THE UNIVERSITY OF TEXAS AT SAN ANTONIO, COLLEGE OF BUSINESS

Working Paper SERIES

WP # 0044IS-019-2013

Date May 7, 2013

Information Security Subcultures of Professional Groups in Organizations: A Conceptual Framework

V. Srinivasan (Chino) Rao
Department of Information Systems and Cyber Security
University of Texas at San Antonio
San Antonio, TX 78249

Sriraman Ramachandran
Global Program Manager
Dell, Inc.
Austin, TX.

Diane Walz
Department of Information Systems and Cyber Security
University of Texas at San Antonio
San Antonio, TX 78249

UTSA
COLLEGE OF BUSINESS KNOWLEDGE FOR A NEW WORLD

ONE UTSA CIRCLE
SAN ANTONIO, TEXAS 78249-0631
210 458-4317 | BUSINESS.UTSA.EDU

Information Security Subcultures of Professional Groups in Organizations: A Conceptual Framework

By

V. Srinivasan (Chino) Rao
Department of Information Systems and Cyber Security
University of Texas at San Antonio
San Antonio, TX 78249
Phone: (210)-458-5786
Email: chino.rao@utsa.edu

Sriraman Ramachandran
Global Program Manager
Dell, Inc.
Austin, TX.
Email: sriraman_ramachandra@dell.com

Diane Walz
Department of Information Systems and Cyber Security
University of Texas at San Antonio
San Antonio, TX 78249
Phone: (210)-
Email: diane.walz@utsa.edu

UTSA Working Paper, 2013

Information Security Subcultures of Professional Groups in Organizations: A Conceptual Framework

Abstract

The need for a strong security culture in organizations has been emphasized by many researchers. Cultures in some organizations are known to be differentiated, i.e., there may be variations in cultures across professional groups within a single organization. The (sub)culture of a professional group in an organization is influenced by many factors. In the current article, we propose a theory-based conceptual framework for security subcultures of professional groups in organizations. The framework relates security subcultures to its antecedents. We emphasize the importance of examining security culture at the subculture level, the need to consider the security-based beliefs (espoused security subculture) separately from the security-based behaviors (enacted security subculture), and, to account for the conflicts between security and performance expectations.

Keywords: Information Security, Organizations
JEL Codes: L86; C8; L80

Introduction

Information security incidents continue to be reported at an alarming rate. Efforts to reduce such incidents are focused both on developing technical defenses and on controlling security-related behaviors of users. There are many approaches to influencing user or employee behaviors. One approach recommended by several researchers is the development of a strong information security culture in organizations. The culture of an organization is influenced and molded by many different factors. A conceptual framework relating factors relevant to security culture is essential to help develop an integrated plan to build a strong information security culture in an organization.

Organizational scholars have identified three perspectives in organizational culture: integrated, differentiated and fragmented (Martin 1992). In the current study, we adopt the differentiated perspective, i.e., there may be differences in the cultures of different groups in organizations. The existence of differences in cultures across professions has been documented by Trice (1993). Others have argued that cultures in an organization are not monolithic, but often differentiated (Chatman et al, 1998; Jermier et al, 1991). Consistent with these statements, it would not be surprising to find diverse information security subcultures within a single organization. In fact, differences in the information security cultures of different professions have been reported (Ramachandran et al, 2013, *forthcoming*). So, we build our framework on the premise that information security culture in an organization may also be differentiated. i.e., we build a framework for the information security subcultures of professional groups in an organization. We believe it is important to examine the framework for each profession separately to enable management to tailor the efforts to build information security culture to the specific needs of each profession.

The rest of the article is organized as follows. In the next section, we review the relevant literature. Following that, we develop the conceptual framework. Theoretical and empirical support is provided for each relationship. The article concludes with sections on discussion and conclusions.

Literature Review

Culture

In 1963, it was reported that there were over 160 definitions of culture (Kroeber and Kluckhorn, 1963). By 2006, more than 350 definitions had been articulated (Leidner et al., 2006). A review of the definitions suggests that culture is an aggregation of knowledge, beliefs, habits, values, ideas, behaviors, concepts, attitudes and so on (Ramachandran et al, 2013, *forthcoming*).

The generic perspective of culture has been viewed more specifically at different levels of analysis. For instance, Ouchi and Johnson (1978) define organizational culture as "how things are done around here." Peters and Waterman (Peters, 1982), in their best selling book *In Search of Excellence*, extend the Ouchi and Johnson (1978) work on culture and argue that the status of excellence of a company is strongly linked to the ability of the organization to create a strong culture with a strong vision. O'Reilly et al (1991) define organizational culture as "a set of cognitions shared by members of a social unit" and Hofstede (1980) views organizational culture as "the collective programming of the mind that distinguishes the members from one organization from another".

Organizational Culture's many components are parsimoniously reflected in the three-layer model (artifacts, values and assumptions) proposed by Schein (Schein, 1985) (see Fig. 1).

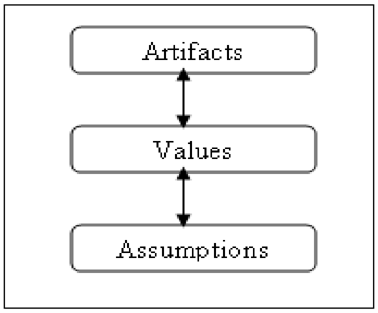


Fig. 1 Schein's (1985) **Model of Organizational Culture**

According to Schein (1985), organizational culture exists in three levels: on the surface are artifacts, underneath artifacts lies values and at the core are basic assumptions. Artifacts as seen in organizations are visible, tangible, and audible results of activity grounded in values and assumptions, and, include the behavior of members of the group. Values in organizations are the social principles, philosophies, goals, standards and beliefs considered to have intrinsic worth for members of the organization. Values include the beliefs held by members of the culture, which is another key element in the present study. Assumptions represent taken for granted beliefs about reality and human nature. Schein suggests interdependencies between the three layers, with reciprocal relationships between artifacts and values, and values and assumptions.

Summarizing the three level model of organizational culture, Schein refers to cultures as “the pattern of basic assumptions that a given group has invented, discovered or developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid, and therefore to be taught to new members as the correct way to perceive, think and feel in relation to these problems” (Schein 1985).

Differentiated Cultures in Organizations

In an organizational context, when the three layers are consistent with each other, there is an integrated culture (Martin, 1992). Martin further suggests that organizations may have differentiated or fragmented cultures. The differentiation or fragmentation may be the result of differences in cultures across groups in an organization. Alternately, there may be differences in the culture reflected in the various layers of Schein’s model. Often, espoused culture, i.e., culture as reflected in the stated beliefs of organizational members, may vary from enacted culture, i.e., culture observed in the behaviors of the organizational members. The difference between espoused and enacted cultures is referred as to action inconsistency (Martin, 1992).

Professional Cultures

Differentiation in cultures across professional groups has been reported by Trice (Trice, 1993a). Trice (1993b) notes that the occupational culture consists of a “set of taken-for-granted, emotionally charged beliefs, called ideologies”, identified with that particular occupation. Trice refers to the values and beliefs underlying a profession as the tacit component of occupational culture. In contrast, the explicit and easily observable parts of the occupational culture are the artifacts, which are mechanisms by which members express and affirm their beliefs. Some of the occupational artifacts include occupation-based myths, ceremonies, symbols, languages and gestures, physical artifacts, sagas and legends, rituals, taboos and rites. As individual members of the occupation express the underlying ideologies through various cultural forms and interact with other members, the ideologies tend to evolve and add new beliefs and values back into the system. Additions of new ideology and cultural forms help in the enrichment and expressiveness of the culture, but also complicate culture by making it fuzzy. Further, the differences in professional cultures are often the potential source of conflicts (Guzman et al 2008; Rao and Ramachandran, 2011), and consequently deserve attention in organizations.

In the fields of sociology, management and organization psychology, studies have been devoted to identifying the culture of various professions. Exemplars are studies of accounting (Montagna 1973), nursing (Brooks 1999), fishing (Miller and Van Maanen 1982), policing (Cochran and Bromley 2003), boxing (Wienburg 1952) and so on. There have been few studies focused on the understanding and characterization of IS occupational culture. Among these Schein (1985), Bahn (1995) and Iivari and Abrahmsson (2002) restrict their focus to only specialized subgroups of members in the IS profession (e.g., software engineers), whereas Guzman and associates have looked at a broader group of IS professionals (Guzman, Stanton, Stam, Vijayasri, Yamodo, Zakaria and Caldera 2004). Schein (1985) fleetingly indicates that data processing fraternity have their own norms, traditions and vision about the use and importance of technology; Bahn (1995), and Iivari and Abrahmsson (2002) restrict their focus to system designers and software engineers respectively. Bahn (1995) reviews existing literature in IS field about IS professionals, and, from that makes an argument for the existence of occupational subculture among the system designers. Iivari and Abrahamsson (2002) use case study of a small software development company to elicit the role of organizational culture in the implementation of user-centered design. From the analysis of the company, they report evidence to support that software engineers form a separate occupational subculture. Both Guzman et al (2004) and Rao and Ramachandran (2011) have reported the differences in professional cultures of IS personnel and managers.

Trice (1993a) argues that within an organization, members from a profession are subject to the influences of both the professional culture and the organizational culture. This may cause cultures of professional groups within an organization to differ from each other as a result of differences in the influences of the professional culture (Sackmann 1992), and may also be different from the primary organizational culture. Culture shared among members of different professional groups within organizations may enhance or undermine or coexist with the culture of the organization (Trice 1993a). Cultures of professional groups in organizations play an important role in defining the values and beliefs of the organizational members belonging to the profession. This in turn leads to differences in the thinking, reasoning and priorities of members of different professional groups (Hansen 1995). This raises the possibility that security subcultures of different professional groups may be different from each other in an organization. Ramachandran et al (2013, forthcoming) have reported differences in security cultures of professional groups outside the context of a single organization. Thus, the security subcultures of the professionals in an organization are likely to subject to both professional and organizational influences.

Espoused and Enacted Cultures

The Bath consultancy group put forth a model of culture (Hawkins 1997) based on Bollas's (1987) work on the exploration of "the unthought known". Hawkins (1997) points out that based on Bath's second model, organizational culture can be viewed along three levels of consciousness:

- *Unconscious culture:* Unconscious culture represents the unthought known that is consciously experienced but "unnoticed by conscious reflection and not able to be verbalized" (Hawkins 1997, p.429). This part of culture, while conceptually interesting, is difficult to study, and will not be included in further discussions.
- *Espoused culture:* Espoused culture represents "the public presentation of the collective self; i.e. the organizational persona" (Hawkins 1997, p.428) , and can be studied by reading and observing the public face of the organization. For instance, some auto companies may run television advertisements expressing their belief that gas mileage of their cars is important. Thus, the public pronouncements to their customers and their employees are that they subscribe to a culture of fuel efficiency.
- *Enacted conscious culture:* Enacted conscious culture represents "the lived culture that is externally noticed and can be clearly verbalized or expressed" (Hawkins 1997, p.428). In the hypothetical example cited above, it is possible that the auto company acts to improve

> the fuel efficiency of the cars and complies with government mandated goals for miles/gallon. Alternately, the company may fail to promote fuel efficiency innovations, and may negotiate with governmental authorities for exemptions from mandated fuel efficiency requirements. These actions reflect enacted culture.

The Bath model relates to the models proposed by Schein (1985). Unconscious culture in the Bath model relates partially to the assumptions in Schein's (1985) model. Some assumptions in the Schein model may be known and acknowledged at the conscious level, while others may not be. The unknown assumptions in the Schein model would correspond to the unconscious culture in the Bath model. Espoused culture in the Bath model reflects beliefs, which corresponds to the known assumptions in the assumptions layer of the Schein model, and the middle layer of values in the Schein (1985) model and includes ideologies and norms. Lastly, the enacted culture in the Bath model is the culture reflected in the behaviors of organizational members, which is a part of the artifacts in Schein's (1985) model.

The distinction between espoused and enacted culture becomes important when there is divergence between the two. For example, in professing cultural beliefs (espoused) about security, respondents are likely to state that they will comply with security rules and procedures. When it comes to actual behavior, they may be guided by more than security considerations, e.g., most actions in organizations have to take into consideration efficiency and productivity needs, which may lead to the compromising of security needs.

Security Culture

Dhillon's (1995) definition of security culture is as "the totality of human attributes such as behaviors, attitudes, and values that contribute to the protection of all kinds of information in a given organization" is generally accepted in the field, and is also consistent with the concept of culture. The relevance of security culture in organizations is best illustrated by Von Solm's wave model (Von Solms 2000) of the progression of IS security. The three waves in the progression of management of IS security have been identified as technical wave, management wave, and institutionalization wave (Von Solms 2000). The first wave, the technical wave, focused primarily on managing IS security by using computer technologies like authentication, and access control lists. In the second wave, the management wave, equal emphasis was placed on technical and management aspects of IS security management. The management wave was characterized by security policies, Chief Information Security Officers, organizational structures for IS security and so on. The third wave, the institutionalization wave, includes adoption of the best practices and codes of practices of IS security management from inside the organization (Von Solms 2000). There are four components of institutionalization wave: "information security standardization, international information security certification, cultivating an information security culture throughout a company, and implementing metrics to continually and dynamically measure information security aspects in a company" (Von Solms 2000). Out of the four components of the institutionalization wave, Von Solms (2000) places special emphasis on the cultivation of security culture. The special emphasis reflects the potential of security culture to ingrain secure behaviors into the day to day activities of the employees of the organization. Such behaviors are considered essential for successful realization of management's vision about

IS security (Von Solms 2000). Thus, the development of strong security culture in an organization is one of the key factors in the efforts of institutionalization of security practices.

Much of the study of security culture has been in an organizational context (e.g., Martins and Eloff, 2002; Ruighaver, Maynard and Chang 2007). Others have focused on the role of policies on security culture (Von Solms and Von Solms, 2004; Halliday and Von Solms, 1997). Recently, Ramachandran et al (2013), have raised the issue of variations in security cultures across professions. The issue of differentiated security cultures in organizations has not been addressed in published literature.

Overall, the review of literature on security cultures suggests the following issues. Organizational culture tends to be treated as a monolithic construct. Some researchers have argued that multiple subcultures may exist in one organization, usually delineated by professional affiliations (Jermier et al, 1991). It is generally accepted that subcultures usually form in organizations around existing divisions, departments, functional groups or professional groups (Trice, 1993a). The existence of professional security subcultures has been argued by Ramachandran et al (2013, forthcoming). Security subcultures in organizations is an issue that remains to be studied.

Conflicts between Security and Performance

In the current section, we review two bodies of literature. First, there is a body of literature that examines the conflicting demands placed on employee groups by the needs of safety and performance in the manufacturing environment. Saase et al. (2001) and Brostoff and Sasse (2001) have shown the parallels between safety and security based on Reason's (1990) model of human error. Thus, it is useful to review the literature on safety culture to examine if useful analogies can be drawn to inform the area of information security. Second, there is a body of literature that addresses the conflicting demands placed on employee groups by the needs of computer security and performance.

We reiterate that the term performance is used as a general term to refer to the output measures that are used to evaluate employees at different levels. For instance, the performance of a CEO of a company may be evaluated by the earnings per share, or the appreciation in the market value of the company over a period of time. The performance of project managers may be evaluated by observing the completion of projects in the projected time and within budget. The performance of a customer service agent may be evaluated by the number of customers complaints addressed in unit time. The examples emphasize that the term performance is being used in a generic term across all levels.

Parallels between Security and Safety

Safety focuses on physical assets including the lives of human beings, while security focuses on information security. Safety, in the context of industrial and occupational safety, is defined as protection of organization assets including material and human assets against failure, damage, error, accidents or harm. Information security is defined by The U.S. National Information Systems Security Glossary defines as:

> *"The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or provision of service to authorized users,*

> *including those measures necessary to detect, document and counter such threats.” (Committee 2003)*

Sasse et al. (2001) refer to safety and security tasks as ‘enabling tasks.’ An enabling task “.. is not a goal most users strive for; rather, it is seen to get in the way of their production tasks” (Sasse et al. 2001 , pp.128). In a manufacturing environment, safety is not the ultimate goal. The ultimate goal is the production of products or energy. Actions and investments related to safety do not increase the quantity of products made, but may prevent the loss of products already made or the damage to production facilities or human lives. Similarly, in the information processing environment, security is not the ultimate goal. The goal of information processing systems is to enable user access to information to facilitate decision making and the execution of other information tasks. Actions and investments related to information security, do not facilitate decision making directly, but are steps taken to prevent unauthorized access or destruction or alteration of data. Hence, both safety and security goals are referred to as “secondary goals” as opposed to the primary goals of production and information processing (Brostoff et al. 2001). In other words, security is a secondary goal to the primary goal of information processing, even as safety is a secondary goal to the primary goal of manufacturing. Bostroff and Sasse (2001) indicate that both security and safety may help organizations to be productive in the long-term, by reducing losses. However, in the short-term, the security tasks are competing with the information processing tasks for resources, even as safety tasks are competing for resources with production tasks.

Safety and Performance

In the context of nuclear energy, International Atomic Energy Agency (IAEA) defined safety culture as “…assembly of characteristics and attitudes in organizations and individuals which established that, as an overriding priority, nuclear plan safety issues receive the attention warranted by their significance” (IAEA 1991). Others provide similar definitions. For example, Cox and Cox (1991) note that safety culture reflects attitudes, perceptions, beliefs, and values of employees in relation to safety. Similarly, Carroll (1998) defines safety culture as “..a high value priority placed on worker safety and public safety by everyone in every group and at every level of the plant. It also refers to safety expectations that people will act to preserve and enhance safety, take personal responsibility for safety, and be rewarded consistent with these values”. In their extensive review of definitions of safety culture Wiegmann et al (2002) note that, most definitions of safety culture are stated at the group level or higher, and defined as the one encapsulating safety related beliefs, values, and attitudes that are shared by a group.

Further, there is evidence of heterogeneity in the safety culture across employee groups within the same organization. For instance, Zohar (1980) reports between-group variations in safety climate perceptions. Arboleda et al (2003) report differences in safety perceptions between truck drivers, dispatchers and safety directors in a trucking company.

Safety culture literature provides several examples of studies detailing the influence of performance expectations and safety expectations on safety performance of employees (Dawson, Willman, Clinton and M. 1988; Embrey 1992; Klen 1988; Wright 1986). In general, it is argued that performance pressures can compromise safety (Hoffman and Stetzer, 1996). Hoffman and Stetzer (1996) define performance pressure (also referred to as role overload) “as the degree to which role performance is seen as being affected by inadequate time, training, and resources" (p.310). They offer two explanations why performance related issues may lead to lapses in safety behavior, on the basis of a review of earlier literature. First, they argue that safety violations do not always lead to negative consequences, and in fact, may lead to benefits (at least in the short-term), i.e., being able to complete a task in less time. This often leads to a tendency to favor "short cuts." Second, when confronted with situations in which employees are falling behind on a task schedule, "they will focus on performance rather than safety objectives, because the former are more like to be more salient" (p.311).

Recent studies continue to confirm the influence of performance pressure on safety performance includes Mearns et al (2001), Leveson et al (2005), Weyman et al (2003), and Dong-Chul (2005). Based on a survey of 722 offshore oil workers, Mearns et al (2001) suggest that accidents can be better predicted by assessing the unsafe behavior of employees, and, unsafe behavior is in turn driven by performance pressures.

Thus, in sum, in the safety literature, there is evidence to argue that performance pressures may have a negative influence on safety behavior.

Security and Performance

The conflicting relationship between information security and performance has been discussed at several levels. For example, at the CEO level, Austin and Darby (2003) explain the CEO's dilemma regarding information security in this way:

> *Suppose a CEO spends aggressively to protect his company against the possibility of a serious security breach and that his competitors do not. Suppose further that nobody in the industry experiences a major security breach for a couple of years. The CEO will have nothing to show for his investment, and the company's earnings will be considerably lower than those of competitors. The CEO who persists too long in investments that result in nothing happening might soon be out of a job.* (p.123)

Austin and Darby (2003) go on to suggest that CEOs may consider doing the right thing about security as naïve, "when markets remain so willing to punish companies for not showing steady growth" (Austin et al. 2003, p.123).

Security conflicts with productivity goals at other levels also (see (Shimeall and McDermott 1999); (Adams and Sasse 1999)). Shimeall and McDermott (1999) discussing software security in an internet world state: "For example, most long-time programmers can remember using fixed-length buffers for input at one time or another in our careers. We can remember not testing for "can't happen" cases because writing and testing that code would delay a project even further" (Shimeall et al. 1999, p.59). This illustrates performance pressures experienced by project managers and programmers in the course of a systems development project.

At a user level, Sasse et al (2001) argues ".. users respond by circumventing security mechanisms, and perceive security as something that makes their life difficult." They go on to cite an example, "If a user has forgotten a password, but needs to log in to complete an urgent task, he will ask a colleague. Security policies stipulate that users should not share their passwords. Refusing the request in such a situation, however, makes the colleague appear uncooperative, and means she does not trust her colleague." This illustrates the conflict between the demands of security and performance at a user level. Other security researchers including Huston (2001), Besnard and Arief (2003), and, Sapp and Behrens (2003) also address the issue of conflict between security and performance at the user level.

Thus, computer security literature is consistent with safety literature in the expectation that performance pressures have negative influences on security behaviors.

Influences of Top Management Teams

A firm's TMT, i.e., the "dominant coalition" (Cyert and March 1963; March and Simon 1958), consists of Chief Executive Officers (CEO) and several of his or her upper-level managers. Typically members of the dominant coalition may differ from one another on several factors including age, tenure in the organization, educational background, and functional expertise (Wiersema and Bantel 1992). The "dominant coalition" (Cyert et al. 1963) of individuals play an important role in the organization. TMTs identify environmental opportunities and problems, interpret relevant information, assess the capabilities of the organization, device organizational strategy and nurture the culture that would be followed across the firm (Mintzberg 1979).

In 1984, Hambrick and Mason (1984) put forth the Upper Echelon Theory, which conceptualized the influence of top management teams (TMT) on organizational outcomes. The main argument of Upper Echelon Theory is that the values and cognitive bases of powerful actors, who comprise the TMT, influence the strategic choices and outcomes in organizations (Hambrick et al. 1984).

Research on TMT focuses on understanding the factors, which influence the decision making of upper level managers, and, on empirically demonstrating the influence of TMT on strategic choices and organizational performance. The factors affecting TMT decision making is based on March's assertion (March, 1958) that upper level managers make decisions which are consistent with their cognitive base, and the "givens" they bring into to the decision. The givens of the decision makers reflect their "1) knowledge or assumptions about the future events, 2) knowledge of alternatives, and 3) knowledge of consequences attached to alternatives" (Hambrick et al. 1984). Givens of the upper level managers are also tightly coupled with their values and beliefs. Their values and beliefs may be influenced by a multitude of factors including their functional expertise, educational background, the culture of the professional group they subscribe to in the organization and the dominant profession of the organization. The cognitive base and the givens of the members of the TMTs act as a filter between the decision maker and understanding of the problem. Hambrick and Mason (1984) further argue that TMT will collectively work as a team to economize the influences of each member's cognitive bases on their understanding of the problem.

The effects of TMT have been reported by several scholars. For instance, there is evidence that TMT do influence organizational outcomes (Finkelstein and Hambrick 1990), organizational innovation (Bantel and Jackson 1989), and strategic change (Wiersema et al. 1992). Research in the strategic management literature provides support for the linkage between upper level managers' beliefs and strategic decision processes. For example, upper level manager's belief about value of change was found to influence organization strategy to be innovative (Hage and Dewar 1972), and similarly the upper level manager's belief about sales and profit was found to explain the success of manufacturing firms in the same industry (Narayanan and Fahey 1990). Other studies validating upper echelon theory have been published in organizational studies and strategic management literature (Carpenter, Geletkanycz and Sanders 2004; Finkelstein and Hambrick, 1996; Jackson 1992). The theory has also been found to be applicable across different types of organizations, including US and multi-national organizations, thus influence the level of support that TMT provides to organizational initiatives through their actions. The primary rationale used to explain the influence of TMT on organizational outcomes is that upper level managers are empowered to take decisions which have repercussions throughout the organization (Hambrick et al. 1984).

The influence of TMT on security initiatives, or the lack thereof, has not been reported in literature, nor is there direct evidence of the influence of TMT beliefs on the security-related beliefs or actions of employees.

Influences of Security Initiatives

Security compliance at a behavioral level can be enhanced by using a variety of organizational initiatives, which operate well in different time frames (Ramachandran et al, 2013, forthcoming). Mandatory initiatives aim to effect compliance in the immediate time frame. In reality, the reported success of mandatory initiatives is mixed (Boss et al, 2009; Smith et al, 2010). Education, training and awareness operate in the medium time frame. Once again, the reported efficacy of the medium term initiatives is not uniform across studies. The longer term initiative is the development of security culture. In general, the development of culture seeks to more deeply ingrain beliefs and behaviors, a process which takes place over a period of time.

While there are many factors that may influence the cultural beliefs and behaviors, the short- and medium-term security initiatives also contribute to the development of culture. The initiatives can achieve this in one or both of two ways. First, the existence of written security policies and guidelines (Wood, 2000), regular security audits and check lists (Watne and Turney, 1990) and so on are symbolic of the importance of security to the organizations. Further, regular compliance with short-term initiatives makes the processes a routine part of the work-day, and over time the behavior patterns are culturally ingrained into the organizational group members. Thus, security initiatives can contribute to the security culture of organizations.

Summary

The literature survey addresses several major themes that are relevant to the purpose of the current study i.e. to develop a theory of security subcultures in organizations: culture, security and performance pressure, TMT influences, and, the effect of security initiatives on security culture. The theme on culture begins with the conceptualization of culture in diverse studies. Then the literature on organizational culture is reviewed to highlight two issues. First, organizational culture may be viewed as a collection of professional subcultures. Correspondingly, security culture in an organization may also be a collection of security subcultures. Second, organizational culture includes both cultural beliefs and cultural behavior, and that there may be conflicts between the two. The theme on security and performance pressure draws upon two bodies of literature, the safety culture literature and the security literature to highlight the existence of conflicts between the demands of security and performance. The theme of TMT influences draws upon the Upper Echelon Theory to highlight their influence on organizational outcomes including culture. Lastly, the possible connections between security initiatives and security cultures are briefly touched upon.

The Conceptual Framework

The purpose of the current article is to develop a conceptual framework of security subcultures of professional groups in organizations. In this section, we focus on three issues. First, the approach taken to develop conceptual framework is articulated. Second, the key terms used in the framework are explained. Third, the two assumptions or premises underlying the framework are stated. Fourth, the level of analysis of the research is stated. Lastly, the framework is developed, link by link. The theoretical and/or empirical underpinnings of each relationship are discussed.

Paths to Developing Conceptual Frameworks

Two paths have generally be been recommended for the development of conceptual / theoretical frameworks or models. (Miles and Huberman, 1994; Anderson and Aydin, 1994). They are:

i) Using an existing theory or borrowing theories from other fields and complementing them with logic to develop a *conceptual framework*

ii) Gathering data without being constrained by prior theory from the native field or from other fields, and, letting the theory evolve from the data.

The first approach is referred to as a structured approach and the second as an unstructured approach (Miles and Huberman, 1994). They point out that while the unstructured approach sounds ideologically more appropriate, it is difficult for the researcher to execute in the field. All information will seem equally important, making it difficult for the researcher to stay focused on the pertinent issues. For this reason, Miles and Huberman (1994) suggest a combination approach to building theory, one which uses both the structured and unstructured methods, but favoring the structured.

In the combination approach, researchers start with a *conceptual framework,* built from existing theoretical and empirical knowledge and logic. A *conceptual framework* explains in either a pictorial or a narrative way "..the main things to be studied – the key factors, constructs or variables - and the presumed relationships among them" (Miles et al. 1994, pp.18). The *conceptual framework* is meant to help the researcher to selectively choose the concepts that the researcher deems to be important initially, and, the relationships between the concepts that the researcher finds meaningful. The scope of the current research is limited to developing the framework.

The next step in the combination approach involves the gathering of qualitative data. The structured part of the data collection process is guided by the initial set of questions suggested by the conceptual framework. The unstructured part of the data collection process includes other questions that arise during data gathering. The unstructured part of data collection will provide the flexibility for the researcher to unearth new concepts and relationships not initially identified in the *conceptual framework.* During the data analysis phase, the conceptual framework suggests the initial codes for analyzing the data. Additional codes can be developed as suggested by the data. Analysis of the data leads to the theoretical model of interest. We reiterate that the current article does not address the data gathering and analysis step.

Other researchers have also suggested the use of the combination of structured and unstructured methods to develop a theoretical model (e.g., Anderson and Aydin, 1994). Examples of studies that have used the combined approach are Pare (1995), who used the method for his dissertation, and, Lapointe and Rivard (2005) in their study of IT implementation.

In the current article, we report the development of a conceptual framework for the information security subcultures of professional groups in organizations.

Definitions and Conceptualizations

The concepts used in the study are clarified in the current sub-section. They include: productivity and performance, top management team (TMT) beliefs, managerial security initiatives, managerial productivity initiatives, performance pressure, beliefs related to performance pressure, beliefs among the larger professional groups, espoused security subcultures, and enacted security subculture.

- *Productivity and performance:* Productivity and performance are closely related terms. Broadly, productivity is the yield per unit resource expended. Performance refers to the quality of execution of tasks, e.g., an employee's performance is good. Performance can also be stated in quantitative terms, e.g., an employee produced ten units of product in a day. This quantitative statement of performance can also be referred to as the employee's productivity. This logical sequence reflects the overlap in the usage between the two terms. In discussions of culture, a productive culture (or a performance oriented culture) would include beliefs about productivity measures at all levels, i.e., the number of customer calls answered by a customer service agent, the number of units produced by a production line worker, the resources expended by a project manager in completing a project etc: would all be indicative of a culture of productivity. In the current study, the terms productivity and performance are used in a qualitative sense to reflect the general organizational expectation of employees and management to be productive and to perform efficiently and effectively.
- *TMT beliefs about the relative importance of security and productivity:* Top management team refers to the dominant coalition in an organization which decides on organizational strategies and high level budget allocations. TMT beliefs about the relative importance of security and productivity refers to their beliefs about security and their beliefs about productivity considered independently, and also considered in conjunction, particularly in times when there is a shortage of resources to meet all the desired goals.
- *Managerial security initiatives:* Managerial security initiatives refer to steps taken to improve information security in the organization. They include:
    - the development of policies, guidelines, and procedures that employees are required to follow with respect to security.
    - training programs and other initiatives supported by management. They include

        - programs to increase security awareness of employees – the existence of threats and vulnerabilities, and,
        - programs to educate on ways to avoid security pitfalls
    - reward or penalty structures in place to encourage and ensure information security.
- *Managerial productivity initiatives:* Managerial productivity initiatives refer to steps taken to improve employee productivity in the organization. The initiatives parallel the initiatives to improve security. They include the development of policies, guidelines, and procedures that employees need to follow with respect to productivity. It also includes training programs supported by management to enhance the level of productivity of employees. Lastly, it includes any reward or penalty structures in place to encourage and ensure productivity of employees.
- *Performance Pressure:* Performance pressure is the stress and anxiety experienced by employees when they are driven to get work done in a limited period or to get work done with limited resource availability or to work on a project with non-specific goals. Such pressures are experienced when employees are expected to complete tasks with insufficient resources. It is also possible that employees self-induce such pressure by placing high expectations of themselves.
- *Beliefs related to performance pressures:* Beliefs related to performance pressure refer to the beliefs of employees regarding the existence of unreasonable expectations to complete tasks without sufficient resources. Beliefs related to performance pressure is represented through a cluster of related beliefs, including the group's beliefs about risk taking, beliefs about taking short cuts, and beliefs about role overload.
- *Beliefs among the professional groups (external to the target organization):* This refers to beliefs among the members belonging to a profession, but working in diverse organizations, i.e., the beliefs harbored by members of the profession transcending across organizations. In the context of the present study, security related beliefs of the larger professional groups are considered.
- *Espoused security subcultures:* Espoused security subculture is defined as the totality of security-related beliefs of members of professional groups in organizations that contribute to the protection of all kinds of information in a given organization. Espoused culture is conceptualized by the Bath Consultancy Group as represented through the stated beliefs and values, which the group claims to profess (Hawkins 1997). In the current study, espoused security subculture of professional groups within organizations is conceptualized to represent the security-related beliefs professed by the group.
- *Enacted security subcultures:* Enacted security subculture of professional groups is defined as the totality of security-related behaviors of members of professional groups in organizations that contributes to the protection of all kinds of information in a given organization. Enacted culture is conceptualized by the Bath Consultancy Group as representing the lived culture that is externally noticed, and represents the culture that is reflected as actual actions (Hawkins 1997). In the current study, enacted security subculture of professional groups within organizations is conceptualized to represent the actual, externally noticeable, security-related behavior of members of the group. The set of security-related behaviors discussed in the current study include those sets of actions on which employees have total control, (i.e., can decide whether to perform or not), and have the potential to create security concerns.

Premises of the Conceptual Framework

The current study is built on two premises. First, organizational culture is not a monolithic construct, but comprises a collection of subcultures in the organization. Second, cultural beliefs may be different from cultural behaviors. Support for each premise from literature is provided.

Some studies of organizational culture have treated it as a monolithic construct (Pettigrew 1976; Rosen 1985; Schein 1985; Smircich 1983b; Stablein and Nord 1985) but other studies have argued that cultures within organizations are not monolithic, but exists as a collection of subcultures (Boisnier et al. 2002; Jermier et al. 1991; Martin 1992; Martin et al. 1983). Subcultures within organizations may form around professional groups or functional departments or task types (Trice 1993b). The subcultures may complement each other or conflict with each other, but in either case, they exist within an overarching culture (Martin et al. 1983). In the context of security culture, it may be argued that security culture among employees in organizations may vary across the diverse professional groups in the organization. Thus, the current dissertation assumes that each of the professional groups within organizations may have their own security subculture, which may be different from each other. The aggregation of these subcultures constitutes the security culture of the organization.

> *Premise 1: Security subcultures of different professional groups within an organization may be different from each other.*

Schein (1985) argues that culture within organizations exists at three levels: assumptions, values and artifacts. Assumptions, which form the core of any culture, represent the taken for granted beliefs about reality with the organization and are hard to identify and measure. Values in organizations include the social principles, philosophies, beliefs, goals and norms of the members. Artifacts represent the tangible and most visible part of the culture, which include the behaviors, actions and the visible structures within the organization acting as a showcase of culture of the organization. In the current study, cultural beliefs and cultural actions are of interest.

Security cultures in organizations may be identified in several ways. One, security culture can be elicited by observing visible artifacts, such as managerial security initiatives. Such initiatives may include security policies, security training programs, security awareness programs and so on. Two, security culture may be identified by documenting and analyzing the security-related behaviors of employees, which also represents the artifacts of the culture. Both managerial security initiatives and the security-related behaviors of employees could be mapped to the artifacts level of culture in Schein's model (1985). Three, security culture may be identified by eliciting the security-related beliefs of employees. Security-related beliefs of employees could be mapped to values level of culture in Schein's model (1985). It is possible that the security cultures identified through the three ways are consistent with each other, but contradictions are also possible. Traditionally, researchers assess culture in organizations by focusing on one level of the culture, either at the level of beliefs, or, at the level of artifacts. They rarely assess cultures using a multi-level approach. This limits their ability to assess differences between cultural beliefs and actions. In the context of security subcultures of various professional groups within organizations, we argue that security subculture elicited through the beliefs may be different from the security subculture elicited through their behaviors. In professing beliefs about security, members of various professional groups within organizations are not likely to favor risky behaviors or violations of accepted secure practices. However, their actions in the real world may be guided by more than their security beliefs and organizational security considerations e.g., actions in organizations have to take into consideration efficiency and productivity needs, which may lead to violations of recommended security procedures, and thus compromising security. Hence, we argue that under certain conditions, espoused security subcultures (security beliefs) of various professional groups within organizations may be different from their enacted security subculture (security behaviors). Martin (1992) refers to this as action inconsistency. “Action inconsistency occurs when an espoused content theme is seen as inconsistent with actual practices” (Martin 1992, p.85).

> *Premise 2: Enacted security subculture of various professional groups within organizations may be different from their espoused security subcultures.*

Level of Analysis

Culture as represents the set of shared and evolved assumptions, beliefs, norms and behaviors about a particular phenomenon among a collection of individuals (Hofstede, 1980; Schein, 1985). In studies of organizational culture, this collection of individuals may include all members of the organization, or subsets of members of organizations. In the current study, the focus in on the security related beliefs and behaviors of various professional groups within organizations. Thus, the level of analysis is at the group (professional) level. As mentioned earlier, it is possible that security culture varies across professional groups in an organization. Also, security related beliefs and behaviors can be explored at the individual level of employees. The choice of group level in preference to the individual level for the level of study is guided by the following logic. The identification of differences in security beliefs and behaviors across professional groups in organizations will enable the customization of organizational initiatives to improve culture by professional groups. Organizational initiatives are rarely customized at the individual level. Hence, it was considered more appropriate to focus the study at a group level.

Conceptual Framework Development

In the current section, the conceptual framework is developed. In particular, theoretical and empirical support is provided for the relationships proposed in the framework. The development of the conceptual framework is done as follows. First, the factors influencing the enacted security subculture of professional groups in organizations are discussed. The factors are espoused security culture, managerial security initiatives, the moderating influence of performance pressures. Second, factors affecting the espoused security subculture are discussed. These include security beliefs originating in the professional association of the group, the security beliefs of IS professional group in the organization, managerial security initiatives, and the direct and indirect effects of TMT beliefs about security. Lastly, the factors influencing group’s beliefs about performance pressures are discussed. These factors include the direct and indirect effects of TMT's beliefs about the relative importance of security and productivity/performance on group's beliefs about performance pressure.

Factors Influencing Enacted Security Subculture of Professional Groups in Organizations

The intent of the current section is to discuss the factors influencing enacted security subculture of professional groups within organizations. In the following subsection enacted security subculture of professional groups is briefly discussed, followed which various factors influencing enacted security subculture are discussed.

Enacted Security Subcultures: For the purpose of this research, enacted security subculture of professional groups is conceptualized as the actual, security-related behaviors of members of the group (Hawkins 1997). Security oriented behaviors include those sets of actions, which have the potential to create security concerns, and on which employees in the organization have total control, i.e., the employees can decide whether to perform or not. A hypothetical example of an action that employees have total control over may be as follows. An organization may have written security policies forbidding the use of external storage devices for storage and transfer of corporate data. Even after the above policies are set in place, employees in the organization may use external storage devices like flash drives and pen drives as a part of their work within the organization, thus creating security vulnerabilities. An example of an action that the employee is not able to control is as follows. Most organizations require passwords to be changed periodically. At the end of the specified period, the system will prompt a user to change the password. The user has no choice but to comply. The user will not be able to use his/her computer if he/she does not comply. Enacted security subculture of various professional groups within organizations is the primary dependent variable in the framework.

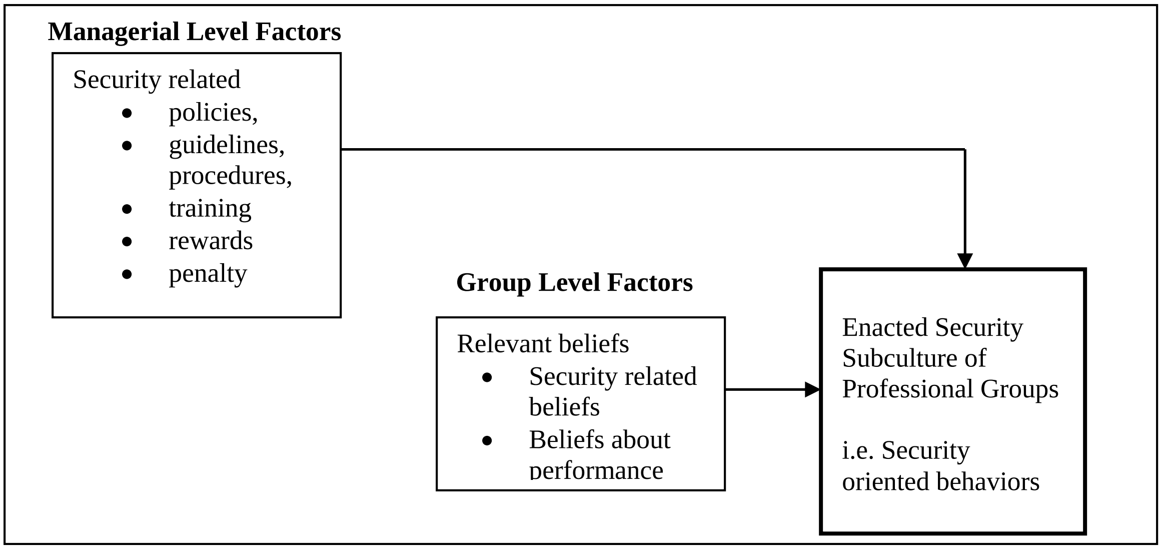


Figure 2. Factors Influencing Enacted Security Subculture of Professional Groups

Antecedent Categories of Enacted Security Subcultures of Professional Groups: Two categories of factors (group level factors and managerial level factors) are argued to influence the enacted security subcultures of various professional groups in an organization. Group level factors represent the relevant belief structures of the target professional group in the organization. The belief structures include the group's security related beliefs, and group's beliefs related to performance pressure. The managerial level factor is the set of managerial security initiatives that emphasize and enhance information security through appropriate employee behaviors. Managerial security initiatives include security related policies, guidelines, procedures, security training programs, rewards, and penalty structure. Figure 2 shows the group and managerial level factors that influence enacted security subculture of professional groups. The theoretical rationale to support the influence of group level factors and managerial level factors is explained next.

Theoretical Rationale for the Influence of Group Level Factors (*Relevant Belief Structures of the Group)* on Enacted Security Subcultures: Group level factors include the group's security related beliefs (espoused security subculture) and the group's beliefs related to performance pressure. Detailed discussion of each factors and theoretical support for the influences are provided in the following subsections.

Influence of Espoused Security Subcultures of Professional Groups i.e. Security Related Beliefs of Group: **E**spoused security subculture of professional groups is conceptualized as the culture represented by the professed security related beliefs and values of the group (Hawkins 1997). Some of the primary security related beliefs of the various professional groups include beliefs about importance of security within organization, beliefs about the security risk exposure of the organization, beliefs about security preparedness of the organization, beliefs about who is responsible about security within the organization, beliefs about the role played by them to improve the security posture of the organization, beliefs about risk taking and so on. In addition to the above set of beliefs, other beliefs could be considered as secondary set of security related beliefs. These include beliefs about rules and procedures in the organization, beliefs about hierarchy, beliefs about the importance of being accountable for their own actions, and so on.

The relationship between beliefs and behaviors has been argued at both the group and individual levels of analysis. At the group level, Schein's three-layer model of culture argues that the cultural artifacts can be driven by the cultural values which in turn can be driven by cultural assumptions (Schein, 1985). Both cultural values and cultural assumptions include cultural beliefs as components. Thus, cultural beliefs (espoused culture) can be seen to drive cultural behavior (enacted culture), and by analogy, espoused security subculture can be argued to drive enacated security subculture.

At the individual level, the theory of reasoned action (TRA) (Fishbein and Ajzen 1975) and the Theory of planned behavior (TPB) (Ajzen 1985) explain the factors influencing individual behaviors. The TRA model posits that the most important determinant of an individual's behavior is his/her behavioral intention. Individual's behavior intention towards a particular behavior is influenced by the attitude towards performing the act, and, subjective norm of others (including peers). The attitude, in turn, is derived from beliefs about the outcome of the behavior, and the desirability of the outcome (Fishbein et al. 1975). Similarly, subjective norms are derived from the normative beliefs about the behavioral expectations of important referent groups (Ajzen 1985). Thus, normative beliefs of the referent group and the outcome beliefs of the behaviors influence actual behaviors.

The theory of planned behavior (TPB) extends TRA to situations, in which the individual does not have total control over the behavior. In TPB, the concept of perceived behavioral control is introduced. This in turn is derived from control beliefs. In effect, a collection of beliefs – normative, outcome and control beliefs – influence behaviors. In the current instance, normative beliefs of the referent group parallel espoused (sub)culture, and behaviors parallel enacted (sub)culture, the relationships between normative beliefs and behavior can be used as a basis to argue the relationship between espouse security subculture and enacted security subculture.

In sum, theories both at the group and individual level argue that beliefs can influence behaviors, supporting the link in the framework between espoused security subculture and enacted security subculture.

Influence of Beliefs Related to Performance Pressure on Enacted Security Subculture: We also argue that the group's beliefs related to performance pressure will moderate the influence of the group's beliefs to security on the group's enacted security subculture. The theoretical basis for the moderating influence is drawn from research in the safety culture literature. The parallels between safety and security has been argued by others (Brostoff et al. 2001; Sasse et al. 2001), and discussed earlier. In brief, neither safety nor security is the ultimate goal of an organization; productivity and profits are the ultimate goals. Safety contributes to the safeguarding of physical and human assets, while security contributes to the safe-guarding of information assets, and thus both "enable" long-term productivity of the organization. However, in the short-term, safety or security measures can get in the way of production tasks (Sasse et al. 2001).

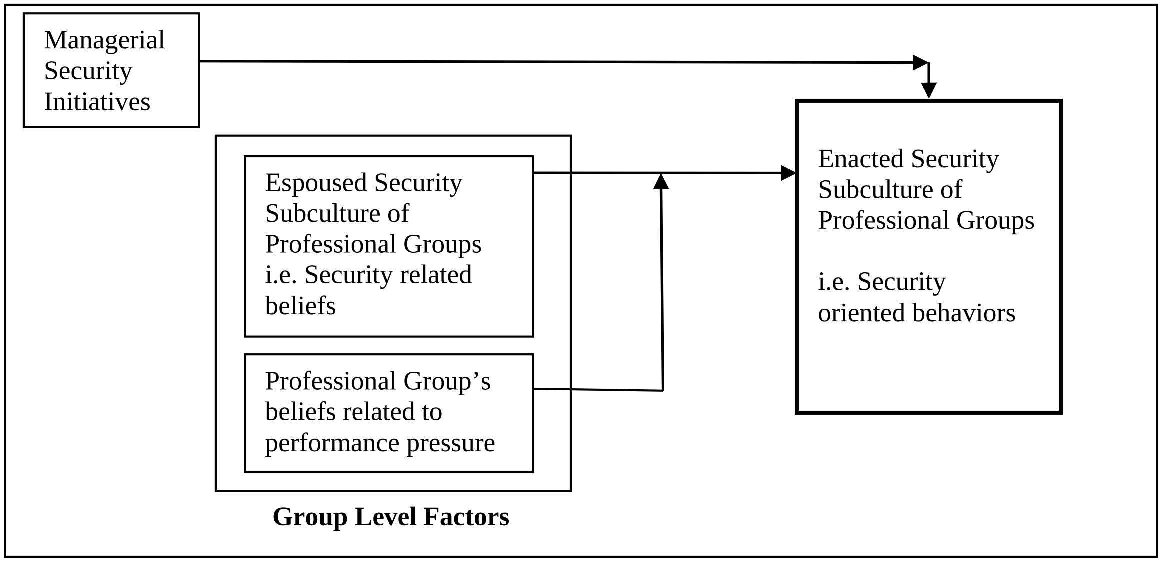

Managerial Security Initiatives
Espoused Security Subculture of Professional Groups i.e. Security related beliefs
Professional Group's beliefs related to performance pressure
Enacted Security Subculture of Professional Groups
i.e. Security oriented behaviors
Group Level Factors

Fig. 3. Group Level Factors Influencing Enacted Security Subculture of Professional Groups

Safety culture literature (Dawson et al. 1988; Embrey 1992; Klen 1988; Wright 1986) argues that in addition to the direct influence from safety related beliefs of employees, safety performance of the employees will also be influenced by their beliefs related to performance pressure. Beliefs related to performance pressure is represented through a cluster of related beliefs, including the group's beliefs about risk taking, beliefs about taking short cuts, and beliefs about role overload.

According to safety culture literature (Dawson et al. 1988; Embrey 1992; Klen 1988; Wright 1986), when performance pressure is low, safety behavior will be consistent with safety beliefs; when performance pressure is high, safety behaviors may be inconsistent with safety beliefs. An analogous argument is made for the relationship between security behaviors (enacted security culture) and security beliefs (espoused security beliefs).

Figure 3 details the group level factors influencing enacted security subculture of professional groups within organizations, i.e. the group's security related behaviors.

Managerial Level Factors and their Influences on Enacted Security Subcultures*:* Managerial security initiatives, such as security-related policies, guidelines, procedures, training programs, reward structures and penalty structures, are reflective of managerial emphasis on information security. Such emphasis is expected to influence security-related behaviors of employee groups. Each of the managerial initiatives is briefly discussed before the empirical and theoretical support is provided to support the proposition linking managerial security initiatives to enacted security culture.

- *Security Policies*: Security policies of organizations act as a statement of the organization's beliefs, goals and objectives about protection of information assets within the organization (Peltier 2002). Security policies are generally high level statements without clear definition of steps to achieve the security objectives. Peltier indicates that policy statements may be informal or formal, and, they may be generic or topic specific. Informal security policies are often passed around employees by word of mouth (Bishop 2005; Peltier 2002). Formal written security policies provide the organizations with control over the security related goals and objectives, and also act as a mechanism through which management's commitment to security is conveyed to the employees. General policies represent the overall information security vision of the organization; in contrast; topic specific policies address specific information security concerns identified within the organization and lastly, application specific policies focus on particular application or systems germane to the organization. International Standards Organization (ISO) has adopted a standard, ISO 17799, for information security in December 2000, which has identified a number of policies which every organization should consider. Some of the security policies which we come across normally in organizations include internet usage policy, email policy, information classification policy, information access policy, media handling policy, and, so on.

  Even though security policies play a major role in defining the management's vision and objective about security within the organization, effectiveness of security policies depend upon appropriate standards, procedures, training programs, reward/penalty structures and security controls implemented by the organization.

- *Guidelines:* Peltier (2002) defines guidelines as statements that reflect how to achieve security policies (Peltier 2002). For example, if an organization's information access policy states that the organization restricts access of information to authorized users only, then the organization should have corresponding guidelines stating what steps should be taken to ensure only authorized users have access to information assets within organization. Another example of an appropriate guideline would be one which details the acceptable length of passwords and the combinations allowed in it. Literature also indicates that some organizations don't have written security related guidelines, and, in some of the organizations which do have guidelines, the guidelines don't mesh with the security policies set in place (Bishop 2005; Peltier 2002).

- *Procedures:* Security related procedures within organization, detail the steps to be taken to implement policies and guidelines (Peltier 2002). For example, in order to implement the policy relating to information access restriction, an organization may have set procedures that employees have to follow in case they forget their passwords.

- *Training Programs:* The effectiveness of policies, guidelines and procedures are improved when employees are aware of them, and follow them competently. Security related training programs can be used to achieve several goals. First, they can increase employee awareness of the security risks that the organization is exposed to, and the employees' role in reducing the risks. Second, they can increase the employee awareness of the security policies, guidelines and procedures in place in the organization. Lastly, they can train employees to competently follow security procedures of the organization. Thus, security training programs like online training modules or personal training programs created and established by organizations, help in the transformation of organization's visions about security into reality.

- *Reward/Penalty Structures for security-related behaviors:* In addition to security related training programs, organizations may also rely on reward and penalty structures as a part of their carrot-and-stick logic to influence the security oriented behaviors of employees. Penalties seem to be the norm to control security-related behaviors, and, range from simple verbal reprimands to termination of employment. In safety literature, safety awards and other rewards are reported; similar reward systems, while possible, have not been reported in the security literature.

The empirical and theoretical support for the relationship between managerial security initiatives and enacted security culture are discussed next.

Influence of managerial safety initiatives on safety performance has recently been given some attention in the security literature and has been extensively examined in the safety culture/safety climate literature[1]. In the security literature, Stanton and his associates (Marcinkowski and Stanton 2003; Stanton et al. 2005) reviewed extant security policies in organizations and found that managerial security initiatives like rewards, incentives and penalties have a motivational impact on the security behaviors of employees in organizations. In a recent review of safety culture/safety climate literature, Flin et al (2000) identified 18 instruments of safety climate used among the safety culture/safety climate studies. Based on a thematic analysis of the 18 scales used to assess safety climate, Flin et al (2000) found that 72% of scales assessed safety climate

[1] Denison, D.R. "What is the Difference Between Organizational Culture and Organizational Climate? A Native's Point of View on a Decade of Paradigm Wars," *Academy of Management Review* (21:3) 1996, pp 619-654. analyses the distinctions between culture and climate and ends by stating "culture and climate literatures actually address a common phenomenon." The focus in this study is on culture, but climate literature is incorporated when appropriate.

through the dimension of role of management. Other dimensions identified by Flin et al (2000) include work pressure, risk and safety of the system. Guldenmund (2000) and Yule (2003) also note that the role of managerial initiatives is the often measured construct in safety culture/safety climate literature. Based on a review of 20 years of safety culture and safety climate literature, Guldenmund (2000) proposes an integrative framework to merge the two constructs of safety culture and safety climate. As a part of his analysis, Guldenmund (2000) notes that the role of supervisors (aka management) has been the most frequently measured dimension. Along similar lines, Yule (2003) reviews safety culture and safety climate studies. Based on his analysis, Yule (2003) points out that even though there is a lack of consensus among safety culture and safety climate researchers on the issues of factors that should be used to assess safety culture and safety climate, they still agree on the importance of assessing the role of management due to its strong association with safety outcomes.

Zohar (1980) was the first to argue for support from management, in terms of managerial initiatives, as a definite prerequisite of successful initiatives aimed to improve safety outcomes within organizations. Strong support for Zohar's (1980) argument about the influence of managerial initiatives emphasizing safety on safety outcomes has been found in the safety culture/safety climate literature (Diaz and Cabrera 1997; Donald and Canter 1994). Management's emphasis on safety was generally represented in safety culture literature through managerial initiatives like policies, procedures, training programs and reward systems. More recently, an extensive review of safety culture and safety climate literature by Yule (2003) reveals a strong degree of association between managerial factors and safety outcomes. Drawing a parallel from the relationship between managerial safety initiatives and safety behavior of employees, security oriented behavior of professional groups within organization could be argued to be influenced by managerial security initiatives.

The theoretical basis for the influence of managerial security initiatives on enacted security culture is drawn from Self determination theory (SDT) research by Ryan and Deci (2000). Self determination theory examines the factors that enhance or undermine self-determined motivation, which includes both intrinsic and extrinsic motivation (Ryan et al. 2000). Extrinsic motivation is defined in SDT as the motivation to perform a task in order to achieve external approval or reward, and, involves compliance with external regulation. Intrinsic motivation is defined in SDT as the motivation to perform a task in order to achieve internal satisfaction and involves personal choice (Ryan et al. 2000). Self Determination Theory (Ryan et al. 2000) posits that extrinsic motivation exists in different forms and there can be different contextual factors that can either hinder or promote regulation needed for externally motivated behaviors. According to Self-Determination Theory, policies, procedures, guidelines, rewards and punishments set in place by the management act as relevant regulatory processes set to enforce compliance by the employees, and, thus externally motivate employee's behavior. Self-determination theory has been put forth at the individual level. An individual level theory may be applied to group levels if a similar or common response is expected by all members of the group, as is usually expected in studies of culture (Klein, Dansereau and Hall 1994). Thus, we apply self-determination theory to argue that managerial security initiatives are external regulatory factors, which motivate the security oriented behaviors of professional groups within organizations i.e. their enacted security subculture.

Summary of Factors Affecting Enacted Security Culture: In summary, enacted security subculture of professional groups within organizations i.e. their security oriented behaviors could be influenced by group level factors like the group's beliefs structures, and managerial level factors. The group level belief structure about security (i.e., security-related beliefs or espoused security culture) is expected to affect enacted security culture directly. The relationship between espoused security culture and enacted security culture is expected to be moderated by the group's beliefs with respect to performance pressures. Managerial level factor includes managerial security initiatives like polices, guidelines, procedures, training programs and reward/penalty structures and is expected to influence enacted security culture directly. Figure 4 provides a visual representation of the factors influencing enacted security subculture of professional groups in organizations.

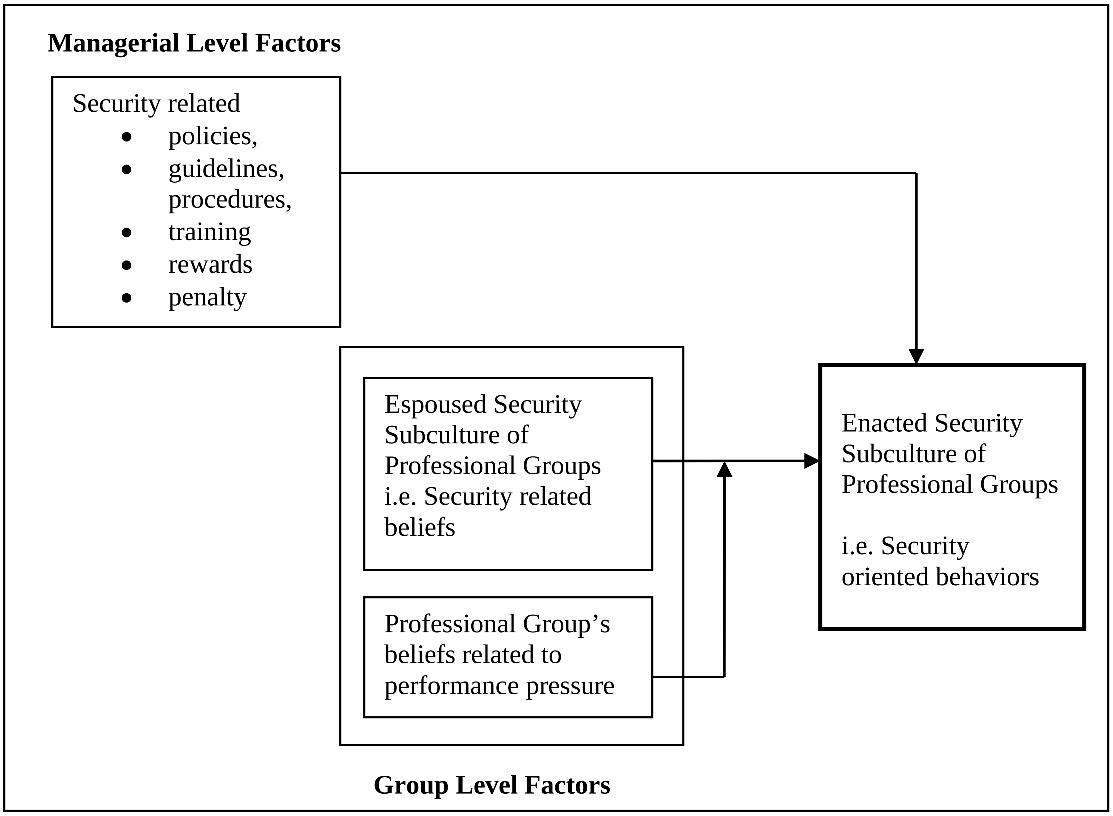

Managerial Level Factors
Security related
• policies,
• guidelines, procedures,
• training
• rewards
• penalty
Espoused Security Subculture of Professional Groups i.e. Security related beliefs
Professional Group's beliefs related to performance pressure
Enacted Security Subculture of Professional Groups
i.e. Security oriented behaviors
Group Level Factors

Fig. 4. Factors Influencing Enacted Security Subculture of Professional Groups

Factors Influencing Espoused Security Subcultures of Professional Groups in Organizations

Espoused security subculture represents the security culture that the professional group professes to have. It is argued in the current research that espoused security subculture of professional groups within organizations are influenced by two sets of factors: factors internal to the organization and factors external to the organization. Factors internal to the organization that influence espoused security subculture of professional groups include managerial security initiatives, TMT beliefs, and, security related beliefs of other relevant professional groups within the organization like Information Systems (IS) professional group. Factors external to the organization that may influence the security related beliefs of the group may be the security related beliefs held by members of the profession that the group belongs to. Figure 5 provides a visual representation of the factors that influences the espoused security subculture of professional groups within organization i.e. the group's security related beliefs.

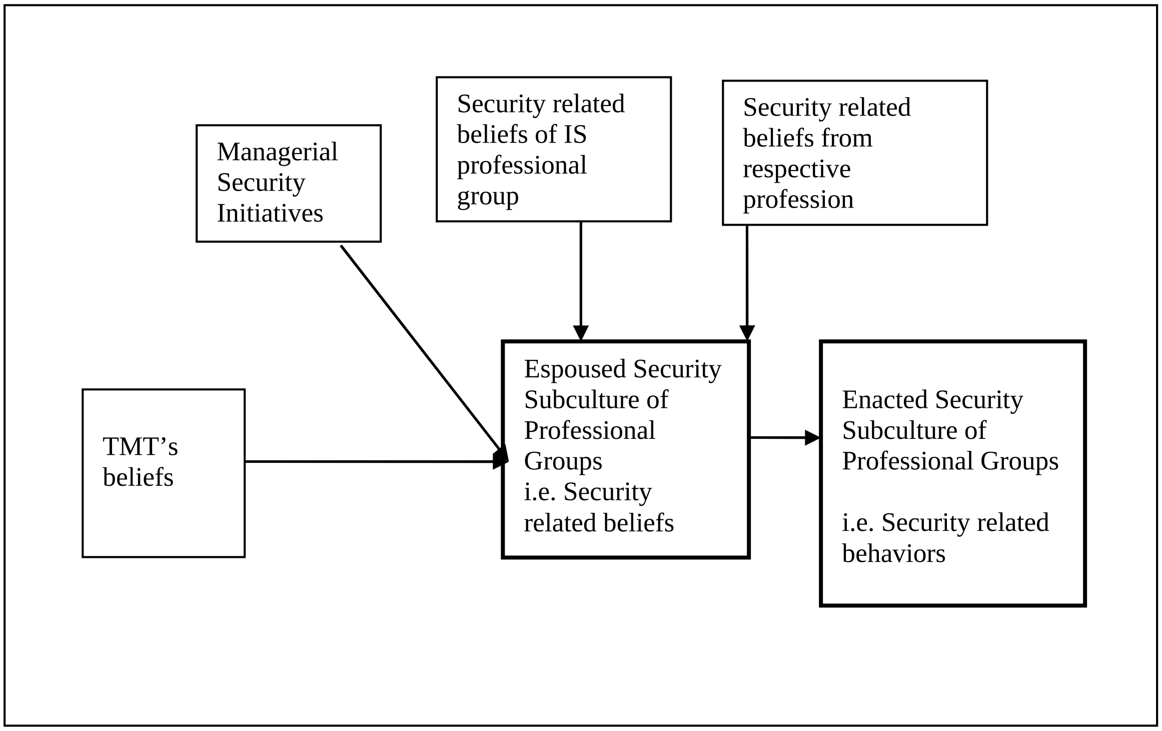

Managerial Security Initiatives
Security related beliefs of IS professional group
Security related beliefs from respective profession
TMT's beliefs
Espoused Security Subculture of Professional Groups i.e. Security related beliefs
Enacted Security Subculture of Professional Groups
i.e. Security related behaviors

Fig. 5. Factors Influencing Espoused Security Subculture of Professional Groups within Organizations

Internal Factors and their Influences on Espoused Security Subcultures: The internal issues being considered are security initiatives, TMT beliefs about security and performance and the influence of the information systems department.

Influences of Managerial Security Initiatives on Espoused Security Culture: Managerial security initiatives, such as training programs, policies, guidelines, procedures, reward structures, and penalty structures are expected to influence the espoused security subculture (security-related beliefs) of professional groups in organizations. Theoretical basis for such an influence is drawn from IS literature. Several researchers (e.g., Leonard-Barton and Deschamps (1988), Purvis et al (2001), and Sharma and Yetton (2003)), have examined the influence of management initiatives on success of IS efforts within organizations. They have shown that management initiatives play a symbolic role in conveying the support of the management for a cause, such as an IS project, and, could influence the employee's beliefs about the project under consideration. Analogously, in the context of security, managerial security initiatives like security related policies, guidelines, procedures, training programs, reward structures and penalty structures could be argued to convey symbolic cues of management commitment to information security to the employee groups within organizations, and therefore influence employee beliefs about security.

Influences of TMT beliefs: TMT beliefs can influence espoused security subculture either directly or indirectly through managerial security initiatives. In the current section, the support for the relationship between TMT beliefs and managerial security initiatives, and the support for the direct relationship between TMT beliefs and espoused security, will be developed.

TMTs, also referred to as "the dominant coalition" (Cyert et al. 1963), play a very important role in the organization. TMTs identify environmental opportunities and problems, interpret relevant information, assess the capabilities of the organization, device organizational strategy and nurture the culture that would be followed across the firm (Mintzberg 1979). TMTs make decisions which will have repercussions throughout the organization, and, such decisions made by TMTs are tightly coupled to their beliefs and values (Hambrick, Cho and Chen 1996). According to Upper Echelon Theory, values and cognitive bases of powerful actors in the organization, who normally comprise the TMT, influence the strategic processes, outcomes and beliefs within the organization (Hambrick et al. 1984).

In considering TMT beliefs, two issues are of relevance. First, it is necessary to consider if any government mandated security standards are applicable to the industry. Second, it is necessary to examine the resources available for investment in productivity-related and security-related projects.

Investments in security may be mandated or discretionary. In some industries, governmental standards like HIPAA may mandate investments in information security. In this case, there may or may not be a connection between TMT beliefs and managerial security initiatives. TMT beliefs may be consistent with the mandated requirements, in which case, there will be a connection between TMT beliefs about security and managerial security initiatives. On the other hand, TMT beliefs may be at odds with mandated security requirements, in which case there will be a disconnect between TMT beliefs about security and managerial security initiatives.

In environments in which security spending is discretionary, two situations are possible, i.e., there may be no monetary resource constraint, or, they may be resource constraints leading to competition for the available monies for different projects.

When no monetary constraint exists, TMT can invest in security initiatives according to their beliefs. Thus, TMT beliefs about security will influence managerial security initiatives. When monetary constraints exist, TMTs will have to choose between competing initiatives. Some of the competition for funding will be between initiatives to improve productivity, and others will be initiatives to improve security. Thus in this situation, TMT beliefs about the relative importance of security and productivity will influence managerial security initiatives. Few organizations experience the condition of no monetary constraint. Thus, in most instances, TMT beliefs about the relative importance of productivity and security will influence managerial security initiatives. Thus, TMT beliefs about the relative importance of security and productivity can have an indirect effect on espoused security subculture of professional groups within organizations, mediated by the managerial security initiatives.

Further, upper echelon theory (Hambrick et al., 1996) argues that TMT beliefs and values will influence employee beliefs. Thus TMT beliefs about the relative importance of security and productivity will directly influence the security beliefs of the employee groups.

Influences from IS Professional Group within Organizations: In management literature, boundary spanning involves bridging gaps between two or more units within or across organizations. The bridging of gaps between the units may be for one or more purposes. Management literature considers IS departments as boundary spanning units within organizations. For instance, IS departments help bridge the gap between functional groups and vendors of information processing technologies. Their knowledge of technology allows them to play a wider role within and outside the organization, and, be a source of social influence within organizations (Pfeffer and Salancik 1978; Thompson 1967).

The protection of information inside an organization is often viewed as a function of the IS department in an organization. Thus, the IS department plays the role of a boundary spanning unit between different departments in the organization and the external units generating knowledge about information security. As stated earlier, boundary spanning units exert a social influence on the other groups in the organization. In this case, the IS department, because of its perceived knowledge about security, exerts a social influence on other groups with respect to security, i.e., the security beliefs of the IS department or the IS professional group in the organization, influences the security beliefs of the other professional groups (espoused security culture).

External Factors and its Influences on Espoused Security Subcultures: One of the external influences of belief systems of groups in organizations is the profession or the professional association that they belong to. Organizational members belonging to a profession communicate and interact with members of the same profession in other organizations. Most members of a profession are further subject to common influences trade magazines, professional journals and conferences, and continuing education initiatives. According to Trice (1993), the culture of a profession plays a significant role in the belief systems of professional groups within organizations, i.e., the culture of the profession provides an anchor for the employee's belief systems. Thus, it could be argued that the security culture of the external professional association influences the espoused security culture of the members of the corresponding profession in organizations.

Summary of Influences on Espoused Security Beliefs: In summary, espoused security subculture of professional groups within organizations i.e. the group's security related beliefs will be influenced by factors internal and external to the organization. TMT beliefs may influence espoused beliefs directly or indirectly through managerial security initiatives. IS departments may be viewed as boundary spanning units for security knowledge and thus the beliefs of IS professional group in the organization may influence the security beliefs of other professional groups in the organization. Lastly, the external professional association corresponding to the profession of the group inside the organization may also influence the security beliefs of the employee group. Fig. 6 provides a visual representation of the factors influencing espoused security subcultures of professional groups within organizations.

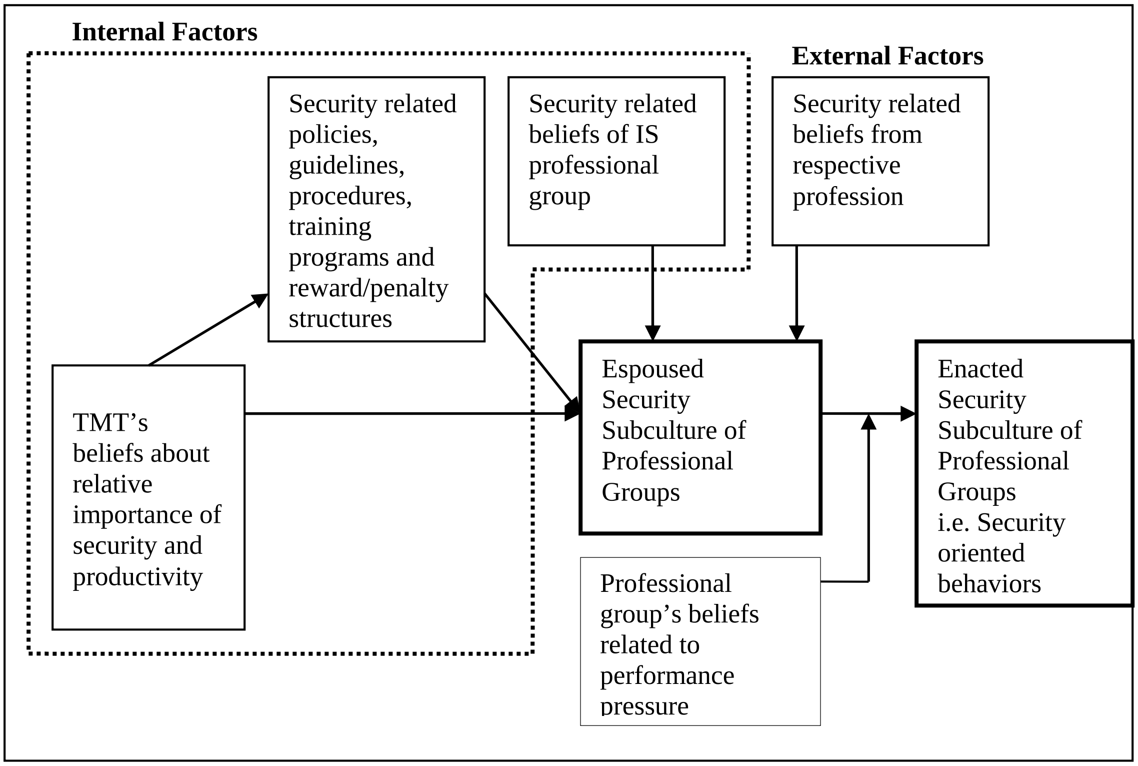

Internal Factors
External Factors
Security related policies, guidelines, procedures, training programs and reward/penalty structures
Security related beliefs of IS professional group
Security related beliefs from respective profession
TMT's beliefs about relative importance of security and productivity
Espoused Security Subculture of Professional Groups
Enacted Security Subculture of Professional Groups i.e. Security oriented behaviors
Professional group's beliefs related to performance pressure

Fig. 6. Factors Influencing Espoused Security Subculture of Professional Groups within Organizations

Factors Influencing the Professional Group's Beliefs Related to Performance Pressure

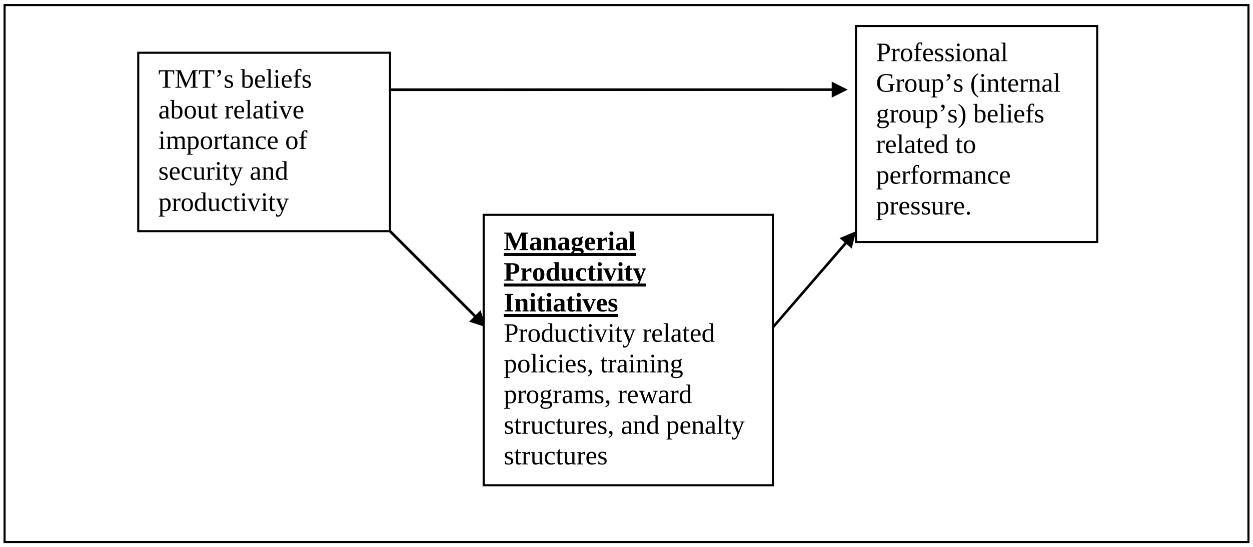
In this last section, the factors influencing the professional group's beliefs related to performance pressure are discussed. It is argued that such beliefs will be influenced by TMT beliefs, directly, and, indirectly through managerial initiatives. Again as argued by Upper Echelon Theory (Hambrick et al. 1984), TMT's beliefs about the relative importance of security and productivity within the organization will affect managerial initiatives to support productivity. It is argued that if TMT's belief is that the importance of security relative to productivity is low, then TMT will favor productivity initiatives over security initiatives. Under these conditions, they will be expending considerably more resources on supporting productivity initiatives like machinery, technology, and productivity-related training programs, than on security initiatives within the organization.

TMT's beliefs about the relative importance of security to productivity, and managerial initiatives supporting productivity, will directly influence professional group's beliefs related to performance pressure.

Theoretical bases for these influences are drawn from safety culture literature. Safety culture literature (Dawson et al. 1988; Embrey 1992; Wright 1986) argues that the professional group's beliefs related to performance pressure will be influenced by management cues of performance expectations through their beliefs and actions related to productivity. Management initiatives play a symbolic role in conveying the support of the management for a cause (Purvis et al. 2001; Sharma et al. 2003). In other words, by supporting productivity initiatives, management emphasizes performance, which creates performance pressure for employee groups within the organization.

Finally, upper echelon theory (Hambrick et al., 1996) argues that TMT beliefs and values will influence employee beliefs. Thus TMT beliefs about the relative importance of security and productivity will directly influence the beliefs that employee groups have about performance pressures in the organization.

Summary of Factors Influencing Beliefs about Performance Pressure: In summary, beliefs related to performance pressure of professional groups within organizations will be directly influenced by TMT's beliefs about the relative importance of security to productivity, and indirectly influence through productivity initiatives in the organization. Fig 7 shows the fact


TMT's beliefs about relative importance of security and productivity

Professional Group's (internal group's) beliefs related to performance pressure.

Managerial Productivity Initiatives
Productivity related policies, training programs, reward structures, and penalty structures

Fig. 7. Factors Influencing Beliefs about Performance Pressure

The Integrated Framework

The integrated framework is shown in Figure 8, which integrates all the concepts and the relationships discussed in the current section. The framework includes influences from factors internal and external to the organization. The internal factors are primarily TMT beliefs about security and productivity, managerial initiatives about security and productivity, and, IS group beliefs about information security. The primary external factor is the security-related beliefs of the professional group corresponding to the target group in the organization. The framework also distinguishes between the espoused security culture and enacted security culture of the group, and, highlights the moderating influence of the performance pressures that the group is subject to. Further, the conceptual framework focuses on the security subcultures of delineated professional groups in organizations, emphasizing the idea that security culture is likely to be differentiated in organizations across groups.

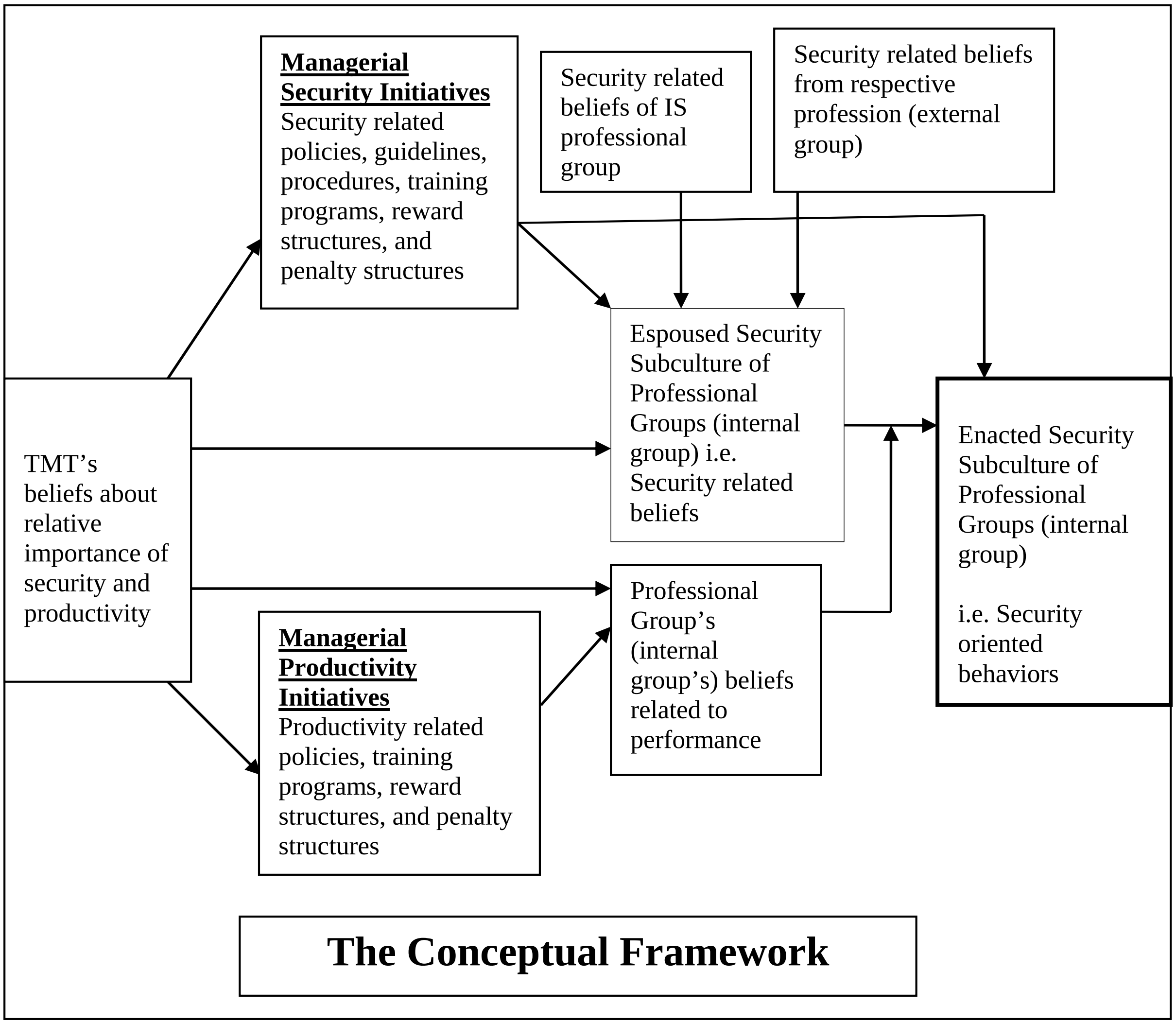

Managerial Security Initiatives
Security related policies, guidelines, procedures, training programs, reward structures, and penalty structures
Security related beliefs of IS professional group
Security related beliefs from respective profession (external group)
Espoused Security Subculture of Professional Groups (internal group) i.e. Security related beliefs
TMT's beliefs about relative importance of security and productivity
Enacted Security Subculture of Professional Groups (internal group)
i.e. Security oriented behaviors
Professional Group's (internal group's) beliefs related to performance
Managerial Productivity Initiatives
Productivity related policies, training programs, reward structures, and penalty structures
The Conceptual Framework

Fig. 8. The Conceptual Framework of Security Subcultures of Professional Groups in Organizations

Discussion

Contributions

Security culture as a means to enhancing organizational information security has been proposed for many years (e.g., Dhillon, 1995; Vroom and Von Solms, 2004). Studies of security culture focus on identifying the dimensions of security culture (Chia, Maynard and Ruighaver, 2002; Tejay and Dhillon, 2005), characterizing security cultures in organizations (…) and examining the antecedents of security culture (..). The underlying motivation for all these studies appears to be the need to find ways to strengthen security culture in organizations. The development of a conceptual framework falls within the scope of work aimed at understanding what influences security culture, as a prelude to formulating methods to enhance security culture.

Our aim is to generate a holistic view, i.e., identify all (or at least the major) antecedents. We believe a holistic view is necessary to ensure that all relevant antecedents are being taken into account when formulating and assessing initiatives to improve security culture. For instance, many studies of security culture emphasize the use of managerial initiatives, such as awareness programs and training to strengthen security culture and improve compliance. Undoubtedly, such initiatives are important. But inattention to other factors at the same time, such as performance pressure, can negate or reduce the effects of managerial initiatives. Thus, plans to strengthen security culture should be holistic or comprehensive rather than piecemeal.

A second and equally important issue is the need to accommodate the possible inconsistency between espoused and enacted security cultures. From a research perspective, it is often easier to query respondents about their beliefs than observe the behaviors of members of the target population. Observing behaviors that weaken security is even more difficult. The behaviors manifest at diverse times in diverse ways, and some behaviors leave no trace. The requirements of committees charged with ethical approval of studies complicate observing security behavior contemporaneously or gathering historical data of security behavior. Thus, there is a tendency to rely on questionnaires that address beliefs, attitudes and intents, and on theories that have showed a positive relationship between these factors and behaviors. We argue that the positive relationships have been demonstrated in the absence of conflicting behavioral demands. In the case of security, the demands for secure behaviors have to be met in the face of demands for productivity, and often the two sets of demands, are in direct conflict with each other. Our framework accounts for the possible differences in the espoused and enacted security cultures by incorporating the moderating influence of performance pressure.

Third, there is empirical evidence that security cultures of professional groups are different from each other. For instance, Ramachandran et al (2013, forthcoming) have reported variations in the security cultures of four professions: accounting, human resources, information systems and marketing. The beliefs and behaviors of a professional group in an organization are likely to be subject to both professional influence and organizational influence. Our conceptual framework takes that into account also. The primary impact of this issue is that organizations may have to emphasize different training programs for different professional groups in the organizations, and / or emphasize different issues.

In developing the conceptual framework, we have taken pains to provide strong support for the proposed relationships. We rely on both direct and indirect theoretical and empirical evidence. Behavioral research in security is at an early stage, and thus there is a greater reliance on indirect evidence, i.e., analogies are drawn from other phenomena similar to security. For instance, Sasse et al (2001) has shown that there are parallels between industrial safety and information security. We have reached out to related phenomena when appropriate to provide support for specific relationships in the framework.

Limitations and Future Research

The conceptual framework is an aerial view of the relationships affecting security subcultures. There is much that needs to be studied to help organizations achieve a high level of information security. For instance, some relationships, such as the need for training, are almost self-evident.

Implementing practical and effective training programs is a totally different issue. Similarly, identifying and acknowledging the conflicts between security and performance is only the first step. The real challenge is in formulating ways to achieve real security without compromising productivity. Thus there is a rich plethora of issues that need to be researched in helping organizations reach their quest for information security.

Conclusions

With the increasing threats to information assets of organizations, it is necessary to adopt multiple approaches to protect the assets. A significant point of weakness in the defense of organizational information is the employee, whose behaviors can leave information assets vulnerable to attack. To reduce this weakness, various remedial programs have been recommended, of which the development of a strong security culture is one. In the current article, we have developed a theory-based conceptual framework that highlights the factors which will impinge on the security subcultures of professional groups in organizations. The key issues that are worth of note are:

- The framework is based on the idea that organizational culture is differentiated in nature and must account for variations in subcultures across professions.
- The framework provides the theoretical basis for differentiating between espoused security culture and enacted security culture.
- The framework accounts for the conflict that usually exists between the need for security and the need for productivity.

Empirical validation of the framework is recommended prior to its use to strengthen the security subcultures in organizations.

Acknowledgements

Summer funding from the Dean of the College of Business at the University of Texas at San Antonio in support of the first author’s participation in this research is acknowledged.

References

Adams, A., and Sasse, M.A. "Users are not the Enemy," *Communications of the ACM* (42:12) 1999.

Ajzen, I. "From Intentions to Actions: A Theory of Planned Behavior," in: *Action-control: From cognition to behavior* J. Kuhl and J. Beckman (eds.), Springer, Heidelberg, Germany, 1985, pp. 11- 39.

Anderson, J.G., and Aydin, C.E. "Overview: Theoretical Perspectives and Methodologies for the Evaluation of Health Care Information Systems," in: *Evaluating Health Care Information Systems, Methods and Applications*, J. Anderson, G., E.A. Carlyn and J.J. Stephen (eds.), SAGE Publications, Thousand Oaks, CA, 1994, pp. 5-29.

Arboleda, A., Morrow, P.C., Crum, M.R., and Shelley II, M.C. "Management Practices as Antecedents of Safety Culture within the Trucking Industry: Similarities and Differences by Hierarchical Level," *Journal of Safety Research* (34) 2003, pp 189-197.

Austin, R.D., and Darby, C.A.R. "The Myth of Secure Computing," *Harvard Business Review* (81 6) 2003, pp 120-126.

Bahn, D.L. "System Designer-User Interaction: An Occupational Subcultures Perspective," SIG-CPR, 1995.

Besnard, D., and Arief, B. "Computer Security Impaired by Legal Users," *Journal of Computer and Security*) 2003.

Bishop, M. *Introduction to Computer Security* Addison Wesley, Boston, MA, 2005.

Boisnier, A., and Chatman, J.A. "Cultures and Subcultures in Dynamic Organizations," in: *The Dynamic Organization,* R. Peterson, and Mannix, E. (ed.), Lawrence Erlbaum Associates, Mahwah, NJ, 2002, pp. 87-114.

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, pp. 151-164.

Bollas *The shadow of the object: Psychoanalysis of the unthought known* Free Association Books, London, 1987.

Brooks, I. "For Whom the Bell Tolls: An Ethnography of a Night-Nurse Sub-Culture," *Studies in Cultures, Organizations and Societies* (5) 1999, pp 347-369.

Brostoff, S., and Sasse, M.A. "Safe and Sound: A Safety-Critical Design Approach to Security," New SecurityParadigms Workshop ACM Press, Cloudcroft, NM, 2001, pp. 41-50.

Carpenter, M.A., Geletkanycz, M.A., and Sanders, G., Wm. "Upper Echelons Research Revisited: Antecedents, Elements, and Consequences of Top Management Team Composition " *Journal of Management* (30:6) 2004, pp 749-778.

Carroll, J.S. "Safety Culture as an Ongoing Process: Culture Surveys as Oppurtunities for Enquiry and Change," *Work & Stress* (12) 1998, pp 272-284.

Chatman, J.A., Polzer, J. T., Barsade, S. G., and Neale, M. A. "Being Different Yet Feeling Similar: The Influence of Demographic Composition and Organizational Culture on Work Processes and Outcomes," *Administrative Science Quarterly* (43:4) 1998, pp 749-780.

Chia, P.A., Maynard, S.B., and Ruighaver, A.B. "Understanding Organizational Security Culture," Pacific Asia Conference on Information Systems, 2002.

Cochran, J.K., and Bromley, M.L. "The Myth of the Police Sub-Culture," *Policing* (26:1) 2003, pp 88-117.

Committee, N.S.T.a.I.S.S. "National Information Systems Security Glossary," N.S.T.a.I.S.S. Committee (ed.), 2003.

Cox, S., and Cox, T. "The Structure of Employee Attitudes to Safety: A European Example," *Work & Stress* (5) 1991, pp 93-104.

Cyert, R., and March, J.G. *A Behavioral Thoery of the Firm* Prentice-Hall, New Jersey, 1963.

Dawson, S., Willman, P., Clinton, A., and M., B. *Safety at Work The Limits of Selfregulations* Cambridge University Press, Cambridge, England, 1988.

Dhillon, G. "Interpreting the Management of Information Systems Security," London School of Economics and Political Science, London, 1995.

Diaz, R., and Cabrera, D. "Safety Climate and Attitude as Evaluation Measures of Organisational Safety," *Accident Analysis and Prevention* (29:5) 1997, pp 643-650.

Donald, I., and Canter, D. "Employee Attitudes and Safety in the Chemical Industry," *Journal of Loss Prevention in the Process Industries* (7) 1994, pp 203-208.

Dong-Chul, S.E.O. "An explicative model of unsafe work behavior," *Safety Science* (43:3) 2005, pp 187-211.

Embrey, D.E. "Incorporating Management and Organisational Factors into Probabilistic Safety Assessment," *Reliability Engineering and System Safety,* (38) 1992, pp 199-208.

Finkelstein, S., and Hambrick, D. C. *Strategic Leadership: Top Executives and their Effects on Organizations* West Publishing, Minneapolis, 1996.

Finkelstein, S., and Hambrick, D.C. "Top-Management-Team Tenure and Organizational Outcomes: The Moderating Role of Managerial Discretion," *Administrative Science Quarterly* (35) 1990, pp 484-503.

Fishbein, M., and Ajzen, I. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research.* Addison-Wesley, Reading, MA, 1975.

Flin, R., Mearns, K., O'Connor, P., and Bryden, R. "Measuring Safety Climate: Identifying the Common Features," *Safety Science* (34) 2000, pp 177-192.

Guldenmund, F.W. "The Nature of Safety Culture: A Review of Theory and Research," *Safety Science* (34:1) 2000, pp 215-257.

Guzman, I.R., Stanton, J.M., Stam, K.R., Vijayasri, V., Yamodo, I., Zakaria, N., and Caldera, C. "A Qualitative Study of the Occupational Subculture of Information Systems Employees in Organizations," SIGMIS-CPR, 2004.

Guzman, I. R., K.R. Stam, and J.M. Stanton (2008) “The Occupational Culture of IS/IT Personnel within Organizations,” *The DATA BASE for Advances in Information Systems*, 39(1), pp. 33.

Hage, J., and Dewar, R. "Elite Values Versus Organizational Structure Predicting Innovation," *Administrative Science Quarterly* (17) 1972, pp 279-290.

Halliday, J., and Von Solms, R. "Effective Information Security Policies," in: *Information Technology on the Move,* R. Von Solms (ed.), Port Elizabeth Technikon, Port Elizabeth, 1997, pp. 12-20.

Hambrick, D.C., Cho, T.S., and Chen, M. "The Influence of Top Management Team Heterogeneity on Firms' Competitive Moves," *Administrative Science Quarterly* (41) 1996, pp 659–684.

Hambrick, R.C., and Mason, P.A. "Upper Echelons: The Organization as a Reflection of Its Top Managers," *Academy of Management Review* (9:2) 1984, pp 193-206.

Hansen, C.D. "Occupational Cultures: Whose Frame are We Using?," *The Journal of Quality and Participation* (18:3) 1995, pp 60-64.

Hawkins, P. "Organizational Culture: Sailing Between Evangelism and Complexity," *Human Relations* (50:4) 1997.

Hoffman, D.A., and Stetzer, A. "A Cross-Level Investigation of Factors Influencing Unsafe Behaviors and Accidents," *Personnel Psychology* (49) 1996, pp 307-339.

Hofstede, G. *Culture's Consequences: International Differences in Work-Related Values* Sage, Beverly-Hills, CA, 1980.

Huston, T. "Security Issues for Implementation of E-Medical Records," *Communications of the ACM* (44:9) 2001, pp 89-94.

IAEA "Security Culture: A Report by International Safety Advisory Group," Vienna International Safety Advisory Group, 1991.

Iivari, N., and Abrahamsson, P. "The Interaction Between Organizational Subcultures and User Centered Design – A Case Study of an Implementation Effort," Proceedings of the 35th Hawaii International Conference on Systems Sciences, Hawaii, 2002.

Jackson, S. "Consequences of Group Composition for the Interpersonal Dynamics of Strategic Issue Processing," in: *Advances in Strategic Management,* P. Shrivatsava, Huff, A., and Dutton, J. (ed.), JAI Press, Greenwich, CT, 1992, pp. 345-382.

Jermier, J.M., Slocum, J.J.W., Fry, L.W., and Gaines, J. "Organizational Subcultures in a Soft Bureaucracy: Resistance Behind the Myth and Facade of an Official Culture," *Organization Science* (2:2) 1991, pp 170-194.

Klein, K.J., Dansereau, F., and Hall, R.J. "Levels Issues in Theory Development, Data, Collection, and Analysis," *Academy of Management Review* (19:2) 1994, pp 195-229.

Klen, T. "Subjective and Objective Risk Estimate in Logging Work," International Conference on Ergonomics, Occupational Safety and Health and the Environment, Beijing, China, 1988.

Kroeber, A.L., and Kluckhohn, C. *Culture: A Critical Review of Concepts and Definitions.*, 1963.

Lapointe, L., and Rivard, S. "A Multilevel Model of Resistance to Information Technology Implementation," *MIS Quarterly* (29:3) 2005, pp 461-492.

Leidner, D. L. and T. R. Kayworth (2006) "A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict," *MIS Quarterly*, 30(2), pp. 357–399.

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

Leveson, N.G., Barrett, B., Carroll, J., Cutcher-Gershenfeld, J., Dulac, N., and Zipkin, D. "Modeling, Anayzing, and Engineering NASA's Safety Culture," MIT.

March, J.G., and Simon, H.A. *Organizations* Wiley, New York, 1958.

Marcinkowski, S.J., and Stanton, J.M. "Motivational Aspects of Information Security Policies," *IEEE - Systems, Man and Cybernetics*) 2003, pp 2527-2532.

Martin, J. *Cultures in Organizations: Three Perspectives* Oxford University Press, New York, 1992.

Martin, J., and Siehl, C. "Organizational Culture and Counterculture: An Uneasy Symbiosis," *Organizational Dynamics* (12:Autumn) 1983, pp 52-64.

Martins, A., and Eloff, J. "Information Security Culture," SEC2002, 2002.

Mearns, K., Flin, R., Gordon, R., and Fleming, M. "Human and Organizational Factors in Offshore Safety," *Work & Stress* (15:2) 2001, pp 144-160.

Miles, M.B., and Huberman, A.M. *An Expanded Sourcebook: Qualtitative Data Analysis*, (2 ed.) Sage Publications, Thousand Oaks, CA, 1994.

Miller, M., and Van Maanen, J. "Getting into Fishing: Social Identities Among Fisherman," *Urban Life* (11) 1982, pp 27-54.

Mintzberg, H. *The Structuring of Organizations* Prentice-Hall, Englewood Cliffs, NJ, 1979.

Montagna, P.D. "The Public Accounting Profession," in: *The Professions and their Prospects,* E. Freidson (ed.), Sage Publications, Beverly Hills, 1973, pp. 135-151.

Narayanan, V.K., and Fahey, L. "Evolution of Revealed Causal Maps During Decline: A Case Study of Admiral," in: *Mapping Strategic Thought,* A.S. Huff (ed.), Wiley, New York, 1990, pp. 109-133.

O'Reilly III, C.A., Chatman, J., and Caldwell, D. F.. "People and Organizational Culture: Assessing Person-Organizational Fit," *Academy of Management Journal* (34:3) 1991, pp 487-516.

Ouchi, W.G., and Johnson, A. B. "Types of organizational control and their relationship to emotional well-being " *Administrative Science Quarterly* (23) 1978, pp 292-317.

Pare, G. "Understanding the Dynamics of Information Technology Implementation: The Case of Clinical Information Systems," in: *Information Systems*, Florida International University, Miami, Florida, 1995 p. 673.

Peltier, T.R. *Information Security Policies, Procedures, and Standards: Guidelines for Effective information Security Management* Auerbach Publications, Boca Raton, Florida, 2002.

Peters, T.J., and Waterman, R. *In Search of Excellence* Harper and Row, New York, 1982.

Pettigrew, A. "The Creation of Organizational Cultures," London Graduate School of Business Studies, 1976.

Pfeffer, J., and Salancik, G.R. *The External Control of Organizations: A Resource Dependence Perspective* Harper and Row, New York, 1978.

Purvis, R.L., Sambamurthy, V., and Zmud, R.W. "The Assimilation of Knowledge Platforms in Organizations: An Empirical Investigation," *Organization Science* (12:2) 2001, pp 117-135.

Ramachandran, S. , and Rao, V. Srinivasan, Goles, Tim J., and Dhillon, G. (*forthcoming). "*Variations in Information Security Cultures across Professions: A Qualitative Study," *Communications of the Association of Information Systems.*

Rao, V. Srinivasan and S. Ramachandran (2011) “Occupational Cultures of Information Systems Personnel and Managerial Personnel: Potential Conflicts,” *Communications of the Association of Information Systems,* 29, Article 21.

Reason, J. *Human Error* Cambridge University Press, Cambridge, UK, 1990.

Rosen, M. "Breakfast at Spiro's: Dramaturgy and Dominance," *Journal of Management* (11:2) 1985, pp 31-48.

Ruighaver, A.B., Maynard, S.B., and Chang, S. "Organisational Security Culture: Extending the End-User Perspective," *Computers & Security* (26:1) 2007, pp 56-62.

Ryan, R.M., and Deci, E.L. "Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being," *American Psychologist* (55:1) 2000, pp 68-78.

Sackmann, S.A. "Culture and Subcultures: An Analysis of Organizational Knowledge," *Administrative Science Quarterly* (37:1) 1992, pp 140-161.

Sapp, M.L., and Behrens, T.L. "Single Logon: Balancing Security and Healthcare Productivity," Mayo Foundation for Medical Education and Research, Rochester, Minnesota, pp. 1-13.

Sasse, M.A., Brostoff, S., and Weirich, D. "Transforming the 'Weakest Link': A Human-Computer Interaction Approach to Usable and Effective Security," *BT Technology Journal* (19:3) 2001 pp 122-131.

Schein, E.H. *Organizational Culture and Leadership* Jossey-Bass, San Francisco, 1985.

Sharma, R., and Yetton, P. "The Contingent Effects of Management Support and Task Interdependence on Successful Information Systems Implementation " *MIS Quarterly* (27:4) 2003 pp 533-555.

Shimeall, T., and McDermott, J.J. "Software Security in an Internet World: An Executive Summary," *IEEE Software* (July) 1999.

Smircich, L. "Concepts of Culture and Organizational Analysis," *Administrative Science Quarterly* (28) 1983a, pp 339-358.

Smircich, L. "Studying Organizations as Cultures," in: *Beyond Method: Strategies for Social Research*, G. Morgan (ed.), Sage, Beverly Hills, CA, 1983b, pp. 160-172.

Smith, S., D. Winchester, D. Bunker and R. Jamieson (2010) "Circuits of Power: A Study of Mandated Compliance to an Information Systems Security *De Jure* Standard in a Government Organization," *MIS Quarterly*, 34(3), pp. 463-486.

Stablein, R., and Nord, W. "Practical and Emancipatory Interests in Organizational Symbolsim: A Review and Evaluation," *Journal of Management* (11:2) 1985, pp 13-28.

Stanton, J.M., Stam, K.R., Mastrangelo, P., and Jolton, J. "Analysis of End User Security Behaviors," *Computers & Security* (24) 2005, pp 124-133.

Tejay, G., and Dhillon, G. "Developing Measures of Information Security," in: *The Fourth Workshop on e-Business (WeB 2005)* Las Vegas, 2005.

Thompson, J.D. *Organizations in Action: Social Sciences Bases of Administrative Theory* McGraw Hill, New York, 1967.

Trice, H. *Occupational Subcultures in the Workplace* ILR Press, Ithaca, NY, 1993a.

Trice, H., and Beyer, J.M. *The Culture of Work Organizations* Prentice-Hall, Englewood Cliffs, NJ, 1993a.

Trice, H.M. *Occupational Subcultures in the Workplace* ILR Press, Ithaca, NY, 1993b.

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

Vroom, C., and Von Solms, R. "Towards Information Security Behavioral Compliance," *Computers & Security* (23) 2004, pp 191-198.

Watne, D., and Turney, P. *Auditing EDP Systems* Prentice-Hall, Englewood Cliffs, NJ, 1990.

Wiegmann, D.A., Zhang, H., Thaden, T., Sharma, G., and Mitchell, A. "A Synthesis of Safety Culture and Safety Climate Research," University of Illinois at Urbana-Champaign, Savoy, Illinois, pp. 1-20.

Wienburg, S.K. "The Occupational Culture of the Boxer," *The American Journal of Sociology* (57:5) 1952, pp 460-469.

Wiersema, M.F., and Bantel, K.A. "Top Management Team Demography and Corporate Strategy Change," *Academy of Management Journal* (35:1) 1992, pp 91-121.

Wilensky, H.L. "The Professionalization of Everyone?," *American Journal of Sociology* (70:2) 1964, pp 137-158.

Winston, S. *Culture and Human Behavior*, New York, 1933.

Wood, C. "Integrated Approach Includes Information Security," *Security* (37:2) 2000, pp 43-44.

Wright, C. "Routine Deaths: Fatal Accidents in the Oil Industry," *Sociological Review* (4) 1986, pp 265-289.

Yule, S. "Senior Management Influence on Safety Performance in the UK and US Energy Sectors," University of Aberdeen, Aberdeen, Scotland, 2003.

Zohar, D. "Safety Climate in Industrial Organizations: Theoretical and Applied Implications," *Journal of Applied Psychology* (65:1) 1980, pp 96-102.