit significant associations with PMBs. It is important to note that correlations with the PMB construct were performed with both the summated formative and averaged reflective measures of PMBs in order to obtain a better perspective of the nomological network.

Because inter-construct correlations rather than regression or structural equation models were assessed for nomological validity testing purposes, it was not necessary to factor analyze them. However, these tests were run ad hoc, and several constructs did not exhibit adequate internal and external validities due in part to high correlations with each other (e.g., felt responsibility for constructive change and taking charge).

Discussion

Summary of Findings

As shown by Table 2.2, many of the hypothesized associations were empirically supported. In the following sections, a summary of the individual portions of the nomological validity test are provided. The contributions of the nomological validity tests are then discussed.

Antecedents in the Nomological Network of PMBs

Hypotheses 1 – 4d suggested that several constructs should exhibit significant positive correlations as antecedents in the nomological structure of PMBs. Hypothesis 1 posited that individuals who believe that they have a responsibility to bring positive change in the workplace should engage in more PMB activity. This association was verified by significant associations with both measures of PMBs. Hypotheses 2, 3, 4a, 4b, 4c, and 4d also received empirical support. Therefore, proactive personality, role based

self-efficacy, and the components of psychological empowerment (i.e., meaning, competence, self-determination, and impact) are significant members of the PMB nomological network.

Hypotheses 5 – 7c posited that negative affectivity, employee absenteeism, role conflict, role ambiguity, and role overload would exhibit significant negative associations with PMBs. However, these hypotheses were not largely supported. In fact, only role ambiguity demonstrated a significant, negative correlation with both PMB measures: negative affectivity exhibited a significant negative association with the formative composite of PMBs (r = -.179).

Correlates in the Nomological Network of PMBs

Hypotheses 8a, 8b, and 9 posited significant positive correlations between organizational citizenship behaviors and taking charge with PMBs, respectively. Because the organizational measure of OCBs did not exhibit acceptable internal consistency, the individual component of this construct could only be examined as stated in Hypothesis 8. OCBIs were significantly and positively correlated with both the formative measure (r = .294) and reflective measure (r = .290) of PMBs; therefore, Hypothesis 8b was supported. In similar fashion, Hypothesis 9 was supported with strong associations between taking charge and the formative (r = .295) and reflective (r = .377) measures of PMBs.

Constructs expected to be negative correlates in the PMB nomological network were organizational (H10a) and interpersonal (H10b) forms of deviance as well as internal computer abuse (H11). All of these constructs exhibited significant negative correlations with both forms of the PMB measure, thereby supporting the hypotheses. As would be expected, the technology form of deviance (i.e., internal computer abuse)

demonstrated the highest negative correlation with PMBs (r = -.430). Both organizational and interpersonal forms of deviance also displayed strong but lower associations with PMBs (r = -.365 and r = -.318, respectively).

Consequence in the Nomological Network of PMBs

The lone consequence included in the nomological network of PMBs was job performance (H12). As Table 2.2 shows, this construct demonstrated significant, positive associations with both the formative (r = .180) and reflective (r = .211) measures of PMBs. Therefore, Hypothesis 12 is empirically supported.

In the next section, the associations discovered during the analysis of PMBs' nomological validity are discussed further. These findings provide key insights in the protective behavior of organizational insiders. Advice is provided as to how to best utilize the empirical findings so that managers can help motivate insiders to engage in PMBs.

Contributions

This work contributes to the field of behavioral information in several key ways. First, PMBs have been explicitly defined and important facets of its conceptualization have been discussed. For a concept as new as PMBs is, it is vital to its progression to have these conceptualizations stated so that future research can further validate them. Despite the fact that prior research has examined PMBs and provided the basic foundation from which this work was based, this paper presents a more rich dialogue on the conceptualization of this newly introduced construct as well as the first efforts in developing an instrument that captures insiders' participation in PMBs.

Second, as a way to help explore how PMBs fit in among other existing constructs in the academic literature and to help validate the conceptualization, the

nomological network of PMBs was empirically explored. The associations discovered from this assessment provide many key insights into PMBs. For example, PMBs were visualized as stemming from individuals' personal feelings of responsibility to protect their organization from harm. The strong correlations of PMBs with both felt responsibility for constructive change and proactive personality help support this conceptualization. Organizational insiders who engage in protective actions that help defend organizations from information security threats do so in part because they see these activities as a way to make positive change in the workplace. Individuals who are proactive and who feel a sense of responsibility for creating a better work environment actively seek out opportunities to make it a safer, better defended one as well despite constantly evolving information security threats that target increasing amounts of information.

Third, PMBs are believed to be beneficial rather than detrimental to organizational missions and goals. While an assessment of the organizational form of organizational citizenship behaviors could not be made, positive associations with both the individual form of OCBs and taking charge provide support for this belief. Conversely, the strong negative correlations with both forms of deviance and internal computer abuse indicate that individuals who engage in PMBs are not likely to engage in detrimental behaviors.

Another key finding that supports PMBs' conceptualization is its significant associations with the psychological empowerment construct of competence and role breadth self-efficacy. Competence specifically captures individuals' perceptions of their ability to perform their in-role tasks, whereas RBSE elicits an insider's belief in their

personal capability to perform a wide array of tasks, most of which extend beyond normal duties. PMBs define a set of behaviors whose individual components may be considered in role or extra role depending on the organization and position. Therefore, PMBs represent a very broad arrangement of protective behaviors. These two efficacy-based constructs in the nomological validity tests help solidify the notion that PMBs are composed of both in-role and extra-role activities. Individuals must feel capable of handling both stated job obligations and new tasks that go beyond those obligations to act in the various domains comprising the overall PMB structure. The significant associations with organizational citizenship behaviors, taking charge, and job performance are also evidence that supports PMBs being composed of both in-role and extra-role activities.

PMBs were also conceptualized to require organizational insiders to expend effort sometimes beyond their formal job roles. In fact, some behaviors likely require more effort on part of the insider than others. In order for individuals to become motivated to expend this energy, it was hypothesized that these individuals must believe that they are engaged in a worthwhile endeavor and that their efforts can positively affect the well being of their organization. Positive associations with the psychological empowerment constructs of meaning and impact support this perspective. Individuals who do not believe that the work that they engage in on a daily basis matters in the "big scope of things" and that they play little part in bringing about positive influence will be less likely to become motivated to engage in protective actions.

In addition to lack of meaning and impact, individuals who do not know their obligations to their organization will not spend effort in protecting it. The significant

correlation between PMBs and role ambiguity indicate that motivating individuals to participate in PMBs will prove difficult if the individuals do not first comprehend what they are supposed to do on a daily basis. Such ambiguity is definitely a deterrent to someone who is asked to actively protect something they have little information and understanding about.

At this juncture, several recommendations can be made to organizations. First, individuals who actively scan their environment for opportunities for positive change and who are willing to take a stand for what they believe is right make better stewards of organizational information. Also, individuals who are comfortable engaging in new and challenging experiences can help provide added measures of protection to information and information systems within firms. Therefore, institutions that require significant levels of information security (e.g., nuclear facilities, military, financial service providers) should attempt to better assess these characteristics of potential employees during the vetting process.

Second, organizations will not fully experience personnel who act as an excellent line of defense against security threats if they do not explicitly let insiders know their role in the organization. Going beyond typical job roles, it follows that organizations cannot simply assume that employees will know what to do when faced with information security threats. One important discovery from this research is that 15.2%, 16.9%, and 12.9% of the respondents from our first, second, and third data collections, respectively, stated that no formal information security information or training had been offered to them during their tenure at their firm. Certainly much room for improvement exists in better preparing organizational insiders in regard to information security threats.

Limitations

This research is not without its limitations. One of the limitations of this work is the fact that all responses were based on self-report surveys. Researchers have posited that single-source surveys promote inflation of correlations due to common method variance (Lindell and Whitney 2001; Podsakoff et al. 2003). However, data for some constructs may be better attained from the individual rather than a referent other like a co-worker, family member, or supervisor (Spector 2006). While there are behaviors in the overall PMB set that could have been acquired from a superior (e.g., reporting a co-worker for negligent behavior), other PMBs do not exhibit the same external visibility (e.g., performing "double checks" of work), thereby rendering multi-source data collection methods questionable at least for the main construct of interest. Also because of the use of cross-sectional surveys, there is no way to determine causality among variables.

Second, a full assessment of the proposed nomological network of PMBs could not be obtained. One of the proposed correlates (i.e., OCBO) did not exhibit an appropriate level of internal reliability. Despite this limitation, it is believed that the associations of PMBs with the remaining constructs provide an adequate understanding of the fit of PMBs among the network of other concepts in the academic literature.

Third, several issues arose with negative beta weights and non-significant loadings of the first-order PMBs on the overall, second-order PMB structure. This research has provided in-depth qualitative and quantitative examinations of these behaviors, but it appears that a few weaknesses remain in the 45-item, formative measure

of PMBs. It is suggested that the PMB structure provided in this paper be embedded in theoretically grounded models to more fully examine the remaining imperfections.

Finally, as stated in the conceptualization of PMBs, some of these behaviors may be more important to organizations than others. Some behaviors are also likely viewed as being more in-role than extra-role as well and vice versa. Unfortunately, the collection instruments used in this research did not capture the perceptions of organizational insiders in regard to these matters. Future research should investigate these characteristics as they may hold important insights for the field of behavioral information security and the design of different motivational strategies.

Conclusion

Protection-motivated behaviors (PMBs) of organizational insiders is a relatively new construct to be introduced into the academic literature. Despite the increasing need for information security within modern organizations, limited research has extended the findings from the initial study that formally introduced the concept of PMBs. Given this opportunity, this research more thoroughly addresses this new concept, draws comparisons between it and existing beneficial and detrimental behaviors in the organizational literature, and develops an instrument to capture employees' engagement in these protective activities. The findings from nomological validity tests largely support the conceptualization of PMBs. These findings also provide evidence that both motivators of and inhibitors to PMB activity within organizations exist. Important suggestions for organizations attempting to heighten their internal information security efforts are provided.

CHAPTER 4

PROMOTING INSIDERS' PROTECTION OF ORGANIZATIONAL INFORMATION RESOURCES

Introduction

Organizations utilize various methods to protect their information from security threats. These efforts in obtaining protection range from the acquisition of intrusion detection systems and disaster recovery planning to security education, training, and awareness (SETA) programs and firewall installation and monitoring (van Kessel 2009; Whitman 2003; D'Arcy and Hovav 2008). Information Technology (IT) security efforts in general currently account for the largest IT expenditure (Gartner 2009), and spending is expected to grow at a steady rate of 15.5% until the year 2012 (*Global IT Security Market Forecast to 2012* 2008). Despite these investments, information security within organizations continues to challenge even the most seasoned experts as new threats emerge and old threats evolve (CIOMagazine, CSOMagazine, and PricewaterhouseCoopers 2009). There is a concern that many individuals who oversee security projects overemphasize technologies and lose sight of the fact that information security is not just a technical concern, and that there is no "Holy Grail" (Oppliger 2007) or absolute IT-security solution (Straub and Welke 1998).

In light of this frequent oversight, security efforts that take into account human behavior have the greatest likelihood of being most effective (Im and Baskerville 2005; Choobineh et al. 2007; D'Arcy and Hovav 2007). Researchers have recently discovered that individuals within organizations are largely an untapped resource for the protection of organizational information assets (Albrechtsen and Hovden 2009; Dlamini, Eloff, and Eloff 2009). As important as technology is in organizational information protection (Cavusoglu, Raghunathan, and Cavusoglu 2009; Cavusoglu, Mishra, and Raghunathan 2005), it is users' behaviors that ultimately determine the success of security initiatives (Ng, Kankanhalli, and Xu 2009; Da Veiga and Eloff 2010). This finding is due to the fact that technology can only extend protection so far before control of information must be trusted to organizational insiders (Stanton et al. 2006; Siponen and Oinas-Kukkonen 2007). *Organizational insiders* are full-time employees, part-time employees, temporary workers, and external consultants who have been given authorized access to organizational information (Shaw, Ruby, and Post 1998). Fortunately for organizations, most organizational insiders feel a personal sense of responsibility to protect these resources from security threats (Albrechtsen and Hovden 2009; Stanton and Stam 2006)—a considerable shift from insiders being viewed only as the weakest link in organizational security (Mitnick 2003; Theoharidou et al. 2005; Dhillon and Moores 2001; Choobineh et al. 2007; D'Arcy, Hovav, and Galletta 2009; Vroom and von Solms 2004)

Within this perspective, previous research has examined insiders' motivation to adhere to security policies and rules (Siponen, Pahnila, and Mahmood 2007; Myyry et al. 2009; Herath and Rao 2009; Vance, Siponen, and Pahnila 2009) as well as basic

password, software-upkeep, and backing-up behaviors (Workman, Bommer, and Straub 2008). Despite their importance, these behaviors represent but a few of the protective activities organizational insiders can perform on behalf of their organizations (Ng, Kankanhalli, and Xu 2009). Unfortunately, when a single activity or a small subset of behaviors out of a larger structure are examined in isolation, theoretical development for the overall structure is hindered (Hanisch and Hulin 1991; Hanisch, Hulin, and Roznowski 1998). Information security is a clear example where theoretical development has been limited (Siponen and Willison 2007).

The second and third chapters of this dissertation show that protection-motivated behaviors encompass various clusters of beneficial activities and hence demonstrate that this construct is much broader than mere adherence to security policies. *Protection-motivated behaviors* (PMBs) were formally defined in Chapter 2 as the volitional behaviors organizational insiders can enact that protect (1) organizationally-relevant information within their firms and (2) the computer-based information systems in which that information is stored, collected, disseminated, and/or manipulated from information-security threats. Chapter 3 explored the nomological network of the PMB construct by evaluating correlations between it and other constructs in the applied psychology and organizational behavior literatures. PMBs have not yet been empirically examined in a theoretically derived structural model, however. This limitation prohibits researchers from fully examining the main factors that motivate organizational insiders to engage in PMBs.

This fourth chapter fills this gap by attempting to discover ways organizational insiders become motivated to engage in the entire behavioral structure afforded by PMBs.

A non-deterrence approach helps expand the IS discipline's understanding of the insider from various perspectives (Siponen and Oinas-Kukkonen 2007; Im and Baskerville 2005), and such an approach is taken in this research with the use of Protection Motivation Theory (PMT) (Rogers 1975, 1983). PMT and its components are utilized to help explain the cognitive-appraisal processes insiders experience when their organizations face security threats as well as the influences these processes have on insiders' motivation to engage in PMBs. In addition, rival explanations elicited from interviews with 11 information-security professionals and 22 "traditional" organizational insiders are empirically assessed for their potential motivating roles. Data obtained from 380 organizational insiders were examined via covariance-based structural equation modeling (using AMOS).

Several important findings for the field of behavioral information security emerged from this study. First, fear does not play a significant role in motivating insiders to engage in PMBs. Second, the manner in which insiders assess coping strategies (i.e., coping appraisal) more strongly influences protection motivation than does insiders' assessment of security threats (i.e., threat appraisal). Third, while the rival explanations of financial incentives and perceptions of sanctions (i.e., certainty and severity) failed to demonstrate significant influences on insiders' motivation to protect their organizations from security threats, job satisfaction and management support did. These findings have important theoretical and practical relevance for the study and promotion of PMBs. A review of the behavioral information security literature on the role of organizational insiders will now be given.

Literature Review

While technical methods of ensuring information security within firms have dominated the quest for adequate information protection (Dhillon and Torkzadeh 2006; Siponen and Willison 2007), a systematic study of the impact of organizational insiders on these security efforts has emerged as well (Boss et al. 2009; D'Arcy and Hovav 2007; Warkentin and Willison 2009; von Solms 2000; Vroom and von Solms 2004). This area of research has been referred to as *behavioral information security* research, which represents the examination of human actions that influence the confidentiality, integrity, and availability of information and information systems (Stanton et al. 2006; Fagnot 2008). Research in behavioral information security provides a much-needed complement to the findings already established by research that relies heavily on security technologies (Choobineh et al. 2007) because organizational information security cannot be attained without such coexistence (Schneier 2000).

Behavioral information security research has assessed the methods by which organizational insiders become deterred from committing behaviors that are detrimental to organizational information resources. One of the earliest examples of such work integrates the criminological theory of General Deterrence Theory and displays how individuals' perceptions of sanctions help stifle occurrences of intentional computer abuse (Straub 1990). Other research has incorporated the deterrence framework and largely promotes the use of sanctions as a mechanism to prevent these abusive activities of insiders (Theoharidou et al. 2005; Straub and Welke 1998; D'Arcy, Hovav, and Galletta 2009; D'Arcy and Hovav 2007; Lee, Lee, and Yoo 2004; Siponen and Willison 2007).

There is little argument against the notion that insiders can be the weakest link in organizational information security (Trompeter and Eloff 2001; Mitnick 2003; Vroom and von Solms 2004); however, the overreliance on the deterrence and other criminological frameworks (Siponen and Willison 2007; Siponen and Oinas-Kukkonen 2007) has perhaps blinded both researchers and practitioners of information security to the potential that insiders have to actively promote rather than merely to avoid damaging internal security efforts. Research shows that organizational insiders see themselves as a motivated, underutilized resource in the war against security threats, whereas information security managers continue to espouse the entire group as little more than a threat that needs to be controlled (Albrechtsen and Hovden 2009). For this reason, organizations will never fully benefit from the efforts of their strongest resource (i.e., organizational insiders) in the protection of information as long as this disconnect persists.

Recent efforts by researchers have investigated the positive side of organizational insiders. Researchers have examined individuals' adoption of technologies to protect themselves (Dinev et al. 2009; Woon, Low, and Tan 2005; Johnston and Warkentin 2010; Lee and Kozar 2008; Dinev and Hu 2007) and their organizations (Lee and Larsen 2009) from security threats. Current theoretical perspectives in this domain, however, question the usefulness of traditional theoretical models in understanding this phenomenon and advocate the development of new frameworks that are geared towards safety and protection (Liang and Xue 2009).

Research beyond protective-technology adoption has focused upon the individual protective behaviors that insiders engage in to protect organizational information resources. These behaviors include adhering to security rules and policies (Siponen,

Pahnila, and Mahmood 2007; Myyry et al. 2009), "safe computing practices" of backing up data, changing passwords, refusing to share passwords, scanning emails for viruses, updating security software (Aytes and Connolly 2004; Workman, Bommer, and Straub 2008), and the use of general caution when receiving and opening emails (Ng, Kankanhalli, and Xu 2009). These studies empirically support the qualitative studies (Albrechtsen and Hovden 2009; Stanton and Stam 2006) whose findings suggest that insiders can be used as a protective force against information security threats within organizations.

Chapters 2 and 3 of this dissertation show that PMBs comprise a much wider set of behaviors than the insider actions that have been investigated in previous research efforts in the behavioral information security literature. Further, evidence was provided that organizations may not explicitly articulate these desirable actions of organizational insiders in formal documentation—a finding that limits the applicability of previous research, because those works focus only on a single PMB or a small subset of PMBs. What is needed to advance research in this area is a theoretically driven model that explains why organizational insiders become motivated to engage in the overall structure of PMBs.

The following section discusses protection motivation theory and how it can be used to understand the process by which organizational insiders become motivated to engage in PMBs. The conceptual model is empirically examined with data attained from 380 organizational insiders from a wide variety of industries and positions. The findings from the tests of the model are then discussed from both a theoretical and practical standpoint. The theoretical foundation of the study is discussed first.

Theoretical Foundation

Protection motivation theory (PMT) (Rogers 1975, 1983) specifies the cognitive processes that individuals undergo following the reception of threat information. These processes result in the individual being motivated to engage in either adaptive or maladaptive responses (Rogers and Prentice-Dunn 1997). *Adaptive responses* are actions that effectively minimize the threat (Rogers 1983), whereas *maladaptive responses* are actions that assist in reducing the fear an individual may feel in regard to a danger but fail to reduce the occurrence and/or effects of the actual danger (Rippetoe and Rogers 1987). Therefore, maladaptive responses are used to decrease internal fear rather than the threat.

Two appraisal processes are central to the theory: threat appraisal and coping appraisal. *Threat appraisal* is the process by which an individual analyzes the perceived vulnerability to a threat, the perceived severity of a threat, and any perceived intrinsic and/or extrinsic rewards for engaging in a maladaptive response. *Coping appraisal* is the process by which an individual evaluates the efficacy of potential adaptive responses to a threat, the individual's perceived ability of successfully carrying out the recommended responses (i.e., self-efficacy expectancy; (Bandura 1977)), and any response costs associated with the adaptive coping strategy (Maddux and Rogers 1983; Rogers 1983). Individuals must cognitively assess the benefits and drawbacks in responding to threats. It is important to note that PMT does not assume that the decision maker is rational (Rogers 1983; Rogers and Prentice-Dunn 1997). Figure 4.1 details the cognitive processes outlined by PMT.

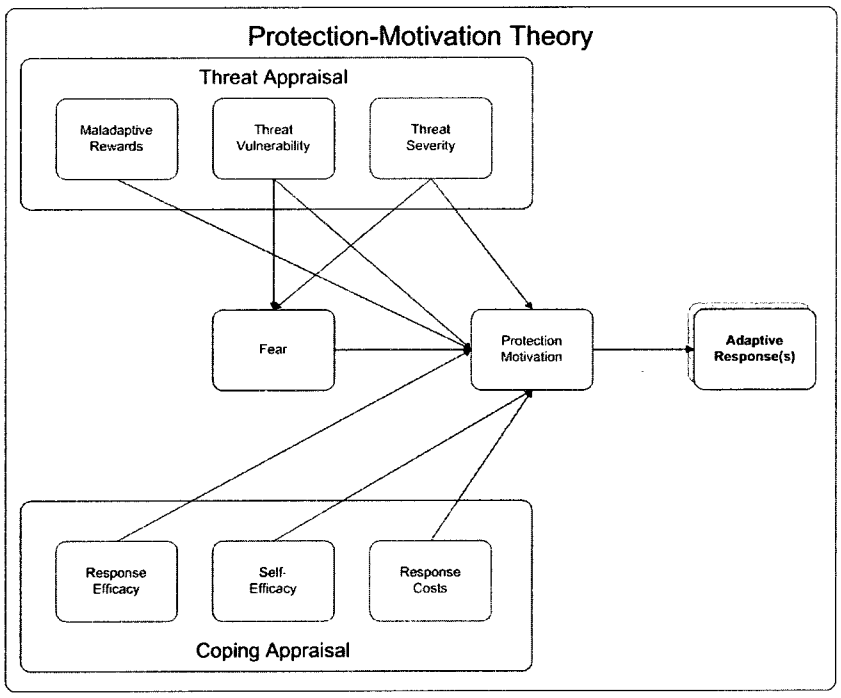


Figure 4.1 Protection Motivation Theory

Previous Utilization of Protection Motivation Theory

The theoretical foundation for PMT has been applied to myriad topics including a large number of studies examining individuals' protective responses following the communication of health threats simulated in experimental settings (Rogers and Prentice-Dunn 1997). For example, previous studies using PMT as a theoretical framework include an examination of individuals' intent to begin exercise regimens (Fruin, Pratt, and Owen 1992), to alter smoking habits (Greening 1997; Pechmann et al. 2003), and to begin breast self-examinations (Rippetoe and Rogers 1987) and cervical screenings (Orbell and Sheeran 1998). PMT has also guided studies of college students' changes in sexual behavior following discussion of the risks of sexually transmitted diseases (Tanner, Day, and Crask 1989; Tanner, Hunt, and Eppright 1991). Outside of preventive medicine, PMT has been used to study individuals' intentions to engage in anti-nuclear

war campaigns (Axelrod and Newton 1991; Wolf, Gregory, and Stephan 1986). While a comprehensive list of all studies using PMT is not appropriate here, several meta analyses note that the predictions made by PMT have largely been upheld with empirical findings from various contexts (Milne, Sheeran, and Orbell 2000; Floyd, Prentice-Dunn, and Rogers 2000). The theoretical assumptions of rewards for maladaptive behavior and response costs for adaptive behaviors, however, have received the least empirical attention (Rogers and Prentice-Dunn 1997).

While PMT's vast background is largely rooted within the field of personal preventive medicine, Rogers (1983) states that PMT may be applied to any situation involving a threat. In fact, any source of information about a threat, including fear appeals, initiates a threat appraisal and a coping appraisal process. PMT can also be applied to incidents that do not arouse one's fear (Rogers 1975) and to situations, which may entail multiple adaptive and/or maladaptive response possibilities (Rogers and Prentice-Dunn 1997). PMT may therefore be used to understand reactions to threat phenomenon outside of personal health communications and experimental settings (Rogers and Prentice-Dunn 1997; Beck 1984; Maddux and Rogers 1983) to include social problems (Tanner, Day, and Crask 1989) as well as individuals' protection of other individuals (Beck and Feldman 1983; Flynn, Lyman, and Prentice-Dunn 1995; Shelton and Rogers 1981) and even organizations (Beck 1984).

To this end, PMT has also recently been applied in IS security research. Because traditional models of technology adoption may not be suitable for all technologies (Liang and Xue 2009), researchers have used PMT to understand adoption of technologies such as home wireless security systems (Woon, Low, and Tan 2005), anti-spyware and anti-

malware software (Gurung, Luo, and Liao 2009; Lee and Larsen 2009), and location-based services (Junglas, Johnson, and Spitzmuller 2008). What is not found abundantly in the literature, however, is the extension of PMT to include behaviors beyond the adoption of specific protective technologies to other behaviors that protect organizational information assets. Despite the fact that researchers have used the PMT framework to examine adherence to information security policies (Vance, Siponen, and Pahnila 2009; Siponen, Pahnila, and Mahmood 2007; Herath and Rao 2009), intention to adopt virus protection behaviors (Lee, Larose, and Rifon 2008), and basic actions such as updating and protection of passwords, updating of security and virus software, and backing up of systems' files (Workman, Bommer, and Straub 2008), the sum of protective insider actions is far more expansive and has not yet been empirically analyzed in a theoretically derived structural model. Further, as noted by previous researchers (Vance, Siponen, and Pahnila 2009), seldom have all of the components of PMT been assessed simultaneously, leaving the full explanatory power of PMT to be evaluated. The current study helps fill this gap by exploring all components of PMT in their relation to PMBs and also discusses and tests rival explanations for such protective engagement.

Hypotheses Development

According to Rogers (1983), an individual may receive information regarding a threat from a variety of sources. External sources for threat information may be verbal communication received from other individuals in one's environment or learning through one's observation of others' actions. In all likelihood, formal security, education, training, and awareness programs are the most significant source for such information (Whitman and Mattord 2009). Internal sources for information utilized in the PMT process include

one's personality, previous experience, or feedback obtained from previous coping activities.

Following the acquisition of this threat information, the individual must appraise the threat prior to evaluating ways to effectively cope with the threat (Floyd, Prentice-Dunn, and Rogers 2000). First, the insider reviews potential rewards for not engaging in protective behaviors. Rather than exert energy in the form of protective activity, the individual may actually experience personal gains from intentionally withholding protective effort. These gains may be *intrinsic* (i.e., those that are experienced internally) or *extrinsic* (i.e., those that are experienced externally). For example, an individual who has received health information regarding smoking may receive some form of internal satisfaction (e.g., curbing of nicotine craving) by failing to quit smoking. Further, the individual may want to be socially accepted by peers at a party and choose not to quit the activity despite the fact that it may cause him/her to have serious medical conditions.

Likewise, organizational insiders may receive both intrinsic and extrinsic rewards for not protecting their organizations from information-security threats. It is expected that such perceived rewards will have a negative influence on insiders' motivation to engage in protective actions. These rewards may be even more influential to the organizational insider as they may be motivated to do nothing because the threat affects their organization rather than themselves directly. Rewards for such responses have received the least attention of all PMT components (Rogers and Prentice-Dunn 1997). This model is displayed in Figure 4.2.

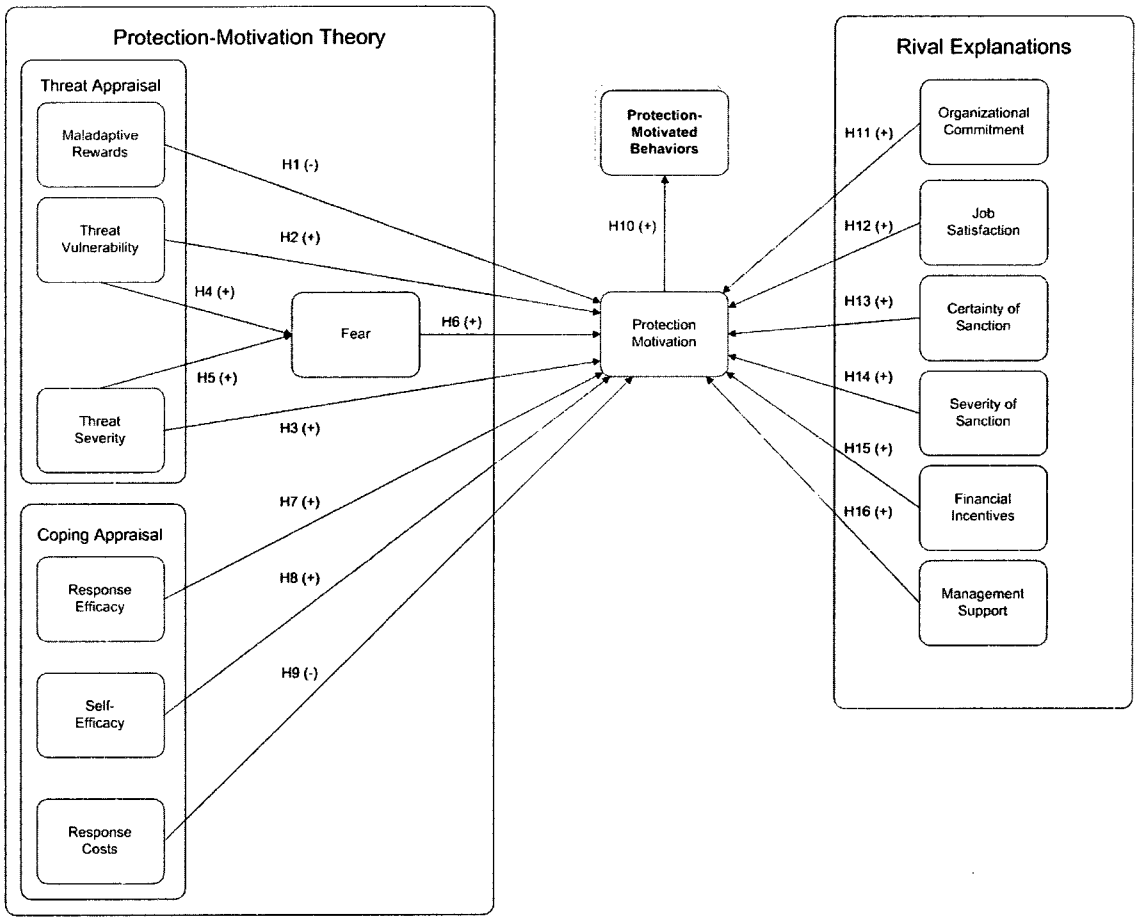


Figure 4.2 Conceptual Model

Hypothesis 1: Insiders' perceptions of rewards for not engaging in protective actions will be negatively related to insiders' motivation to protect organizational information assets.

Though the rewards may be high, individuals may choose to engage in protective activity because their perceived susceptibility to threats may be greater than the perceived rewards. *Threat vulnerability*, or the extent to which the individual feels susceptible to a particular threat, is a significant component in the threat appraisal process and overall formation of protection motivation. For example, an individual who believes that s/he is more likely to contract a sexually transmitted disease than others may be less prone to

engage in unprotected sex (Tanner, Hunt, and Eppright 1991). Further, using this same example, *threat severity*, or the extent to which the threat is perceived to be detrimental and to cause harm, will also influence this individual's decision to wear protection. If the individual believes s/he is not very likely to contract the disease but doing so would create great distress and inconvenience, s/he may choose to use protection.

Organizational insiders assess the threats to their organizations' information and computerized information systems. When they perceive that their organizations are vulnerable to threats, insiders should become more motivated to protect their organization. These motivations are especially likely when insiders feel a personal responsibility to protect the organization (Albrechtsen and Hovden 2009; Stanton and Stam 2006). Threats that are viewed as being more noxious may also heighten these feelings of personal responsibility as the threat severity is higher.

Hypothesis 2: Insiders who perceive that their organization is vulnerable to information-security threats will be more motivated to engage in PMBs than those who do not.

Hypothesis 3: Insiders who perceive that the information-security threats that their organization faces are severe will be more motivated to engage in PMBs than those who do not.

When individuals assess the severity of a threat along with its likelihood of success, fear is often generated. The combination of inevitable events that inflict considerable discomfort cause an individual to become nervous, scared, and upset (Rogers and Prentice-Dunn 1997). Despite the fact that the revised PMT model (Rogers 1983) did not include a direct link from fear to protection motivation, other researchers

argue that fear is a necessary component of the cognitive mediating processes suggested by PMT and should be given greater consideration (Tanner, Hunt, and Eppright 1991; Eppright et al. 2002). Therefore, it is expected that insiders' perceptions in regard to threat characteristics will influence the degree of fear they experience. This fear is also expected to have an influence on the degree by which organizational employees are motivated to protect their firm from those threats.

Hypothesis 4: Insiders who perceive that their organization is vulnerable to information-security threats will experience more fear than those who do not.

Hypothesis 5: Insiders who perceive that the information-security threats that their organization faces are severe will experience more fear than those who do not.

Hypothesis 6: Insiders who become fearful of their organization's information-security threats will be more motivated to engage in PMBs than those who do not.

The second of the two major processes of PMT is the coping appraisal (Rogers 1983), which may be more important than the threat appraisal in forming protective intentions (Milne, Sheeran, and Orbell 2000; Rippetoe and Rogers 1987). Moreover, without information about how to cope with perceived threats, individuals may be more likely to engage in maladaptive behaviors than those who receive no information at all (Rogers and Prentice-Dunn 1997; Neuwirth, Dunwoody, and Griffin 2000; Eppright et al. 2002). This finding is particularly troubling as some insiders mention that they lack knowledge on how to perform such activities (Albrechtsen and Hovden 2009). *Response efficacy*, or the perception that the recommended coping strategies can successfully attenuate the threat, is a vitally important part of forming individuals' intentions to

engage in protective actions. In fact, previous research states that response efficacy is the moreq important predictor of protection motivation than any other component in PMT (Block and Keller 1995; Wolf, Gregory, and Stephan 1986). Likewise, organizational insiders who believe that suggested responses to information-security threats are efficacious in minimizing or eliminating these threats will be more likely to become motivated to engage in these worthwhile efforts.

Hypothesis 7: Insiders who have high response efficacy perceptions will be more motivated to engage in PMBs than those who do not.

The revised version of PMT (Rogers 1983; Maddux and Rogers 1983) included the self-efficacy construct (Bandura 1977) within the coping appraisal process. *Self-efficacy*, or the belief that an individual is personally capable of appropriately implementing the proposed coping strategy, has been shown to strongly predict protective behaviors in many contexts (Milne, Sheeran, and Orbell 2000; Fruin, Pratt, and Owen 1992). This self assurance has also been shown to be a stronger predictor than threat severity perceptions (Pechmann et al. 2003). Therefore, individuals who believe that they can adequately perform the recommended protective actions will do so at a higher frequency than those who believe that their personal capabilities are lacking.

Hypothesis 8: Insiders who maintain high self-efficacy in regard to protective actions will be more motivated to engage in PMBs than those who do not.

The final component of the coping appraisal process, *response costs*, constitutes the perceived drawbacks for engaging in protective actions. These costs include any expenses, inconveniences, difficulties, and potential side effects that an individual believes s/he will incur due to his/her engagement in protective action (Fruin, Pratt, and

Owen 1992). Similar to rewards for maladaptive responses in the threat appraisal process, response costs decrease the likelihood that individuals will perform adaptive responses (Pechmann et al. 2003) and have received limited research attention (Rogers and Prentice-Dunn 1997). Therefore, organizational insiders who perceive that the costs of their engagement in protection-motivated behaviors will be significant are less likely to put forth effort to protect their organization from information-security threats.

Hypothesis 9: Insiders who associate protective actions with high response costs will be less motivated to engage in PMBs than those who do not.

Finally, the outcome of the PMT model is a motivational force termed protection motivation. *Protection motivation* is "an intervening variable that has the typical characteristics of a motive: it arouses, sustains, and directs activity" (Rogers, 1983, p. 158). Protection motivation drives behavior change, is best measured as intentions (Rogers, 1983; Rogers & Prentice-Dunn, 1997), and is the lone mediator between the two appraisals and adaptive responses (Rogers 1983; Floyd, Prentice-Dunn, and Rogers 2000). With this in mind, protection motivation should be the most significant predictor of adaptive engagement (Milne, Sheeran, and Orbell 2000). It is expected that organizational insiders who experience protection motivation will engage in more PMBs.

Hypothesis 10: Insiders who are motivated to protect their organizations from information-security threats will engage in more PMBs than those who are not.

Rival Hypotheses

As with any research relying upon a single theory, it is important to test rival explanations to gain a more thorough understanding of the influences on an organizational phenomenon (Straub 1989; Straub, Boudreau, and Gefen 2004).

Therefore, various other constructs could be responsible for explaining the motivations of organizational insiders to engage in PMBs. The findings elicited from interviews with 11 information-security professionals and 22 organizational insiders indicated that five other constructs could possibly be motivators for PMBs.

First, interviewees mentioned that insiders are likely to protect their organizations from security threats if they feel like they belong to the organization and that their commitment to the organization's goals is strong. This type of commitment has been examined in previous organizational research and has been shown to lead to increased job performance (Meyer et al. 1989; Keller 1997) as well as positive, extra-role activities such as organizational citizenship behaviors (Podsakoff et al. 2009; Dalal 2005). It is also expected that individuals who feel more connected to their organization will expend more effort in protecting it from threats.

Hypothesis 11: Insiders who are more committed to their organizations will be more motivated to engage in PMBs than those who are not.

Second, job satisfaction may also play a role as an antecedent to PMB engagement. Employees who are satisfied with their jobs behave in a manner similar to those who are committed to their organizations via increased in-role and extra-role, citizenship behaviors (Bateman and Organ 1983; Williams and Anderson 1991). Conversely, individuals who are dissatisfied with their jobs are more prone to engage in counterproductive work behaviors (Mount, Ilies, and Johnson 2006). It follows then that insiders who are satisfied with their jobs are also more likely to act in manners that protect their organization's information resources than those who are dissatisfied.

Hypothesis 12: Insiders who are more satisfied with their jobs will be more motivated to engage in PMBs than those who are not.

Third, individuals within organizations may fear the potential of being sanctioned (e.g., job loss, imposition of fines) by their organization for not performing their daily tasks in a protective manner. In the field of behavioral information security, sanctions have been found to act as a deterrent to criminal behavior (Straub 1990; D'Arcy, Hovav, and Galletta 2009; Lee, Lee, and Yoo 2004). *Certainty of sanction* refers to an individual's perceived likelihood of being caught for a criminal act. *Severity of sanction* refers to the degree of punishment that is expected if a individual is caught engaging in a act detrimental to the organization (Straub 1990; Peace, Galletta, and Thong 2003). Both of these constructs work in forming this deterrence.

According to the interviews, it appears that fear of potential sanctions may be used by managers to encourage employees to protect their organizations from security threats. Organizational behavior research describes in-role behaviors as those formally rewarded when appropriately performed (Williams and Anderson 1991). On the other hand, employees may also expect to receive sanctions for failure to perform such in-role behaviors. Since both in-role and extra-role behaviors comprise the overall PMB structure (see Chapter 3), at least a portion of such behaviors can reasonably be expected to be influenced by formal sanctions for non engagement.

Hypothesis 13a: Insiders who believe they would be caught for not engaging in PMBs will be more motivated to engage in PMBs than those who do not.

Hypothesis 13b: Insiders who believe they would be severely punished for not engaging in PMBs will be more motivated to engage in PMBs than those who do not.

Fourth, insiders that believe they will receive financial incentives for engaging in PMBs may be more likely to do so than other employees who do not believe that they will be rewarded for their efforts. Such incentives have previously exhibited varying results with performance at both the individual and organizational levels in the academic literature (Jenkins et al. 1998; Bloom and Milkovich 1998). An empirical examination of the incentive-protective behavior link in behavioral information security would prove important as it has the potential of supporting similar propositions already in the literature (August and Tunca 2006).

Hypothesis 14: Insiders who believe they would receive financial incentives for engaging in PMBs will be more motivated to engage in PMBs than those who do not.

Finally, individuals who were interviewed stated that upper-level management's emphasis on information-security matters was another potential source for motivation. Management support for technology implementations within organizations has been shown to exhibit significant relationships with implementation success as this emphasis is derived from individuals who have authority to allocate resources to the venture (Thong, Yap, and Raman 1996; Sharma and Yetton 2003; Leonard-Barton and Deschamps 1988). Such upper-level support for information-security efforts within the firm may also increase the likelihood of overall employee adoption of security strategies as insiders

likely perceive these strategies as worthwhile investments in the protection of the organization.

Hypothesis 15: Insiders who perceive that managerial support for information-security efforts exists will be more motivated to engage in PMBs than those who do not.

The methodology used to empirically examine the conceptual model derived from these hypotheses will now be discussed.

Methodology

Data Collection

Data for this study was collected using individuals of an external panel provider, Zoomerang. External panels have been used to elicit responses to survey instruments in various contexts (Posey, Lowry et al. 2010; Awad and Ragowsky 2008; Gibney, Zagenczyk, and Masters 2009) and offer several advantages. First, panels allow anonymity to be guaranteed for the respondent—a necessary element in eliciting honest responses to behaviors potentially influenced by social desirability beliefs (Bennett and Robinson 2000). Second, respondents from a wide range of industries and positions can be reached for topics requiring the participation of a broad spectrum of individuals that would be almost impossible to attain by traditional methods. Finally, because of the sensitive nature of information security, organizations are less likely to allow outsider researchers to gain access to employees (Kotulic and Clark 2004).

The sample consisted of 380 organizational insiders from various industries and positions within the United States. The sample was 53.4% female, 10.5% information systems or information technology professionals, and 34.6% managers. 96.1% of the

respondents held full-time positions. The average age of respondents was 43.75 years, and the average amount of a typical working day spent using their organizations' computer systems was reported to be 65.39%.

Construct Measurement

Where possible, previously validated scales in the academic literature were used and adapted to capture the variables of interest in this study (Straub, Boudreau, and Gefen 2004). However, several components of the PMT framework have received little attention (i.e., rewards for maladaptive behaviors and response costs for adaptive behaviors) and do not have validated measurement instruments. In these cases, items were generated and/or added to others to effectively capture the latent variables in the hypothesized model. Also, unless otherwise indicated, responses were collected on a 7-point Likert scale (*1 = Strongly disagree; 7 = Strongly agree*).

Rewards for Maladaptive Behavior

Rewards for maladaptive behavior is one of the most understudied components of the PMT process. Therefore, three items were created to measure insiders' perceived rewards for failing to act in protective behaviors. One of the sample items is "It is likely that I would receive personal rewards for purposefully not protecting my organization's information and information systems from security threats."

Threat Vulnerability

Threat vulnerability was captured by a 4-item measure consisting of two items from Workman et al. (2008) and two items from Witte, Cameron, McKeon, and Berkowitz (1996). Sample items in this measure were "My organization's information

and information systems are vulnerable to security threats" and "My organization's information and information systems are susceptible to security threats."

Threat Severity

Similar to threat vulnerability, threat severity was captured by a 4-item measure consisting of two items from Workman et al. (2008) and two items from Witte, Cameron, McKeon, and Berkowitz (1996). Items in this measure assessed the degree to which organizational insiders believed information security threats to their organizations' information and information systems were severe, significant, and serious.

Fear

The 6-item measure of fear used in this study was taken from Block and Keller (1995). This measure asks respondents to indicate the extent to which they normally experience the following feelings when thinking about the information security threats to their organization: frightened, tense, nervous, anxious, uncomfortable, and nauseous. Responses were collected on a 5-point Likert scale (*1 = Not at all; 5 = Very large extent*).

Response Efficacy

Three items from the Workman et al. (2008) measure of response efficacy were adapted for this study. Respondents were asked to rate their level of agreement with the following items: "Employee efforts to keep my organization's information and information systems safe from information security threats are effective," "The available measures which can be taken by employees to protect my organization's information and information systems from security violations are effective," and "The preventive

measures available to me to stop people from accessing my organization's information and information systems are adequate."

Self-Efficacy

Three items from the self-efficacy measure of Workman et al. (2008) were adapted to measure self-efficacy to engage in PMBs. This measure included the following items: "For me, taking information security precautions to protect my organization's information and information systems is easy," "I have the necessary skills to protect my organization's information and information systems from information security violations," and "My skills required to stop information security violations against my organization's information and information systems are adequate."

Response Costs

The 3- item measure from Workman et al. (2008) and one additional item were combined to measure insiders' perceptions about the costs of adaptive security behaviors. Sample items include "The inconvenience to implement recommended security measures to protect my organization's information and information systems exceeds the potential benefits" and "The negative side effects of recommended security measures in my organization are greater than the advantages."

Protection Motivation

Three items were created to measure protection motivation. As stated in PMT, protection motivation is best measured by intentions (Rogers and Prentice-Dunn 1997; Rogers 1983; Tanner, Day, and Crask 1989). Respondents rated their level of agreement with the following items: "I intend to protect my organization from its information security threats," "It is likely that I will engage in activities that protect my organization's

information and information systems from security threats," and "I do not intend to expend effort to protect my organization from its information security threats."

Protection-Motivated Behaviors

PMBs were measured in two ways. First, the reflective items used in Chapter 3 were combined with three additional items to capture the general PMB construct. Sample items include "I actively attempted to protect my organization's information and computerized information systems" and "I did my best to protect all forms of sensitive information within my organization."

Second, the insiders' self-reported engagement in the 48 individual PMBs listed in the third chapter was also collected. These behaviors comprise 9 unique first-order clusters that comprise the entire PMB construct, and when used in conjunction with the reflective items, allow PMBs to be measured in a Multiple Indicators and MultIple Causes (MIMIC) (Joreskog and Goldberger 1975) model. Responses to both PMB measures were collected on a 7-point Likert scale (*1= Never; 7 = Always*).

Organizational Commitment

The revised affective organizational commitment scale was used to capture respondents' feelings of attachment and belonging to the organization (Meyer and Allen 1997). This 6-item measure consists of items such as "I would be very happy to spend the rest of my career with this organization," " I really feel as if this organization's problems are my own," and "This organization has a great deal of personal meaning for me."

Job Satisfaction

The 3-item measure from Cammann, Fichman, Jenkins, and Klesh (1983) was utilized to capture insiders' level of job satisfaction. Items in this measure were "All in

all, I am satisfied with my job," "In general, I don't like my job," and "In general, I like working here."

Certainty of Sanction

Despite the considerable focus on general deterrence theory in the information security literature (Siponen and Willison 2007), few measures have been developed to capture individuals' perceptions of both certainty and severity of sanctions. With that being said, I chose to adapt the certainty of sanction measure from Posey, Bennett, Roberts, and Lowry (2010) from sanctions about committing computer abuse to sanctions for failure to engage in PMBs. This 3-item measure included the items "If I failed to attempt to protect my organization's information and information systems from their security threats, my organization would find out," "If I chose not to protect my organization from security threats, the probability that my organization would find out would be high," and "Employees who do not actively try to protect the organization's information and information systems from security threats will be caught by my organization."

Severity of Sanction

Similar to the items for certainty of sanction, the items for severity of sanction were derived from Posey, Bennett et al. (2010). This 3-item measure was comprised of the following items: "If I were caught not trying to protect my organization from information security threats, I would be punished severely by my organization," "Organizational sanctions for employees who do not attempt to protect the organization from information security threats are severe," and "My organization would take strict

action against employees caught not putting forth effort to protect it from information security threats."

Financial Incentives

Three items were created to measure insiders' perceptions of financial incentives to engage in PMBs. The items were "My organization would reward me financially for helping protect its information and information systems from security threats," "I would likely receive monetary rewards for performing my job duties in a secure manner," and "Performing my tasks securely means that I would be financially rewarded by my organization."

Managerial Support

A 4-item measure was used to elicit insiders' perceptions of managerial support for information security initiatives within their organizations. Two items were derived from the management support measure of Campion, Medsker, and Higgs (1993), and two additional items were added. Sample items include "Higher management in the company supports the concept of information security" and "Information security is topic that is supported by management in my organization."

Analysis

The theoretical model shown in Figure 2 was examined using the structural equation modeling program AMOS 16.0 (Arbuckle 2007). The two-step process of examining separate measurement and structural models (Anderson and Gerbing 1988) was followed. A discussion of this process is provided in the next sections.

Measurement Model and Construct Validity

The first step in assessing the hypothesized model was to perform a confirmatory factor analysis (CFA). The initial CFA model exhibited the following statistics: χ^2 of 2506.2 (df = 1605), CFI = 0.935, and a 90% confidence interval for RMSEA is 0.036 – 0.041 thereby indicating a good initial fit but that improvements could be made (Hair et al. 2006). All items loaded with a highly significant t-value (i.e., $p < 0.001$) on their respective constructs, but several items (i.e., OrgCommit2 = 0.521, FinIncentives2 = 0.536, MgmtSupport3 = 0.473, ProtMotivation2 = 0.409, ResponseCosts4 = 0.491, PMBReflect5 = 0.574, and PMBReflect7 = 0.598) exhibited standardized regression weights less than 0.60 and were removed from further analysis. The standardized residual covariance matrix was also analyzed to assess other potentially problematic items within the model (Bagozzi and Yi 1988). Items exhibiting significant values in this matrix (i.e., 2.58 or greater) should be given consideration for removal (Hair et al. 2006). One item (i.e., Fear3) yielded an undesirable standardized residual value and was discarded.

Convergent validity of all constructs in the model was assessed with the three following criteria: (1) factor loadings; (2) average variance extracted; and, (3) internal consistency estimates. As stated above, all remaining factor loadings are highly significant and are above the 0.60 cutoff value. Average variance extracted (AVE) values were calculated for each construct (see Table 1). All constructs exhibited AVEs greater than the 0.50 heuristic (Fornell and Larcker 1981). Finally, all constructs represented internal consistency Cronbach alphas greater than 0.70 (except a slightly less alpha for Protection Motivation), thereby meeting demands set forth by previous research (Nunnally 1978).

Discriminant validity was assessed according to the guidelines suggested by Fornell and Larcker (1981). These guidelines require that constructs in a measurement model maintain discriminant validity if the square root of the AVEs of both constructs under consideration are higher than the correlation between those two constructs. As shown in Table 4.1, two paired correlations did not meet this criterion. Organizational commitment and job satisfaction exhibited a correlation of 0.874, and the correlation between response efficacy and self-efficacy was 0.849. In addition to these high correlations, the AVEs for organizational commitment and self-efficacy were not high enough to justify discrimination and unfortunately had to be discarded from the model. All remaining constructs met this third criterion, and construct validity was established. The final CFA model fit the data well with a χ^2 of 1150.7 (df = 824), CFI = 0.969, and a 90% confidence interval for RMSEA of 0.028 – 0.037.

As a caveat, two additional construct pairs exhibited high correlations in the CFA model: threat severity and threat vulnerability (r = 0.791) and certainty of sanction and severity of sanction (r = 0.814). Despite the magnitude of these correlations, the square roots of the constructs' AVEs were large enough to justify keeping the constructs separate. Failure to allow these variables to remain in the model would severely limit the ability to examine a significant portion of PMT and the rival components that often comprise general deterrence theory.

Table 4.1 Means, Standard Deviations, and Correlations

	Mean	σ	α	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. Maladaptive Rewards	1.77	1.24	0.84	**0.644**														
2. Threat Vulnerability	3.41	1.45	0.90	.158**	**0.696**													
3. Threat Severity	3.35	1.57	0.90	.173**	.791***	**0.696**												
4. Fear	1.92	1.15	0.93	.127*	.299***	.288***	**0.739**											
5. Response Efficacy	5.09	1.21	0.83	-.198**	-.347***	-.119*	-.183**	**0.589**										
6. Self-Efficacy	5.05	1.23	0.82	-.130*	-.169**	-.005	-.121*	.849***	**0.537**									
7. Response Costs	2.75	1.35	0.82	.345***	.154*	.150*	.247***	-.371***	-.299***	**0.582**								
8. Protection Motivation	5.64	1.40	0.68	-.231**	-.026	.018	-.060	.476***	.482***	-.407***	**0.512**							
9. PMBs	5.71	1.25	0.87	-.114	-.088	.038	-.058	.529***	.485***	-.296***	.603***	**0.531**						
10. Org. Commitment	4.76	1.50	0.86	-.085	-.196***	-.077	-.026	.405***	.203***	-.169**	.307***	.316***	**0.536**					
11. Job Satisfaction	5.36	1.48	0.90	-.053	-.183**	-.071	-.103	.362***	.199***	-.183**	.379***	.300***	.874***	**0.761**				
12. Certainty of Sanction	4.56	1.41	0.87	-.056	-.110	.103	-.015	.495***	.395***	-.208***	.308***	.438***	.250***	.191***	**0.699**			
13. Severity of Sanction	4.42	1.52	0.89	-.033	-.088	.160**	.050	.408***	.315***	-.115	.245***	.368***	.161**	.106	.814***	**0.723**		
14. Financial Incentives	2.81	1.70	0.85	.369***	-.070	.137*	.185**	.127*	.095	.090	.130	.190**	.331***	.298***	.246***	.308***	**0.735**	
15. Management Support	5.56	1.41	0.89	-.153*	-.077	.019	-.169**	.494***	.367***	-.308***	.520***	.367***	.467***	.457***	.422***	.390***	.225***	**0.739**

* $p < 0.05$

** $p < 0.01$

*** $p < 0.001$

Bolded numbers on diagonal represent AVEs

Structural Model

Following the validation of the constructs and obtaining an acceptable fit to the dataset's covariance matrix in CFA, hypotheses testing began by converting the CFA model into a structural model. The structural model exhibited the following characteristics: χ^2 of 1225.1 (df = 843), CFI = 0.963, and RMSEA = 0.035. Thus, the structural model indicates an acceptable fit to the dataset given the model's complexity (Hair et al. 2006). This model is displayed in Figure 4.3.

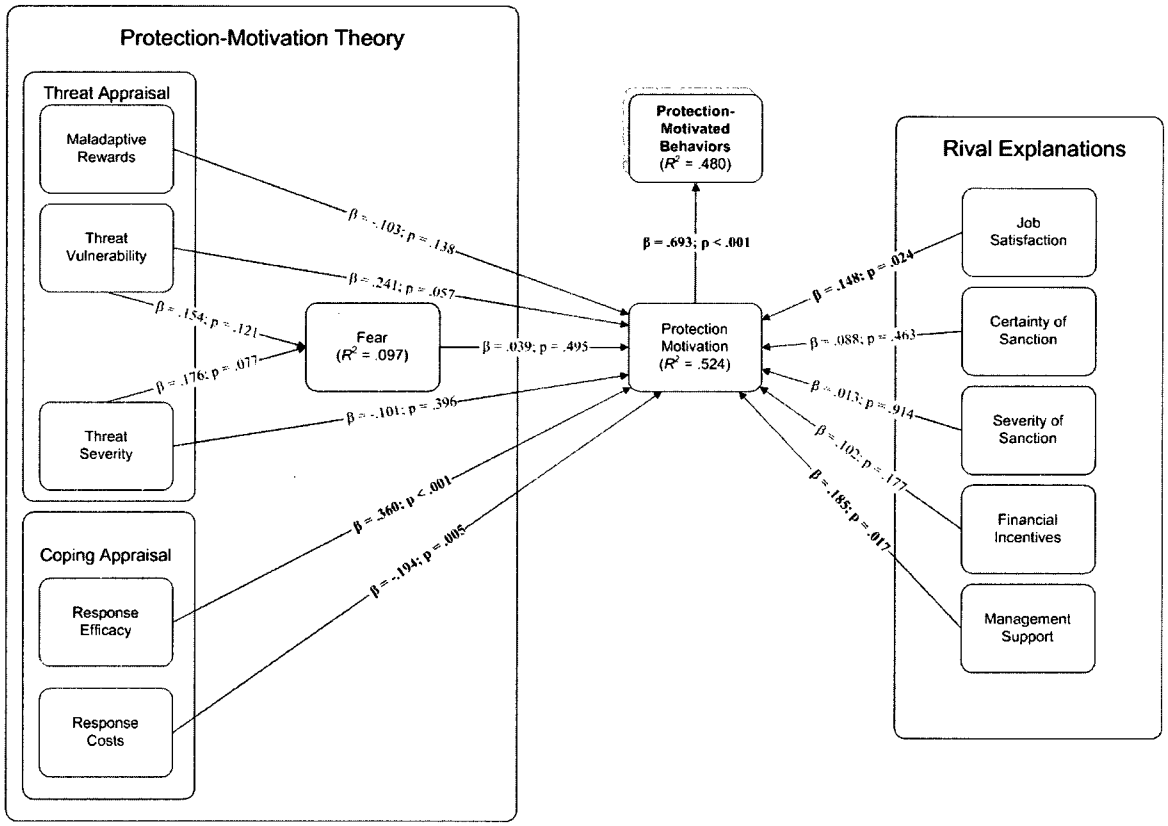


Figure 4.3 Structural Model Results with PMBs as Reflective Construct

It should be noted that PMBs can also be represented as a latent variable having multiple indicators and multiple causes (MIMIC) (Joreskog and Goldberger 1975; Diamantopoulos and Winklhofer 2001). Chapter 3 of this dissertation demonstrates this

fact, and the 9 first-order clusters of PMBs were entered into a second structural model. Because differences could exist between the structural models depending on the manner by which the PMB construct is modeled, I felt that it was necessary to empirically assess this possibility.

Other than the variance explained in PMBs increasing considerably to 82.6%—which it should as the 9 clusters explain over 70% of the variance of PMBs themselves—the relationships found to be of consequence in the first structural model continued to be supported in the second structural model. The results from this assessment are graphically noted in Figure 4.4. The results of the first structural model assessment are reported below, and Table 4.2 shows the results of both structural models.

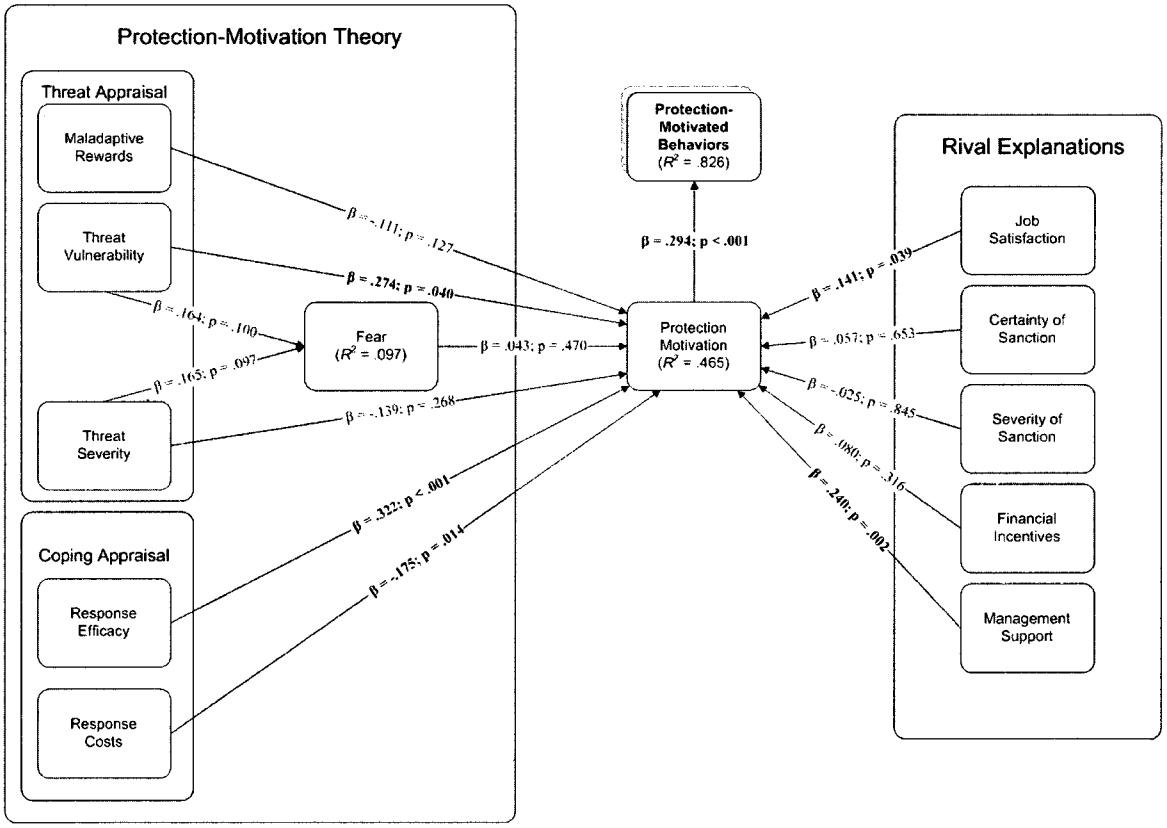


Figure 4.4 Structural Model Results with PMBs as MIMIC Model

Table 4.2 Results of Structural Models

	PMBs (Reflective)		PMBs (MIMIC Model)	
	Path Coefficient (β)	t-value, p-value	Path Coefficient (β)	t-value, p-value
Hypotheses derived from PMT				
Maladaptive Rewards → (-) Protection Motivation	(-0.103)	t=(-1.483), p=0.138	(-0.111)	t=(-1.526), p=0.127
Threat Vulnerability → Protection Motivation	0.241	t=1.903, p=0.057+	0.274	t=2.053, p=0.040*
Threat Severity → Protection Motivation	(-0.101)	t=(-0.848), p=0.396	(-0.139)	t=(-1.107), p=0.268
Threat Vulnerability → Fear	0.154	t=1.550, p=0.121	0.164	t=1.645, p=0.100
Threat Severity → Fear	0.176	t=1.771, p=0.077+	0.165	t=1.659, p=0.097+
Fear → Protection Motivation	0.039	t=0.682, p=0.495	0.043	t=0.722, p=0.470
Response Efficacy → Protection Motivation	0.360	t=4.116, p<0.001***	0.322	t=3.047, p<0.001***
Response Costs → (-) Protection Motivation	(-0.194)	t=(-2.812), p=0.005***	(-0.175)	t=(-2.451), p=0.014*
Protection Motivation → Protection-Motivated Behaviors	0.693	t=7.882, p<0.001***	0.294	t=5.935, p<0.001***
Hypotheses derived from Rival Explanations				
Job Satisfaction → Protection Motivation	0.148	t=2.255, p=0.024*	0.141	t=2.060, p=0.039*
Certainty of Sanction → Protection Motivation	0.088	t=0.733, p=0.463	0.057	t=0.449, p=0.653
Severity of Sanction → Protection Motivation	0.013	t=0.108, p=0.914	(-0.025)	t=(-0.196), p=0.845
Financial Incentives → Protection Motivation	0.102	t=1.351, p=0.177	0.080	t=1.003, p=0.316
Management Support → Protection Motivation	0.185	t=2.390, p=0.017*	0.240	t=3.047, p=0.002**

+ $p < 0.10$
* $p < 0.05$
** $p < 0.01$
*** $p < 0.01$

Results

Protection-Motivation Theory Results

Threat Appraisal

Several components of the threat appraisal process were hypothesized to influence the degree by which organizational insiders are motivated to protect their organizations' information resources from security threats: (H1) rewards for maladaptive behaviors, (H2) threat vulnerability, and (H3) threat severity. In addition, the by-product of fear was also hypothesized to significantly relate to protection motivation (H6). Many of these hypotheses, however, were rejected. The relationship between rewards for maladaptive behaviors and protection motivation was in the proper direction but was not significant (β = -.103, p = .138). Fear (β = .039, p = .495) and threat severity (β = -.101, p = .396) also failed to significantly influence protection motivation.

The only component of the threat appraisal process having any influence of consequence on protection motivation was threat vulnerability (β = .241, p = .057). Also, the relationship of threat severity with fear (H5) was of consequence (β = .176, p = .077) whereas the relationship of threat vulnerability (H4) with fear was not (β = .154, p = .121). In summary, only two of the hypotheses stemming from the threat appraisal process were supported (i.e., hypotheses 2 and 5), while the others were rejected.

Coping Appraisal

The hypotheses derived from PMT's second appraisal process (i.e., coping appraisal) received much more support than those from the threat appraisal. Both response efficacy (β = .360, p < .001) and response costs (β = -.194, p = .005) exhibited significant influences on protection motivation. Therefore, both hypotheses 7 and 9 were

supported. However, due to a very high correlation between response efficacy and self-efficacy in the CFA, the relationship with self-efficacy and protection motivation (H8) could not be assessed as it had to be removed from the model in order to reach construct validity requirements.

Protection Motivation

The outcome of the PMT cognitive process is protection motivation. This cognitive mediating variable between the two appraisal processes and actual behavior was hypothesized (H10) to be significantly and positively related to PMBs. This hypothesis received strong support in the structural model ($\beta = .693$, $p < .001$).

Rival Explanations Results

Support for rival explanations was mixed. Hypothesis 11 suggested a positive relationship between job satisfaction and protection motivation. This hypothesis was supported by a significant, positive standardized regression weight ($\beta = .148$, $p = .024$).

The rival explanations of certainty and severity of sanctions did not find support. The degree with which an insider believes they would be caught for failure to engage in protective behaviors on behalf of their organization failed to exert significant influence on protection motivation ($\beta = .008$, $p = .463$). Likewise, the degree to which an individual believes s/he would be punished if caught for failing to act in a protective manner was also found to be insignificant ($\beta = .013$, $p = .914$). Therefore, Hypotheses 12 and 13 were rejected.

Financial incentives also failed to demonstrate a significant relationship with protection motivation. Some of the interviewees expressed that monetary incentives for engaging in the protective activities would increase their motivation to act in those

manners. All organizational insiders, however, do not feel this way as the link between these incentives and protection motivation was insignificant, which rejects Hypothesis 14 ($\beta = .102$, $p = .177$).

The final rival explanation stated that management support for information-security efforts within the organization will help drive motivation of employees to protect the organizational information resources from threats. Management support's influence on protection motivation was supported by a significant, positive standardized regression weight ($\beta = .185$, $p = .017$). Therefore, Hypothesis 15 was supported in the model.

Discussion

Contributions to Theory

Several findings of this study are particularly important to researchers attempting to develop theory in the field of behavioral information security. First, the entire process as suggested by PMT is not wholly applicable to the study of insiders' protection of organizational information resources. With the exception of threat vulnerability, the components of the threat appraisal process demonstrated little influence on insiders' PMB activity. Despite previous researchers' emphasis on fear as a major driving force in personal protective behaviors (Eppright et al. 2002; Tanner, Hunt, and Eppright 1991), fear does not significantly influence the degree to which organizational insiders engage in protective behaviors on behalf of their organization. These findings support the earlier works on PMT that suggest fear is little more than a by-product of the threat appraisal process (Rogers 1975, 1983). Consequently, attempting to scare insiders about potential threats through messages eliciting fear is neither appropriate nor effective. Informing

insiders about their organizations' security threats appears to be an ineffective step in motivating employees to engage in protective behaviors on behalf of their firms.

In contrast, the empirical evidence provided by the model for the coping appraisal was significant in motivating employees to engage in protective behaviors. The findings show that both response efficacy and response costs significantly relate to PMB activity within organizations. Organizational insiders strongly consider the efficacy of protective responses prior to engagement in PMBs while also actively weighing the potential drawbacks (i.e., inconveniences) of these activities. If insiders believe that a particular response will effectively mitigate information security threats and the response will not become burdensome on the insider, the more likely protective activity will occur. Conversely, responses seen as too overbearing and cumbersome in the daily work life of insiders, regardless of the responses' effectiveness, are more likely to be bypassed by the insider. The mental calculus performed in the coping appraisal is more vital to motivating individuals to engage in PMBs than is the threat appraisal—a finding that is consistent with the results of previous PMT research (Milne, Sheeran, and Orbell 2000; Rippetoe and Rogers 1987).

Findings from the rival explanations also increase the field's understanding of insiders' security-related behaviors. Management support demonstrated a significant, positive relationship with PMBs. This finding was not unexpected due to the influence that referent others have on individuals' behaviors. Social Learning Theory (SLT) (Bandura 1977) states that individuals are heavily influenced by the actions of other individuals in their environments through observation. In the context of this study, upper-level managers who actively show their support for internal information-security efforts

are more likely to have a positive impact on the protective behaviors of their subordinates. Further, this finding helps provide evidence that an organization's internal security culture is imperative in the development of insiders' beliefs and actions that help protect organizational information resources (Van Niekerk and von Solms 2010; Da Veiga and Eloff 2010; Thomson, von Solms, and Louw 2006).

Job satisfaction also positively influences levels of protection motivation. This finding is important in that research in job design can mean more than increases in performance. This research suggests that appropriate job design can also increase the degree to which organizational insiders want to engage in efforts to protect information on behalf of their organizations. Happy workers make protective stewards of organizational information resources.

The lack of supportfor the inclusion of both certainty and severity of sanctions is an interesting finding for research in behavioral information security. These sanctions and the foundation from which they derive (i.e., General Deterrence Theory) have been applied and supported in research examining internal computer abuse (D'Arcy, Hovav, and Galletta 2009; Lee, Lee, and Yoo 2004; Straub 1990). The inability of the sanctions to explain significant variation in PMBs suggests that PMBs and internal computer abuse are also not opposite ends of the same behavioral spectrum. Recent research, however, suggests that insiders' compliance with security policies within organizations can be viewed from a combination of PMT- and GDT-based lenses (Herath and Rao 2009, 2009). While compliance with security policies fails to act as a proxy for all PMBs as all PMBs are not explicitly stated requirements of insiders (see third chapter), future

research should continue to explore the possibility of these two theoretical frameworks to coexist in the studies of all activities of importance in the field of behavioral information security.

Contributions to Practice

The findings from this study also have significant implications for practitioners of information security. For example, the finding that insiders are only partially motivated to engage in PMBs upon learning about individual security threats is vitally important to the design of security education, training, and awareness (SETA) efforts. In order to be the most effective, organizational efforts in informing employees of information-security initiatives should not solely focus on *what* the security threats to an organization's information resources are. Rather, it is imperative that practitioners notify organizational insiders *how* to effectively cope with such threats and demonstrate the efficacy of the recommended responses. Out of all components suggested by PMT, response efficacy was the one construct that exhibited the strongest influence on insiders' protection motivation levels—a finding similar to that found in other studies (Rippetoe and Rogers 1987; Wolf, Gregory, and Stephan 1986). Further, practitioners who base internal security programs heavily on a financial reward system may be quite disappointed to discover their efforts have little influence on PMBs within their organization when compared to the other variables in the model.

Another example of the findings of import to practitioners is that organizational insiders weigh the efficacy of recommended responses against any perceived costs. These response costs are synonymous with being an inconvenience to the insider, a hindrance that makes it more difficult for employees to perform their daily tasks. This finding's link along with the significant, positive relationship displayed between job satisfaction and

protection motivation suggests that practitioners should do everything they can to ease these response costs so that they do not become a detriment to the satisfaction insiders feel about their daily jobs.

In addition to decreasing potential hindrances, managers throughout the organization rather than just internal information-security professionals must actively display their support for information security efforts. Organizational insiders are strongly influenced by their supervisors' actions and efforts to see that security efforts are receiving the attention they necessarily deserve. Managers have an immense influence on the security culture of an organization and insiders' protection motivation (Knapp et al. 2006), which results in subsequent PMBs.

Limitations and Future Research

This study has several limitations. First, data were obtained from a cross-sectional panel. This method of data collection prohibits researchers from inferring causality among the constructs in conceptual models. Future research should extend this study by testing the model in experimental settings so that variables external to the research can be better controlled. For example, these researchers should consider standardizing the information given to experimental subjects in regard to information security threats, appropriate responses, etc., to ensure a common starting point for all individuals whose level of protection motivation will be assessed at future time periods.

Second, in addition to adaptive responses, research based on PMT has also examined maladaptive responses (Brouwers and Sorrentino 1993; Eppright et al. 2002; Rippetoe and Rogers 1987). These responses assist the individual in dealing with the fear formed from the threat appraisal yet do nothing to minimize the effects of the threat. This

chapter focused only on the adaptive responses of PMBs and did not include the potential maladaptive responses of religious faith (i.e., "I believe the best way to deal with security threats is to turn to my beliefs in a higher power"), avoidance (i.e., "I try not to look for security threats because I may likely find them"), fatalism (i.e., "There is really nothing I can do to help protect my organization from its security threats—if they are meant to happen, they will happen"), wishful thinking (i.e., "I believe the best solution to security threats is a miracle cure"), etc. Future research in behavioral information security should examine these maladaptive behaviors because they are detrimental to the security of organizational information resources. These behaviors are also important to behavioral information security as a discipline because they likely represent constructs separate from both the intentional harming of information resources (i.e., internal computer abuse) and their purposeful protection (i.e., PMBs).

Conclusion

Organizational insiders are often seen as the largest threat to organizational information security. Recent research in behavioral information security, however, suggests these individuals can also be a great benefit to the security of organizational information resources. This research integrates the theory of protection motivation theory (PMT) as well as rival explanation elicited from interviews with 11 information security professionals and 22 organizational insiders to help explain the process by which individuals become motivated to protect their organizations from information security threats. Models based on data collected from 380 organization insiders from various industries and occupation in the United States show several important findings. These discoveries will assist future developmental efforts in the field of behavioral information

security. Further, the findings from this study help direct information security professionals in the design of security education, training, and awareness (SETA) programs and the overall development of an internal security culture.

CHAPTER 5

CONCLUSIONS

This dissertation represents the most extensive work to date on the protective role that organizational insiders have in the protection of information and information systems within firms. These behaviors were defined as protection-motivated behaviors (PMBs), and both qualitative and quantitative methods were utilized to examine them. These efforts resulted in the discovery of the conceptual space of PMBs as perceived by organizational insiders, the development of a self-report measure of PMBs, the empirical assessment of PMBs' nomological validity, and the examination of the factors that influence insiders' motivation to engage in these protective behaviors on behalf of their organizations. This chapter provides a succinct review of the findings and contributions stemming from this dissertation effort that incorporated 33 semi-structured interviews, elicited the participation of 13 subject matter experts, and issued 6 individual data collections, which when combined contain the responses of more than 1,700 organizational insiders.

In Chapter 2, it was shown that PMBs represent a wide variety of protective behaviors extending well beyond simple adherence to information security policies. Classification techniques (i.e., multidimensional scaling and cluster analysis) demonstrated that these behaviors comprise 14 unique clusters in a three-dimensional

perceptual structure in the minds of organizational insiders. Property fitting techniques were used to objectively determine the dimensions of this structure and ultimately provided a way to position PMBs in a formal typology. This typology declares that PMBs are mentally positioned by insiders whether the behaviors (1) require minor or continual level of improvements within organizations, (2) are widely or narrowly standardized and applied throughout various organizations, and (3) are a reasonable or unreasonable request of organizations to make of their insiders. For both researchers of behavioral information security and information security practitioners, the results of Chapter 2 show that all PMBs are not the same in the mind of the insider—an indication that approaches used to encourage such beneficial activities should be tailored to the respective quadrant in which they reside.

From a methodological standpoint, the second chapter appears to be the first research effort in the IS literature to integrate multidimensional scaling, property fitting, and cluster analysis techniques to determine the general mindset of subjects of interest. The combination of these techniques provides a much needed rigorous and unique method (Choobineh et al. 2007) to quantitatively define and explain the perceptual space of an entire group of individuals. Other IS researchers can now use the powerful combination these techniques become when integrated together and can apply the techniques in their particular field of interest.

Chapter 3 used the typology and cluster configurations from Chapter 2 to develop and validate a self-report measure of PMBs. This measure was structured as a multiple indicators and multiple causes (MIMIC) model (Joreskog and Goldberger 1975). The variance in the overall, second-order PMB construct explained by the first-order

constructs exceeded 70%. This significantly large amount of variance explained provides an attestation that the vast majority of behaviors comprising the PMB construct have been identified.

In this third chapter, initial nomological validity tests were performed to better determine how PMBs are situated among other organizational behaviors of interest to academicians. These tests provided empirical evidence for several key conceptualizations in regard to PMBs. First, PMBs stem from insiders' personal feelings of responsibility to protect their organization from harm. Second, PMBs are seen as way to bring about proactive, positive change in the workplace. Third, PMBs are indeed beneficial to firms. Fourth, PMBs contain both in-role and extra-role behaviors and are best enacted by individuals who are comfortable engaging in activities outside of their explicitly stated job duties. Finally, PMBs are more likely to exist among employees who believe that their jobs have personal meaning and that their roles within the organization are unambiguous.

Chapter 4 used the measure developed and validated in Chapter 3 and placed it within a structural model derived from Protection Motivation Theory (Rogers 1975, 1983) and several rival explanations. One key finding was that the entire process as suggested by protection motivation theory is not wholly applicable to the study of insiders' protection of organizational information resources. Specifically, the coping appraisal was found to be much more closely linked with insiders' motivation to engage in PMBs than the threat appraisal process. Further, fear was found not to exhibit a significant relationship—a finding that supports the notion that fear in this context is nothing more than a by-product of the threat appraisal process.

This chapter also provides ample evidence that organizational insiders perform a mental calculus in which they weigh the potential benefits of engaging in PMBs against the expected drawbacks. Organizational insiders strongly consider the efficacy of protective responses prior to engagement in PMBs while also actively weighing the potential inconveniences of these activities. Only when the benefits of protective actions are greater than the inconveniences will organizational insiders become motivated to protect their firms' information resources from their security threats.

Findings from the rival explanations also increase the field's understanding of insiders' security-related behaviors. Management support has a significant, positive relationship with insiders' motivation to engage in PMBs. Likewise, job satisfaction also positively influences levels of protection motivation. These findings are important in that research in job design can equate to more than increases in performance. This research suggests that appropriate job design can also increase the degree with which organizational insiders want to engage in efforts to protect information on behalf of their organizations.

Another finding stemming from the empirical assessment of rival explanations is the lack of support for both certainty and severity of sanctions influences on protection motivation. These sanctions and the foundation from which they derive (i.e., General Deterrence Theory) have been applied and supported in research examining internal computer abuse (D'Arcy et al. 2009; Straub, 1990). The inability of insiders' perceptions of sanctions for failing to perform PMBs to explain significant variation in protection motivation suggests that PMBs and internal computer abuse are not dichotomous

organizational events. Rather, these two very important activities exhibit different motivators—a finding vital to the field of behavioral information security.

In summary, this dissertation explicitly focused on the more positive, protective side of organizational insiders—a side that still has not received the attention its importance in helping achieve organizational information protection warrants. Rather, this dissertation is a stepping stone in helping researchers better understand the human element of information security more fully. Only when the findings herein are integrated with complementary studies examining the detrimental insider behaviors and their motivators can the field of behavioral information security begin to adequately fill the role for which it is intended.

APPENDIX A

PROTECTION-MOTIVATED BEHAVIORS (PMBS)

Appendix A Protection-Motivated Behaviors (PMBs)

Behavior ID	Behavior
1	An organizational insider does not write his/her system login information down
2	An organizational insider sets the permissions of computer files to prevent unauthorized access
3	An organizational insider properly destroys unneeded data residing on the computer system or his/her computer workstation
4	An organizational insider actively attempts not to accidentally disclose sensitive company information with unauthorized individuals
5	Prior to speaking with someone about sensitive company information, the organizational insider makes sure the other individual(s) has legitimate access to that information
6	An organizational insider does not put sensitive information in emails or other forms of electronic communication (e.g., instant messages) unless authorized to do so as required by his/her job
7	An organizational insider only responds to emails which have a legitimate business request
8	An organizational insider does not set up a wireless network access point in the corporate office without proper approval
9	An organizational insider does not allow unauthorized individuals to do his/her work for him/her
10	An organizational insider does not display sensitive documents in public (e.g., airplane or airport)
11	An organizational insider always properly logs into and out of computer systems at work
12	If an organizational insider needs to use a shared computer station at work but another employee is logged on, he/she logs the other employee out of the station prior to using it
13	An organizational insider does not open emails that he/she believes have a chance of containing a virus or other potentially malicious components
14	An organizational insider does not open emails that "just do not look right" to him/her
15	An organizational insider quickly notifies the sender of an email if that email contained sensitive information that was not meant for him/her
16	An organizational insider does not forward email spam to co-workers
17	An organizational insider discusses sensitive organizational information with authorized individuals only

18	An organizational insider informs his/her co-worker if he/she believes that the co-worker is engaging in behaviors not accepted by their company's information-security guidelines and policies
19	An organizational insider properly destroys and disposes of all unneeded sensitive documents
20	An organizational insider performs a "double check" of his/her work to make certain that the sensitive information he/she enters into the computer system is accurately coded
21	An organizational insider adequately documents any changes he/she makes in the computer system
22	An organizational insider does not discuss sensitive company information with the media unless authorized to do so
23	An organizational insider logs out of the computer system as soon as he/she is done using it
24	An organizational insider does not write his/her passwords down
25	An organizational insider stores information only according to the retention policies specified by his/her organization
26	An organizational insider sets his/her computer workstation's screen saver to password protect (i.e., requires a password once the screen saver detects user activity to regain access to the workstation)
27	An organizational insider creates strong passwords (i.e., passwords having a combination of lower- and upper-case letters, numbers, and special characters)
28	An organizational insider changes his/her passwords according to his/her organization's security guidelines
29	An organizational insider fully reads and pays close attention to security newsletters sent by his/her organization's department that is responsible for information-security matters
30	An organizational insider notifies his/her co-workers of important security information he/she becomes aware of
31	An organizational insider does not install software on his/her computer workstation unless authorized to do so
32	An organizational insider keeps the laptop or other electronic devices issued to them by their organization with them at all times
33	An organizational insider does not leave active computers unattended
34	An organizational insider follows up with an individual who received an inadvertent email from him/her to make sure that the individual disposed of the email and its information properly
35	An organizational insider immediately informs his/her supervisor upon his/her awareness of the physical theft of computer equipment

36	An organizational insider immediately reports a lost access card to the proper organizational authorities
37	An organizational insider does not allow anyone to look over his/her shoulder when he/she works on sensitive documents
38	An organizational insider clears sensitive information off of his/her desk or computer before allowing someone entrance into his/her office or leaving at the end of the work day
39	An organizational insider immediately applies software updates to his/her computer workstation when notified of the update by an authorized individual or department within his/her organization
40	An organizational insider converts sensitive documents to Adobe PDF format so that none of the information in the document can be altered once it is finalized
41	If an organizational insider identifies something that looks out of the ordinary in his/her work environment, he/she immediately reports it to the proper organizational authorities
42	An organizational insider immediately informs the authorized individual or department within the organization if he/she found a potential information-security problem or loophole
43	An organizational insider immediately reports a co-worker's negligent information-security behavior to the proper organizational authorities
44	An organizational insider stores sensitive corporate information only on protected media or locations (e.g., a protected server)
45	An organizational insider locks sensitive, physical documents in a secure location when they are not in use
46	An organizational insider pauses before responding to an email to make certain that he/she is responding to a valid request
47	An organizational insider opens email attachments only if he/she knows the email's sender and was expecting the email
48	If an organizational insider receives an email from someone he/she knows but the topic or content looks suspicious, he/she contacts the sender to verify that the communication attempt was valid
49	When compiling a new email message, an organizational insider double checks the list of recipients in the "To:", "CC:", and "BCC:" fields before he/she actually sends the email to verify that only the intended recipients receive the communication
50	An organizational insider only accesses information in the computer system that is required for his/her job

51	An organizational insider uses corporate email for work-related activities only
52	While at work, an organizational insider utilizes the Internet for work-related tasks only
53	An organizational insider works at a steady but cautious pace to ensure that he/she performs their job tasks in a secure manner
54	If an organizational insider knows of shortcuts in the computer system that would be against the organization's accepted security protocol, he/she does not use them
55	An organizational insider verifies an individual's identity prior to releasing sensitive information to them
56	An organizational insider adheres to the information-security guidelines and policies adopted by his/her organization
57	An organizational insider protects his/her computer-system account information by never giving it to other individuals
58	An organizational insider does not allow anyone else to utilize his/her computer workstation
59	An organizational insider does not allow anyone else to utilize a computer workstation under his/her account and login information
60	An organizational insider does not perform work on a computer workstation with a co-worker's account information or under a co-worker's login session
61	An organizational insider does not bring a laptop from home and attach it to his/her organization's corporate network without authorization to do so
62	An organizational insider only uses secured wireless and/or wired networks approved by his/her organization for off-site network access
63	An organizational insider does not discuss company-specific, information-security information (e.g., internal protocols, breaches) with anyone who does not need to know
64	An organizational insider does not verbally discuss sensitive information in areas where unauthorized persons may be located (e.g., a hallway, an elevator)
65	An organizational insider backs up important data and documents on a regular basis
66	An organizational insider locks his/her workstation when leaving his/her office space so that the workstation cannot be accessed by other individuals
67	An organizational insider reminds his/her fellow co-workers of information-security guidelines and protocols adopted by their organization

APPENDIX B

IDENTIFICATION OF CLUSTERS

Appendix B Identification of Clusters

Cluster ID	Cluster Name	Behavior ID	Behavior Description
1	Legitimate Email Handling	7	An OI only responds to emails which have a legitimate business request
		21	An OI adequately documents any changes he/she makes in the computer system
		34	An OI follows up with an individual who received an inadvertent email from him/her to make sure that the individual disposed of the email and its information properly
		47	An OI opens email attachments only if he/she knows the email's sender and was expecting the email
2	Protection against Unauthorized Exposure	9	An OI does not allow unauthorized individuals to do his/her work for him/her
		12	If an OI needs to use a shared computer station at work but another employee is logged on, he/she logs the other employee out of the station prior to using it
		26	An OI sets his/her computer workstation's screen saver to password protect (i.e., requires a password once the screen saver detects user activity to regain access to the workstation)
		64	An OI does not verbally discuss sensitive information in areas where unauthorized persons may be located (e.g., a hallway, an elevator)
		66	An OI locks his/her workstation when leaving his/her office space so that the workstation cannot be accessed by other individuals
3	Policy-Driven Awareness and Action	16	An OI does not forward email spam to co-workers
		25	An OI stores information only according to the retention policies specified by his/her organization
		28	An OI changes his/her passwords according to his/her organization's security guidelines
		30	An OI notifies his/her co-workers of important security information he/she becomes aware of
		41	If an OI identifies something that looks out of the ordinary in his/her work environment, he/she immediately reports it to the proper organizational authorities

		54	If an OI knows of shortcuts in the computer system that would be against the organization's accepted security protocol, he/she does not use them
		61	An OI does not bring a laptop from home and attach it to his/her organization's corporate network without authorization to do so
4	Appropriate Data Entry and Management	19	An OI properly destroys and disposes of all unneeded sensitive documents
		20	An OI performs a "double check" of his/her work to make certain that the sensitive information he/she enters into the computer system is accurately coded
		53	An OI works at a steady but cautious pace to ensure that he/she performs their job tasks in a secure manner
		65	An OI backs up important data and documents on a regular basis
5	Document Conversion	24	An OI does not write his/her passwords down
		40	An OI converts sensitive documents to Adobe PDF format so that none of the information in the document can be altered once it is finalized
6	Secure Software, Email, and Internet Use	13	An OI does not open emails that he/she believes have a chance of containing a virus or other potentially malicious components
		31	An OI does not install software on his/her computer workstation unless authorized to do so
		39	An OI immediately applies software updates to his/her computer workstation when notified of the update by an authorized individual or department within his/her organization
		46	An OI pauses before responding to an email to make certain that he/she is responding to a valid request
		51	An OI uses corporate email for work-related activities only
		52	While at work, an OI utilizes the Internet for work-related tasks only
7	Verbal and Electronic Sensitive-Information Protection	17	An OI discusses sensitive organizational information with authorized individuals only
		22	An OI does not discuss sensitive company information with the media unless authorized to do so

		37	An OI does not allow anyone to look over his/her shoulder when he/she works on sensitive documents
		44	An OI stores sensitive corporate information only on protected media or locations (e.g., a protected server)
		49	When compiling a new email message, an OI double checks the list of recipients in the "To:", "CC:", and "BCC:" fields before he/she actually sends the email to verify that only the intended recipients receive the communication
8	Wireless Installation	8	An OI does not set up a wireless network access point in the corporate office without proper approval
9	Widely Applicable Security Etiquette	3	An OI properly destroys unneeded data residing on the computer system or his/her computer workstation
		5	Prior to speaking with someone about sensitive company information, the OI makes sure the other individual(s) has legitimate access to that information
		23	An OI logs out of the computer system as soon as he/she is done using it
		29	An OI fully reads and pays close attention to security newsletters sent by his/her organization's department that is responsible for information-security matters
		55	An OI verifies an individual's identity prior to releasing sensitive information to them
		57	An OI protects his/her computer-system account information by never giving it to other individuals
10	Distinctive Security Etiquette	1	An OI does not write his/her system login information down
		2	An OI sets the permissions of computer files to prevent unauthorized access
		4	An OI actively attempts not to accidentally disclose sensitive company information with unauthorized individuals
		6	An OI does not put sensitive information in emails or other forms of electronic communication (e.g., instant messages) unless authorized to do so as required by his/her job
		10	An OI does not display sensitive documents in public (e.g., airplane or airport)
		11	An OI always properly logs into and out of computer systems at work

		27	An OI creates strong passwords (i.e., passwords having a combination of lower- and upper-case letters, numbers, and special characters)
		33	An OI does not leave active computers unattended
		36	An OI immediately reports a lost access card to the proper organizational authorities
		38	An OI clears sensitive information off of his/her desk or computer before allowing someone entrance into his/her office or leaving at the end of the work day
		45	An OI locks sensitive, physical documents in a secure location when they are not in use
		56	An OI adheres to the information-security guidelines and policies adopted by his/her organization
		63	An OI does not discuss company-specific, information-security information (e.g., internal protocols, breaches) with anyone who does not need to know
11	Co-worker Reliance	14	An OI does not open emails that "just do not look right" to him/her
		18	An OI informs his/her co-worker if he/she believes that the co-worker is engaging in behaviors not accepted by their company's information-security guidelines and policies
		58	An OI does not allow anyone else to utilize his/her computer workstation
		62	An OI only uses secured wireless and/or wired networks approved by his/her organization for off-site network access
		67	An OI reminds his/her fellow co-workers of information-security guidelines and protocols adopted by their organization
12	Account Protection	35	An OI immediately informs his/her supervisor upon his/her awareness of the physical theft of computer equipment
		42	An OI immediately informs the authorized individual or department within the organization if he/she found a potential information-security problem or loophole
		50	An OI only accesses information in the computer system that is required for his/her job
		59	An OI does not allow anyone else to utilize a computer workstation under his/her account and login information
		60	An OI does not perform work on a computer workstation with a co-worker's account information or under a co-worker's login session

13	Immediate Reporting of Suspicious Activity	15	An OI quickly notifies the sender of an email if that email contained sensitive information that was not meant for him/her
		43	An OI immediately reports a co-worker's negligent information-security behavior to the proper organizational authorities
		48	If an OI receives an email from someone he/she knows but the topic or content looks suspicious, h/she contacts the sender to verify that the communication attempt was valid
14	Equipment Location and Storage	32	An OI keeps the laptop or other electronic devices issued to them by their organization with them at all times

APPENDIX C

ITEMS IN REVISED PMB STRUCTURE

Appendix C Items in Revised PMB Structure

Cluster ID	Cluster Name	Behavior ID	Behavior Description
1	Account Protection	1	I wrote my system login information (i.e., login ID and password) down (R)
		57	I gave my computer-system account information to unauthorized individuals (R)
		60	I performed work on a computer workstation with a co-worker's account information or under a co-worker's login session (R)
2	Identification and Reporting of Security Matters	18	I informed my co-workers if I believed that they were engaging in behaviors not accepted by our company's information-security guidelines and policies
		30	I notified my co-workers of new, important security information I became aware of
		41	If I identified something that looked out of the ordinary in my work environment, I immediately reported it to the proper organizational authorities
		43	I immediately reported a co-worker's negligent information-security behavior to the proper organizational authorities
		67	I reminded my fellow co-workers of information-security guidelines and protocols adopted by our organization
3	Policy-driven Awareness and Action	3	I properly destroyed unneeded data residing on the computer system or my computer workstation
		19	I properly destroyed and disposed of all unneeded sensitive documents
		20	I performed a 'double check' of my work to make certain that the sensitive information I entered into the computer system was accurately coded
		25	I stored information according to the retention policies specified by my organization
		27	I created strong passwords (i.e., passwords having a combination of lower- and upper-case letters, numbers, and special characters)
		28	I changed my passwords according to my organization's security guidelines

		29	I fully read and paid close attention to security newsletters sent by my organization's department that was responsible for information-security matters
		44	I stored sensitive corporate information on protected media or locations (e.g., a protected server)
		54	I used shortcuts in the computer system that were against the organization's accepted security protocol (R)
		62	I used wireless and/or wired networks not approved by my organization for off-site network access (R)
		65	I backed up important data and documents on a regular basis
4	Verbal and Electronic Sensitive-information Protection	4	I disclosed sensitive company information with unauthorized individuals (R)
		5	Prior to speaking with someone about sensitive company information, I made sure the other individual(s) had legitimate access to that information
		6	I put sensitive information in emails or other forms of electronic communication (e.g., instant messages) for which I was unauthorized to do so (R)
		10	I displayed sensitive documents in public (e.g., airplane or airport) (R)
		22	I discussed sensitive company information with the media when not authorized to do so (R)
		50	I accessed information in the computer system that was not required for my job (R)
		55	I verified an individual's identity prior to releasing sensitive information to them
		64	I verbally discussed sensitive information in areas where unauthorized persons may have been located (e.g., a hallway, an elevator) (R)
5	Legitimate Email Handling	7	I responded to emails which did not have a legitimate business request (R)
		13	I opened emails that I believed had a chance of containing a virus or other potentially malicious components (R)
		49	When compiling a new email message, I double checked the list of recipients in the "To:", "CC:", and "BCC:" fields before I actually sent the email to verify that only the intended recipients would receive the communication

6	Protection against Unauthorized Exposure	9	I allowed unauthorized individuals to do my work for me (R)
		37	I allowed individuals to look over my shoulder when I worked on sensitive documents (R)
7	Distinct Security Etiquette	26	I set my computer workstation's screen saver to password protect (i.e., requires a password once the screen saver detects user activity to regain access to the workstation)
		38	I cleared sensitive information off of my desk or computer screen before allowing someone entrance into my office or leaving at the end of the work day
		45	I locked sensitive, physical documents in a secure location when they were not in use
8	General Security Etiquette	11	I properly logged into and out of computer systems at work
		23	I logged out of the computer system as soon as I was done using it
		33	I left active computers unattended (R)
		58	I allowed unauthorized individuals to utilize my computer workstation or other electronic devices issued to me by my organization (R)
		61	I brought a personal laptop, USB drive, or other electronic device from home and attached it to my organization's corporate network without authorization to do so (R)
		66	I locked my workstation when leaving my office space so that the workstation could not be accessed by other individuals
9	Secure Software, Email, and Internet Use	16	I forwarded email spam (i.e., email whose content was non-business related) to co-workers (R)
		31	I installed software on my computer workstation when not authorized to do so (R)
		39	I immediately applied software updates to my computer workstation when notified of the update by an authorized individual or department within my organization

	51	I used corporate email for non work-related activities (R)
	52	While at work, I utilized the Internet for non work-related tasks (R)

(R) = Item is reverse worded

REFERENCES

Albrechtsen, E., and J. Hovden. 2009. The information security digital divide between information security managers and users. *Computers & Security* 28 (6):476-490.

Alge, B. J., G. A. Ballinger, S. Tangirala, and J. L. Oakley. 2006. Information privacy in organizations: empowering creative and extrarole performance. *The Journal of applied psychology* 91 (1):221-32.

Anderson, J. C., and D. W. Gerbing. 1988. Structural equation modeling in practice: A review and recommended two-step approach. *Psychological bulletin* 103 (3):411-423.

Aquino, K., M. U. Lewis, and M. Bradfield. 1999. Justice Constructs, Negative Affectivity, and Employee Deviance: A Proposed Model and Empirical Test. *Journal of Organizational Behavior* 20 (7):1073-1091.

Arbuckle, J. L. 2007. AMOS Version 16.0.1.

Aryee, S., P. S. Budhwar, and Z. X. Chen. 2002. Trust as a Mediator of the Relationship between Organizational Justice and Work Outcomes: Test of a Social Exchange Model. *Journal of Organizational Behavior* 23 (3):267-285.

August, T., and T. I. Tunca. 2006. Network Software Security and User Incentives. *Management Science* 52 (11):1703-1720.

Avolio, B. J., W. Zhu, W. Koh, and P. Bhatia. 2004. Transformational leadership and organizational commitment: mediating role of psychological empowerment and moderating role of structural distance. *Journal of Management* 25 (8):951-968.

Awad, N. F., and A. Ragowsky. 2008. Establishing Trust in Electronic Commerce Through Online Word of Mouth: An Examination Across Genders. *Journal of Management Information Systems* 24 (4):101-121.

Axelrod, L. J., and J. W. Newton. 1991. Preventing Nuclear War: Beliefs and Attitudes as Predictors of Disarmist and Deterrentist Behavior 1. *Journal of Applied Social Psychology* 21 (1):29-40.

Aytes, K., and T. Connolly. 2004. Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Journal of Organizational and End User Computing* 16 (3):22-40.

Backhouse, J., and G. Dhillon. 1995. Managing computer crime: a research outlook. *Computers & Security* 14 (7):645-651.

Bagozzi, R. P. 1980. *Causal Modeling in Marketing*. New York, NY: John Wiley & Sons, Inc.

Bagozzi, R. P., and Y. Yi. 1988. On the evaluation of structural equation models. *Journal of the Academy of Marketing Science* 16 (1):74-94.

Bandura, A. 1977. Self-efficacy: Toward a unifying theory of behavioral change. *Psychological review* 84 (2):191-215.

———. 1977. *Social Learning Theory*. New York, NY: General Learning Press.

Bateman, T. S., and J. M. Crant. 1993. The Proactive Component of Organizational Behavior: A Measure and Correlates. *Journal of Organizational Behavior* 14 (2):103-118.

Bateman, T. S., and D. W. Organ. 1983. Job Satisfaction and the Good Soldier: The Relationship between Affect and Employee "Citizenship". *Academy of Management Journal* 26 (4):587-595.

Beck, K. H. 1984. The effects of risk probability, outcome severity, efficacy of protection and access to protection on decision making: A further test of protection motivation theory. *Social Behavior and Personality* 12 (2):121-125.

Beck, K. H., and R. H. Feldman. 1983. Information seeking among safety and health managers. *The Journal of psychology* 115 (1st Half):23-31.

Bedeian, A. G., and A. A. Armenakis. 1981. A Path-Analytic Study of the Consequences of Role Conflict and Ambiguity. *Academy of Management Journal* 24 (2):417-424.

Bennett, R. J., and S. L. Robinson. 2000. Development of a measure of workplace deviance. *Journal of Applied Psychology* 85 (3):349-360.

———. 2003. The past, present, and future of workplace deviance research. In *Organizational behavior: The state of the science*, edited by J. Greenberg. Mahwah, NJ: Lawrence Erlbaum.

Berry, C. M., D. S. Ones, and P. R. Sackett. 2007. Interpersonal deviance, organizational deviance, and their common correlates: A review and meta-analysis. *Journal of Applied Psychology* 92 (2):410-424.

Block, L. G., and P. A. Keller. 1995. When to accentuate the negative: The effects of perceived efficacy and message framing on intentions to perform a health-related behavior. *Journal of Marketing Research* 32 (2):192-203.

Bloom, M., and G. T. Milkovich. 1998. Relationships among Risk, Incentive Pay, and Organizational Performance. *Academy of Management Journal* 41 (3):293-297.

Boss, S. R., L. J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss. 2009. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems* 18 (2):151-164.

Brouwers, M. C., and R. M. Sorrentino. 1993. Uncertainty orientation and protection motivation theory: The role of individual differences in health compliance. *Journal of Personality and Social Psychology* 65 (1):102-112.

Byrd, T. A., K. L. Cossick, and R. W. Zmud. 1992. A Synthesis of Research on Requirements Analysis and Knowledge Acquisition Techniques. *MIS Quarterly* March 1992:117-138.

Cammann, C., M. Fichman, D. Jenkins, and J. Klesh. 1983. Assessing the attitudes and perceptions of organizational members. In *Assessing organizational change: A guide to methods, measures and practices*, edited by S. Seashore, E. Lawler, P. Mirvis and C. Cammann. New York, NY: John Wiley.

Campion, M. A., G. J. Medsker, and A. C. Higgs. 1993. Relations between work group characteristics and effectiveness: Implications for designing effective work groups. *Personnel Psychology* 46:823-850.

Cattell, R. B. 1966. The Scree Test For The Number Of Factors. *Multivariate behavioral research* 1 (2):245-276.

Cavusoglu, H., H. Cavusoglu, and S. Raghunathan. 2004. Economics of IT security management: Four improvements to current security practices. *Communications of the Association for Information Systems (Volume 14, 2004)* 14:65-75.

Cavusoglu, H., B. Mishra, and S. Raghunathan. 2004. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce* 9 (1):70-104.

Cavusoglu, Hu., B. Mishra, and S. Raghunathan. 2005. The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research* 16 (1):28-46.

Cavusoglu, Hu., S. Raghunathan, and Ha. Cavusoglu. 2009. Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. *Information Systems Research* 20 (2):198-217.

Choobineh, J., G. Dhillon, M. R. Grimaila, and J. Rees. 2007. Management of Information Security: Challenges and Research Directions. *Communications of the Association for Information Systems* 20 (1):57.

CIOMagazine, CSOMagazine, and PricewaterhouseCoopers. 2009. Global State of Information Security Survey 2010.

Connolly, J. J., and C. Viswesvaran. 2000. The role of affectivity in job satisfaction: a meta-analysis *Personality and Individual Differences* 29 (2):265-281.

Crant, J. M. 1995. The Proactive Personality Scale and objective job performance among real estate agents. *Journal of Applied Psychology* 80 (4):532-537.

Cronan, T. P., C. B. Foltz, and T. W. Jones. 2006. Piracy, computer crime, and IS misuse at the university. *Communications of the ACM* 49 (6):84-90.

D'Arcy, J., and A. Hovav. 2007. Deterring internal information systems misuse. *Communications of the ACM* 50 (10):113-117.

———. 2008. In *Handbook of Research on Information Security and Assurance*.

———. 2009. An Integrative Framework for the Study of Information Security Management Research. In *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*, edited by M. Gupta and R. Sharman: Information Science Reference.

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

Da Veiga, A., and J. H. P. Eloff. 2010. A framework and assessment instrument for information security culture. *Computers & Security* 29 (2):196-207.

Dalal, R. S. 2005. A Meta-Analysis of the Relationship Between Organizational Citizenship Behavior and Counterproductive Work Behavior. *Journal of Applied Psychology* 90 (6):1241-1255.

de Leeuw, J., and W. J. Heiser. 1977. Convergence of Correction Matrix Algorithms for Multidimensional Scaling. In *Geometric Representations of Relational Data* edited by J. Lingoes. Ann Arbor, MI: Mathesis Press.

———. 1980. Multidimensional Scaling with Restrictions on the Configuration. In *Multivariate Analysis*, edited by P. Krishnaiah. Amsterdam, The Netherlands: North Holland Publishing Company.

de Leeuw, J., and P. Mair. 2008. Multidimensional Scaling Using Majorization: SMACOF in R: Department of Statistics at the University of California, Los Angeles.

Defining the Federal Information Security Mission: 2009 – 2014 Market Forecast. 2009. INPUT.

DeSarbo, W. S., R. Grewal, and C. J. Scott. 2008. A Clusterwise Bilinear Multidimensional Scaling Methodology for Simultaneous Segmentation and Positioning Analyses. *Journal of Marketing Research* 45 (3):280-292.

Dhillon, G. 2001. Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security* 20 (2):165-172.

Dhillon, G., and J. Backhouse. 2000. Information System Security Management in the New Millennium. *Communications of the ACM* 43 (7):125.

Dhillon, G., and S. Moores. 2001. Computer crimes: theorizing about the enemy within. *Computers & Security* 20 (8):715-723.

Dhillon, G., and G. Torkzadeh. 2006. Value-focused assessment of information system security in organizations. *Information Systems Journal* 16 (3):293-314.

Diamantopoulos, A., P. Riefler, and K. P. Roth. 2008. Advancing formative measurement models. *Journal of Business Research* 61:1203-1218.

Diamantopoulos, A., and J. A. Siguaw. 2006. Formative Versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration. *British Journal of Management* 17:263-282.

Diamantopoulos, A., and H. M. Winklhofer. 2001. Index Construction with Formative Indicators: An Alternative to Scale Development. *Journal of Marketing Research* 38 (May):269-277.

Dinev, T., J. Goo, Q. Hu, and K. Nam. 2009. User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal* 19 (4):391-412.

Dinev, T., and Q. Hu. 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems* 8 (1):23.

Dlamini, M. T., J. H. P. Eloff, and M. M. Eloff. 2009. Information security: The moving target. *Computers & Security* 28 (3-4):189-198.

Doty, D. H., and W. H. Glick. 1994. Typologies as a unique form of theory building: Toward improved understanding and modeling. *Academy of Management Review* 19 (2):230-251.

Eppright, D. R., J. B. Hunt, J. F. Tanner, and G. R. Franke. 2002. Fear, coping, and information: A pilot study on motivating a healthy response. *Health Marketing Quarterly* 20 (1):51-73.

Fagnot, I. J. 2008. Behavioral Information Security. In *Encyclopedia of Cyber Warfare and Cyber Terrorism*, edited by L. J. Janczewski and A. M. Colarik. Hershey, PA: Information Science Reference.

Falbo, T. 1977. Multidimensional scaling of power strategies. *Journal of Personality and Social Psychology* 35 (8):537-547.

Floyd, D. L., S. Prentice-Dunn, and R. W. Rogers. 2000. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology* 30 (2):407-429.

Flynn, M. F., R. D. Lyman, and S. Prentice-Dunn. 1995. Protection motivation theory and adherence to medical treatment regimens for muscular dystrophy. *Journal of Social and Clinical Psychology* 14 (1):61-75.

Fornell, C., and D. F. Larcker. 1981. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* 18 (1):39-50.

Fruin, D. J., C. Pratt, and N. Owen. 1992. Protection motivation theory and adolescents' perceptions of exercise. *Journal of Applied Social Psychology* 22 (1):55-69.

Fuller, J. B., L. E. Marler, and K. Hester. 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):1089-1120.

Gartner. 2009. Security Software and Services Spending Will Outpace Other IT Spending Areas in 2010.

George, J. M. 1990. Personality, affect, and behavior in groups. *Journal of Applied Psychology* 75 (2):107-116.

Gibney, R., T. J. Zagenczyk, and M. F. Masters. 2009. The Negative Aspects of Social Exchange: An Introduction to Perceived Organizational Obstruction. *Group & Organization Management* 34 (6):665-697.

Global IT Security Market Forecast to 2012 2008. RNCOS E-Services Private Limited.

Goodman, P. S., and S. Garber. 1988. Absenteeism and accidents in a dangerous environment: Empirical analysis of underground coal mines. *Journal of Applied Psychology* 73 (1):81-86.

Green, P. E., and F. J. Carmone. 1970. *Multidimensional scaling and related techniques in marketing analysis*. Boston, MA: Allyn and Bacon.

Greening, L. 1997. Adolescents' Cognitive Appraisals of Cigarette Smoking: An Application of the Protection Motivation Theory. *Journal of Applied Social Psychology* 27 (22):1972-1985.

Grey, J. M. 1977. Multidimensional percpetual scaling of musical timbres. *Journal of the Acoustical Society of America* 61 (5):1270-1277.

Groenen, P. J. F., and M. van de Velden. 2004. Multidimensional Scaling: Econometric Institute Report.

Gurung, A., X. Luo, and Q. Liao. 2009. Consumer motivations in taking action against spyware: an empirical investigation. *Information Management and Computer Security* 17 (3):276-289.

Hackman, J. R., and G. R. Oldham. 1975. Development of the Job Diagnostic Survey. *Journal of Applied Psychology* 60 (2):159-170.

Hair, J. F., W. Black, B. Babin, R. E. Anderson, and R. L. Tatham. 2006. *Multivariate Data Analysis*. Upper Saddle River, NJ: Pearson Education.

Hamill, J. T., R. F. Deckro, and J. M. Kloeber. 2005. Evaluating information assurance strategies. *Decision Support Systems* 39 (3):463-484.

Hanisch, K. A., and C. L. Hulin. 1991. General attitudes and organizational withdrawal: An evaluation of a causal model. *Journal of Vocational Behavior* 39:110-128.

Hanisch, K. A., C. L. Hulin, and M. Roznowski. 1998. The importance of individuals' repertoires of behaviors: the scientific appropriateness of studying multiple behaviors and general attitudes. *Journal of Organizational Behavior* 19 (5):463-480.

Hansen, J. V., P. B. Lowry, R. D. Meservy, and D. M. McDonald. 2007. Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection. *Decision Support Systems* 43 (4):1362-1374.

Harrington, S. J. 1996. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly* 20 (3):257-278.

Harrison, D. A., and J. J. Martocchio. 1998. Time for Absenteeism: A 20-Year Review of Origins, Offshoots, and Outcomes *Journal of Management* 24 (3):305-350.

Herath, T., and H. R. Rao. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47 (2):154-165.

———. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* 28 (2):106-125.

Hitchings, J. 1995. Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Computers & Security* 14 (5):377-383.

Huang, Z., H. Chen, F. Guo, J. J. Xu, S. Wu, and W. H. Chen. 2006. Expertise visualization: An implementation and study based on cognitive fit theory. *Decision Support Systems* 42 (3):1539-1557.

Hui, C., K. S. Law, and Z. X. Chen. 1999. A Structural Equation Model of the Effects of Negative Affectivity, Leader-Member Exchange, and Perceived Job Mobility on In-role and Extra-role Performance: A Chinese Case. *Organizational Behavior and Human Decision Processes* 77 (1):3-21.

Im, G. P., and R. L. Baskerville. 2005. A longitudinal study of information system threat categories: the enduring problem of human error. *ACM SIGMIS Database* 36 (4):68-79.

IT Security Market Report 2009 2009. Key Note Publications Ltd.

ITRC. 2009. 2009 Data Breach Insider Theft Category Summary. San Diego, CA: Identity Theft Resource Center.

Jain, A. K., A. Ross, and S. Pankanti. 2006. Biometrics: a tool for information security. *IEEE transactions on information forensics and security* 1 (2):125-143.

Jenkins, G. D., A. Mitra, N. Gupta, and J. D. Shaw. 1998. Are financial incentives related to performance? A meta-analytic review of empirical research. *Journal of Applied Psychology* 83 (5):777-787.

Johnston, A. C., and M. E. Warkentin. 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly* 34 (2).

Joreskog, K. G., and A. S. Goldberger. 1975. Estimation of a Model with Multiple Indicators and Multiple Causes of a Single Latent Variable. *Journal of the American Statistical Association* 70 (351):631-639.

Judge, T. A., C. L. Jackson, J. C. Shaw, B. A. Scott, and B. L. Rich. 2007. Self-Efficacy and Work-Related Performance: The Integral Role of Individual Differences. *Journal of Applied Psychology* 92 (1):107-127.

Junglas, I. A., N. A. Johnson, and C. Spitzmuller. 2008. Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems* 17 (4):387-402.

Katz, D., and R. L. Kahn. 1978. *The Social Psychology of Organizations*. 2nd ed. New York, NY: John Wiley & Sons, Inc.

Keller, R. T. 1997. Job involvement and organizational commitment as longitudinal predictors of job performance: A study of scientists and engineers. *Journal of Applied Psychology* 82 (4):539-545.

Kenkel, N. C., and L. Orloci. 1986. Applying Metric and Nonmetric Multidimensional Scaling to Ecological Studies: Some New Results. *Ecology* 67 (4):919-928.

Knapp, K. J., T. E. Marshall, R. K. Rainer, and F. N. Ford. 2006. Information Security: Management's Effect on Culture and Policy. *Information Management & Computer Security* 14 (1):24-36.

Kotulic, A. G., and J. G. Clark. 2004. Why there aren't more information security research studies. *Information & Management* 41:597-607.

Kruskal, J. B. 1977. The Relationship between Multidimensional Scaling and Clustering. In *Classification and Clustering*, edited by J. V. Ryzin. New York, NY: Academic Press.

Kruskal, J. B., and M. Wish. 1978. *Multimdimensional Scaling*. Beverly Hills, CA: Sage Publications.

Lee, D., R. Larose, and N. Rifon. 2008. Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology* 27 (5):445-454.

Lee, K., and N. J. Allen. 2002. Organizational citizenship behavior and workplace deviance: The role of affect and cognitions. *Journal of Applied Psychology* 87 (1):131-142.

Lee, S. M., S. G. Lee, and S. Yoo. 2004. An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management* 41 (6):707-718.

Lee, Y., and K. A. Kozar. 2008. An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management* 45 (2):109-119.

Lee, Y., and K. R. Larsen. 2009. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems* 18 (2):177-187.

Leonard-Barton, D., and I. Deschamps. 1988. Managerial Influence in the Implementation of New Technology. *Management Science* 34 (10):1252-1265.

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

Lindell, M. K., and D. J. Whitney. 2001. Accounting for Common Method Variance in Cross-Sectional Research Designs. *Journal of Applied Psychology* 86 (1):114-121.

Loch, K. D., H. H. Carr, and M. E. Warkentin. 1992. Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly* 16 (2):173-186.

Luchak, A. A., and I. R. Gellatly. 2007. A comparison of linear and nonlinear relations between organizational commitment and work outcomes. *Journal of Applied Psychology* 92 (3):786-793.

MacKenzie, S. B., P. M. Podsakoff, and M. Ahearne. 1998. Some Possible Antecedents and Consequences of In-Role and Extra-Role Salesperson Performance. *Journal of Marketing* 62 (3):87-98.

MacKenzie, S. B., P. M. Podsakoff, and C.B. Jarvis. 2005. The Problem of Measurement Model Misspecification in Behavioral and Organizational Research and Some Recommended Solutions. *Journal of Applied Psychology* 90 (4):710-730.

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

Magklaras, G. B., and S. M. Furnell. 2005. A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security* 24 (5):371-380.

Matook, S., and I. Vessey. 2008. Types of Business-to-Business E-Marketplaces: The Role of a Theory-based, Domain-specific Model. *Journal of Electronic Commerce Research* 9 (4):260-279.

McNeely, B. L., and B. M. Meglino. 1994. The role of dispositional and situational antecedents in prosocial organizational behavior: An examination of the intended beneficiaries of prosocial behavior. *Journal of Applied Psychology* 79 (6):836-844.

Meyer, J. P., and N. J. Allen. 1997. *Commitment in the workplace*. Thousand Oaks, CA: Sage Publications.

Meyer, J. P., S. V. Paunonen, I. R. Gellatly, R. D. Goffin, and D. N. Jackson. 1989. Organizational commitment and job performance: It's the nature of the commitment that counts. *Journal of Applied Psychology* 74 (1):152-156.

Milne, S., P. Sheeran, and S. Orbell. 2000. Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology* 30 (1):106-143.

Mitnick, K. 2003. Are You the Weak Link. *Harvard Business Review* 81 (4):18-20.

Moon, H., D. Kamdar, D.M. Mayer, and R. Takeuchi. 2008. Me or We? The Role of Personality and Justice as Other-Centered Antecedents to Innovative Citizenship Behaviors Within Organizations. *Journal of Applied Psychology* 93 (1):84-94.

Moore, A. P., D. M. Cappelli, and R. F. Trzeciak. 2008. The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures: Software Engineering Institute: Carnegie Mellon University.

Morrison, E. W., and C. C. Phelps. 1999. Taking Charge at Work: Extrarole Efforts to Initiate Workplace Change. *Academy of Management Journal* 42 (4):403-419.

Mount, M., R. Ilies, and E. Johnson. 2006. Relationship of personality traits and counterproductive work behaviors: The mediating effects of job satisfaction. *Personnel Psychology* 59 (3):591-622.

Moyle, P. 1995. The Role of Negative Affectivity in the Stress Process: Tests of Alternative Models. *Journal of Organizational Behavior* 16 (6):647-668.

Muralidhar, K., and R. Sarathy. 2005. An enhanced data perturbation approach for small data sets. *Decision Sciences* 36 (3):513-529.

Myyry, L., M. Siponen, S. Pahnila, T. Vartiainen, and A. Vance. 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems* 18 (2):126-139.

Neuwirth, K., S. Dunwoody, and R. J. Griffin. 2000. Protection Motivation and Risk Communication. *Risk Analysis* 20 (5):721-734.

Ng, B. Y., A. Kankanhalli, and Y. Xu. 2009. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems* 46 (4):815-825.

Nunnally, J. C. 1978. *Psychometric theory*. New York: McGraw-Hill.

Oppliger, R. 2007. IT Security: In Search of the Holy Grail. *Communications of the ACM* 50 (2):96-98.

Orbell, S., and P. Sheeran. 1998. "Inclined abstainers": A problem for predicting health-related behaviour. *British Journal of Social Psychology* 37 (2):151-165.

Organ, D. W. 1988. *Organizational citizenship behavior: The good soldier syndrome*. Lexington, MA: Lexington Books.

Organ, D. W., P. M. Podsakoff, and S. B. MacKenzie. 2006. *Organizational Citizenship Behaviors: Its Nature, Antecedents, and Consequences*. Thousand Oaks, CA: Sage Publications, Inc.

Oz, E. 1992. Ethical standards for information systems professionals: A case for a unified code. *MIS Quarterly* 16 (4):423-433.

Padgett, D., and M. S. Mulvey. 2007. Differentiation Via Technology: Strategic Positioning of Services Following the Introduction of Disruptive Technology. *Journal of Retailing* 83 (4):375-391.

Parker, S. K. 1998. Enhancing role breadth self-efficacy: The roles of job enrichment and other organizational interventions. *Journal of Applied Psychology* 83 (6):835-852.

———. 2000. From passive to proactive motivation: The importance of flexible role orientations and role breadth self-efficacy. *Applied Psychology: An International Review* 49:447-469.

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

Peace, A. G., D. F. Galletta, and J. Y. L. Thong. 2003. Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems* 20 (1):153-177.

Pearce, J. L., and H. B. Gregersen. 1991. Task Interdependence and Extrarole Behavior: A Test of the Mediating Effects of Felt Responsibility. *Journal of Applied Psychology* 76 (6):838-844.

Pechmann, C., G. Zhao, M. E. Goldberg, and E. T. Reibling. 2003. What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *The Journal of Marketing* 67 (2):1-18.

Peterson, M. F., P. B. Smith, A. Akande, S. Ayestaran, S. Bochner, V. Callan, N. G. Cho, J. C. Jesuino, M. D'Amorim, P. Francois, K. Hofmann, P. L. Koopman, K. Leung, T. K. Lim, S. Mortazavi, J. Munene, M. Radford, A. Ropo, G. Savage, B. Setiadi, T. N. Sinha, R. Sorenson, and C. Viedge. 1995. Role Conflict, Ambiguity, and Overload: A 21-Nation Study. *Academy of Management Journal* 38 (2):429-452.

Petter, S., D. W. Straub, and A. Rai. 2007. Specifying Formative Constructs in Information Systems Research. *MIS Quarterly* 31 (4):623-656.

Podsakoff, N. P., S. W. Whiting, P. M. Podsakoff, and B. D. Blume. 2009. Individual- and Organizational-Level Consequences of Organizational Citizenship Behaviors: A Meta-Analysis. *Journal of Applied Psychology* 94 (1):122-141.

Podsakoff, P. M., M. Ahearne, and S. B. MacKenzie. 1997. Organizational citizenship behavior and the quantity and quality of work group performance. *Journal of Applied Psychology* 82 (2):262-270.

Podsakoff, P. M., S. B. MacKenzie, J. Y. Lee, and N. P. Podsakoff. 2003. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology* 88 (5):879-903.

Podsakoff, P. M., S. B. MacKenzie, J. B. Paine, and D. G. Bachrach. 2000. Organizational Citizenship Behaviors: A Critical Review of the Theoretical and Empirical Literature and Suggestions for Future Research. *Journal of Management* 26 (3):513-563.

Posey, C., R. J. Bennett, T. Roberts, and P. B. Lowry. 2010. When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse. In *Working Paper*. Ruston, LA: Louisiana Tech University.

Posey, C., P. B. Lowry, T. Roberts, and T. S. Ellis. 2010. The Online Community Self-Disclosure Model: The Case of Working Professionals in France and the UK Who Use Online Communities. *European Journal of Information Systems*.

Price, S. M. 2007. Operations Security. In *Official (ISC)2 Guide to the CISSP CBK*, edited by H. F. Tipton and K. Henry. Boca Raton, FL: Auerbach.

Priem, R. L., L. G. Love, and M. A. Shaffer. 2002. Executives' perceptions of uncertainty sources: a numerical taxonomy and underlying dimensions. *Journal of Management* 28 (6):725-746.

Rabinowitz, G. B. 1975. An introduction to nonmetric multidimensional scaling. *American Journal of Political Science* 19 (2):343-390.

Rice, R. E. 1994. Relating Electronic Mail Use and Network Structure to R&D Work Networks and Performance. *Journal of Management Information Systems* 11 (1):9-29.

Richardson, R. 2007. CSI Computer Crime & Security Survey. San Francisco, CA: Computer Security Institute.

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

Rizzo, J. R., R. J. House, and S. I. Lirtzman. 1970. Role Conflict and Ambiguity in Complex Organizations. *Administrative Science Quarterly* 15 (2):150-163.

Robinson, S. L., and R. J. Bennett. 1995. A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal* 38 (2):555-572.

Robinson, S. L., and A. M. O'Leary-Kelly. 1998. Monkey see, monkey do: The influence of work groups on the antisocial behavior of employees. *Academy of Management Journal* 41 (6):658-672.

Rogers, R. W. 1975. A protection motivation theory of fear appeals and attitude change. *Journal of Psychology* 91:93-114.

———. 1983. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In *Social psychophysiology: A sourcebook*, edited by J. T. Cacioppo and R. E. Petty. New York: Guilford.

Rogers, R. W., and S. Prentice-Dunn. 1997. Protection motivation theory. In *Handbook of health behavior research I: Personal and social determinants*, edited by D. S. Gochman. New York: Plenum Press.

Schiffman, S. S., M. L. Reynolds, and F. W. Young. 1981. *Introduction to multidimensional scaling: Theory, methods, and applications*. New York, NY: Academic Press.

Schneier, B. 2000. *Secrets and Lies: Digital Security in a Networked World*. New York, NY: John Wiley & Sons, Inc.

Seibert, S. E., J. M. Crant, and M. L. Kraimer. 1999. Proactive personality and career success. *Journal of Applied Psychology* 84 (3):416-427.

Shang, J., D. Z. Basil, and W. Wymer. 2010. Using social marketing to enhance hotel reuse programs. *Journal of Business Research* 63 (2):166-172.

Sharma, R., and P. Yetton. 2003. The Contingent Effects of Management Support and Task Interdependence on Successful Information Systems Implementation. *MIS Quarterly* 27 (4):533-556.

Shaw, E., K. G. Ruby, and J. M. Post. 1998. The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin* 2:1-10.

Shelton, M. L., and R. W. Rogers. 1981. Fear-arousing and empathy-arousing appeals to help: The pathos of persuasion. *Journal of Applied Social Psychology* 11 (4):366-378.

Siponen, M. 2000. A conceptual foundation for organizational information security awareness. *Information Management and Computer Security* 8 (1):31-41.

———. 2001. An analysis of the recent IS security development approaches: descriptive and prescriptive implications. In *Information security management - global challenges in the next millennium*, edited by G. Dhillon: Idea Group.

Siponen, M., and H. Oinas-Kukkonen. 2007. A review of information security issues and respective research contributions. *ACM SIGMIS Database* 38 (1):60-80.

Siponen, M., S. Pahnila, and A. Mahmood. 2007. Employees' Adherence to Information Security Policies: An Empirical Study. In *New Approaches for Security, Privacy and Trust in Complex Environments*, edited by H. Venter, M. Eloff, L. Labuschagne, J. Eloff and R. von Solms. Boston: Springer.

Siponen, M., and R. Willison. 2007. A Critical Assessment of IS Security Research Between 1990-2004. Paper read at 15th European Conference on Information Systems, June 7-9, at St. Gallen, Switzerland.

———. 2009. Information security management standards: Problems and solutions. *Information & Management* 46 (5):267-270.

Sircar, S., S. P. Nerur, and R. Mahapatra. 2001. Revolution or Evolution? A Comparison of Object-Oriented and Structured Systems Development Methods. *MIS Quarterly* 25 (4):457-471.

Somers, M. J. 1995. Organizational Commitment, Turnover and Absenteeism: An Examination of Direct and Interaction Effects. *Journal of Organizational Behavior* 16 (1):49-58.

Spector, P. E. 2006. Method Variance in Organizational Research: Truth or Urban Legend? *Organizational Research Methods* 9 (2):221-232.

Spreitzer, G. M. 1995. Psychological Empowerment in the Workplace: Dimensions, Measurement, and Validation. *Academy of Management Journal* 38 (5):1442-1465.

Spreitzer, G. M., S.C. de Janasz, and R.E. Quinn. 1999. Empowered to Lead: The Role of Psychological Empowerment in Leadership. *Journal of Organizational Behavior* 20 (4):511-526.

Stanton, J. M., and K. R. Stam. 2006. *The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets-Without Compromising Employee Privacy or Trust*. Medford, NJ: Information Today, Inc.

Stanton, J. M., K. R. Stam, P. Mastrangelo, and J. A. Jolton. 2005. Analysis of end user security behaviors. *Computers & Security* 24 (2):124-133.

Stanton, J. M., K. R. Stam, P. M. Mastrangelo, and J. A. Jolton. 2006. Behavioral Information Security: An Overview, Results, and Research Agenda. In *Human-Computer Interaction and Management Information Systems: Foundations*, edited by P. Zhang and D. F. Galletta. Armonk, NY: M.E. Sharpe.

Stoeva, A. Z., R. K. Chiu, and J. H. Greenhaus. 2002. Negative Affectivity, Role Stress, and Work–Family Conflict *Journal of Vocational Behavior* 60 (1):1-16.

Straub, D. W. 1989. Validating instruments in MIS research. *MIS Quarterly* 13 (2):147-169.

———. 1990. Effective IS Security. *Information Systems Research* 1 (3):255-276.

Straub, D. W., M. C. Boudreau, and D. Gefen. 2004. Validation Guidelines for IS Positivist Research. *Communications of the Association for Information Systems* 13.

Straub, D. W., and R. W. Collins. 1990. Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *MIS Quarterly* 14 (2):143-156.

Straub, D. W., and W. D. Nance. 1990. Discovering and disciplining computer abuse in organizations: a field study. *MIS Quarterly* 14 (1):45-60.

Straub, D. W., and R. J. Welke. 1998. Coping with systems risk: security planning models for management decision making. *MIS Quarterly* 22 (4):441-469.

Tan, F. B., and M. G. Hunter. 2002. The Repertory Grid Technique: A Method for the Study of Cognition in Information Systems. *MIS Quarterly* 26 (1):39-57.

Tanner, J. F., E. Day, and M. R. Crask. 1989. Protection motivation theory: An extension of fear appeals theory in communication. *Journal of Business Research* 19 (4):267-276.

Tanner, J. F., J. B. Hunt, and D. R. Eppright. 1991. The Protection Motivation Model: A Normative Model of Fear Appeals. *Journal of Marketing* 55 (3):36-45.

Theoharidou, M., S. Kokolakis, M. Karyda, and E. Kiountouzis. 2005. The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security* 24 (6):472-484.

Thomas, K. W., and B. A. Velthouse. 1990. Cognitive Elements of Empowerment: An "Interpretive" Model of Intrinsic Task Motivation. *Academy of Management Review* 15 (4):666-681.

Thompson, J. A. 2005. Proactive Personality and Job Performance: A Social Capital Perspective. *Journal of Applied Psychology* 90 (5):1011-1017.

Thomson, K. L., R. von Solms, and L. Louw. 2006. Cultivating an organizational information security culture. *Computer Fraud & Security* 2006 (10):7-11.

Thong, J. Y. L., C. Yap, and K. S. Raman. 1996. Top Management Support, External Expertise and Information Systems Implementation in Small Businesses. *Information Systems Research* 7 (2):248-267.

Trompeter, C. M., and J. H. P. Eloff. 2001. A framework for the implementation of socio-ethical controls in information security. *Computers & Security* 20 (5):384-391.

Tubre, T. C., and J. M. Collins. 2000. Jackson and Schuler (1985) Revisited: A Meta-Analysis of the Relationships Between Role Ambiguity, Role Conflict, and Job Performance. *Journal of Management* 26 (1):155-169.

Van Kessel, P. 2009. Outpacing Change: Ernst & Young's 12th Annual Global Information Security Survey.

Van Niekerk, J. F., and R. von Solms. 2010. Information security culture: A management perspective *Computers & Security* In Press.

Vance, A., M. Siponen, and S. Pahnila. 2009. How Personality and Habit Affect Protection Motivation. Paper read at Association of Information Systems SIGSEC Workshop on Information Security & Privacy (WISP), at Phoenix, AZ.

Von Solms, B. 2000. Information Security—The Third Wave? *Computers & Security* 19 (7):615-620.

Vroom, C., and R. von Solms. 2004. Towards information security behavioural compliance. *Computers & Security* 23 (3):191-198.

Walsham, G. 1996. Ethical theory, codes of ethics and IS practice. *Information Systems Journal* 6 (1):69-81.

Warkentin, M. E., and R. Willison. 2009. Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems* 18 (2):101-105.

Watson, D., and L. A. Clark. 1984. Negative affectivity: The disposition to experience aversive emotional states. *Psychological Bulletin* 96 (3):465-490.

Watson, D., L. A. Clark, and A. Tellegen. 1988. Development and validation of brief measures of positive and negative affect: The PANAS scales. *Journal of Personality and Social Psychology* 54 (6):1063-1070.

Watson, D., and J. W. Pennebaker. 1989. Health complaints, stress, and distress: Exploring the central role of negative affectivity. *Psychological Review* 96 (2):234-254.

Welbourne, T. M., D. E. Johnson, and A. Erez. 1998. The Role-Based Performance Scale: Validity Analysis of a Theory-Based Measure. *Academy of Management Journal* 41 (5):540-555.

Whitman, M. E. 2003. Enemy at the gate: threats to information security. *Communications of the ACM* 46 (8):91-5.

Whitman, M. E., and H. J. Mattord. 2009. *Principles of information security*: Thomson Course Technology.

Wilcox, J. B., R. D. Howell, and E. Breivik. 2008. Questions about formative measurement. *Journal of Business Research* 61:1219-1228.

Williams, L. J., and S. E. Anderson. 1991. Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. *Journal of Management* 17 (3):601-617.

Willison, R., and J. Backhouse. 2006. Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems* 15 (4):403-414.

Witte, K., K. A. Cameron, J. K. McKeon, and J. M. Berkowitz. 1996. Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. *Journal of Health Communication* 1 (4):317-342.

Wolf, S., W. L. Gregory, and W. G. Stephan. 1986. Protection motivation theory: Prediction of intentions to engage in anti-nuclear war behaviors. *Journal of Applied Social Psychology* 16 (4):310-321.

Woon, I. M. Y., R. T. Low, and G. W. Tan. 2005. A protection motivation theory approach to home wireless security. Paper read at International Conference on Information Systems, at Las Vegas, NV.

Workman, M., W. H. Bommer, and D. W. Straub. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior* 24 (6):2799-2816.

Yue, W. T., and M. Cakanyildirim. 2007. Intrusion prevention in information systems: Reactive and proactive responses. *Journal of Management Information Systems* 24 (1):329-353.