Communications of the Association for Information Systems

Volume 33 Article 11

12-2013

# Variations in Information Security Cultures across Professions: A Qualitative Study

Sriraman Ramachandran
*Global Program Manager, Sales Transformation, Dell Inc.*

Chino Rao
*utsa*, chino.rao@utsa.edu

Tim Goles
*A. R. Sanchez, Jr. School of Business, Texas A&M International University*

Gurpreet Dhillon
*School of Business, Virginia Commonwealth University*

Communications of the Association for Information Systems

CAIS

# Variations in Information Security Cultures across Professions: A Qualitative Study

Sriraman Ramachandran

*Global Program Manager, Sales Transformation, Dell Inc.*

V. Srinivasan Rao

*Department of Information Systems and Cyber Security, The University of Texas at San Antonio*

*Chino.Rao@utsa.edu*

Tim Goles

*A. R. Sanchez, Jr. School of Business, Texas A&M International University*

Gurpreet Dhillon

*School of Business, Virginia Commonwealth University*

Abstract:

The importance of culture in helping explain and understand behavior is generally accepted. Scholars in the area of information security have argued that security culture is a key factor in safeguarding information assets. Scholars in the area of professional culture have argued that differences in cultures across professions must be accounted for, in correctly assessing the influence of culture. Combining these arguments, we suggest that differences in security cultures across professions need to be examined to fully comprehend the influences of security culture. The current study uses a qualitative approach to further the understanding of information security cultures across four professions: Information Systems, Accounting, Human Resources, and Marketing. The concept of security culture is articulated, and the security cultures of the four professions are characterized to demonstrate that there are significant variations in security culture across these professions. The study also shows that information security continues to be viewed as a technical problem, that even the most conservative and rule-compliant groups may violate security rules under performance pressure, and that awareness by itself is not sufficient to build a strong security culture.

**Keywords:** information security culture; professional culture

.

Volume 33, Article 11, pp. 163–204, December 2013

The manuscript was received 01/31/2011 and was with the authors 12 months for 2 revisions.



Communications of the Association for Information Systems

## I. INTRODUCTION

Culture has emerged as a key construct in organizational and information systems (IS) research. There are myriad conceptualizations and definitions of culture (comprehensive reviews are provided by Leidner and Kayworth [2006]; Straub, Loch, Evaristo, Karahanna and Strite [2002]), but there is general agreement that culture includes a shared set of assumptions, values, and beliefs that help shape subsequent behavior of a social group [Kroeber and Kluckhohn, 1963]. When viewed at the organizational level, culture helps employees make sense of the firm and provides norms for their behavior [Deshpande and Webster, 1989; Gregory 1983]. It has also been shown that culture is predictive of performance [e.g., Gordon and DiTomaso, 1992]. As the need to safeguard information assets has become increasingly important [e.g., Dhillon, 1997; Von Solms, 2000], scholars have advocated the development of a strong information security culture[1] to enhance protection of such assets [Ruighaver, Maynard and Chang, 2007; Vroom and Von Solms, 2004]. Researchers believe that technical controls and information security policies alone are not adequate to ensure information security. In addition to the technical controls and security policies, an information security culture is deemed necessary to ensure behavior compliant with information security needs [e.g., Von Solms and Von Solms, 2004].

Most research in the area focuses on information security culture in the context of organizations [e.g., Ruighaver et al., 2007]. Furthermore, most researchers adopt a monolithic view of organizational security culture (i.e., that the security culture is uniform across different groups in organizations). Studies of culture (unrelated to security culture) in organizations have shown the existence of differentiated cultures [Chatman, Polzer, Barsade and Neale, 1998; Jermier, Slocum, Fry and Gaines, 1991], including differences in cultures across occupations and professions [Trice, 1993]. Differentiated cultures have been shown to lead to differences in the thinking, reasoning, and priorities of different professional groups [Hansen, 1995; Mills and Tsamenyeni, 2000], which in turn could lead to intraorganizational conflicts and consequent failure of larger initiatives [e.g., Rao and Ramachandran, 2011]. Analogously, it can be argued that differences in information security cultures across professions could lead to differences in thinking and reasoning about security issues, and possibly conflicts in and failure of information security initiatives. Consequently, it is necessary to understand the differences in information security cultures across professions. Thus, the primary goals of the current research are to determine if there are differences in security cultures across professions, and, if so, what are the differences? Implicit in this statement is that we are studying information security culture at the level of a profession.

An understanding of the differences is important both to research and to practice. In research, monolithic characterization of information security culture may obscure important relationships between security culture and other variables. For instance, a researcher examining the effect of security policies on security culture may not find any effect. In reality, it is possible that it affects the security culture of groups that tend to be more rule-compliant, and not that of groups who tend to be less rule-compliant. Examined as a whole, the relationship may be obscured. In practice, there is the possibility of conflicts between groups because of differences in security cultures. For instance, if a professional group believes that information security is the responsibility of information systems (IS) personnel, and information security personnel believe that all users are responsible, then it is possible that the professional group fails to take seriously security policies proposed by the IS group, particularly if the policies require effort by the professional group. The policies may be viewed by the professional group as an attempt by IS personnel to shirk their responsibilities. Knowledge of such differences in cultural beliefs will enable management to take steps necessary to ensure that security initiatives are not misconstrued. Thus, understanding the differences in security cultures across professions is important for the field of information security.

The rest of the article is organized as follows. In the next section, we discuss relevant literature. Following this, we outline the theoretical bases and methodological issues. Next, we report our results. In the subsequent section, we present our key findings, summarize our contributions, and state the limitations of the study. Lastly, we make some concluding remarks.

[1] We use the terms “information security culture” and “security culture” interchangeably.

## II. LITERATURE REVIEW

### Culture

The complexity and ambiguity associated with the study of culture has been acknowledged by scholars [Leidner and Kayworth, 2006; Schein, 2004; Trice and Beyer, 1993]. In 1963, Kroeber and Kluckhohn identified about 164 definitions [Kroeber and Kluckhohn, 1963]; in 2006, Leidner and Kayworth reported that there were about 359 definitions [Leidner and Kayworth, 2006]. We provide a brief sampling of the definitions over the years to illustrate the complexity (see Table 1). The definitions appear to have two parts. The first part reflects that culture is viewed as an aggregation, and the second part lists the components. The aggregation aspect is seen in the part of the definition that states culture is viewed as "a complex whole which includes…," "…embraces all the manifestations of …" "…the totality of .." "as the sum total of .." and so on. Culture is seen as an aggregation of components that includes terms such as "knowledge," "beliefs," "habits," "values," "ideas," "behaviors," "concepts," "attitudes," and so on.

**Table 1: Some Definitions of Culture from Literature**

| Source | Definition |
|---|---|
| Tylor [1871] | "…complex whole which includes knowledge, belief, art, law, morals, custom and any other capabilities and habits acquired by man as a member of a society." (p. 1) |
| Boas [1930] | "Embraces all the manifestations of social habits of a community, the reactions of the individual as affected by the habits of the group in which he lives, and the products of human activities as determined by these habits." (p. 79) |
| Kroeber and Parsons [1958] | "Transmitted and created content and patterns of values, ideas and other symbolic meaningful systems as factors in the shaping of human behavior and the artifacts produced through the behavior." (p. 583) |
| Thurnwald [1950] | Defines culture as the totality of usages and adjustments that relate to family, political formation, economy, labor, custom, law, and ways of thought. |
| Kluckhohn [1949] | Defines culture as a "social legacy" that an individual acquires from his/her group. |
| Geertz [1973]] | "Historically transmitted pattern of meanings embodied in symbols, a system of inherited conceptions expressed in symbolic forms by means of which men communicate, perpetuate, and develop their knowledge about and attitudes toward life." (p. 89) |
| Kroeber and Kluckhohn [1952] | "It is a plan, not the living itself; it is that which selectively channels men's reactions, it is not the reaction themselves." (p. 120) |

The complexity of the conceptualization presents challenges at two levels: in the meaning of the terms used to define culture, and in the observation and measurement of culture. Terms such as "beliefs" and "ideas" are mostly used in the common everyday meaning of the words, without precise definitions being assigned to them. When observing culture, the challenge is to determine if it is sufficient to focus on one or some aspects of culture or if all aspects have to be taken into consideration. Schein [1985] proposed a three-layer model, which addresses the second of these issues. The three layers comprise artifacts, values, and assumptions. Artifacts are visible manifestations, such as behavior, rituals, jargon, and so on. Values include social principles, standards, beliefs, and so on, which have intrinsic worth to the group. Assumptions include taken for granted beliefs. Schein's model indicates that the three layers are interdependent, with artifacts and values having a reciprocal causal relationship, and values and assumptions having a reciprocal causal relationship. Because of the reciprocal relationships, it is usually considered sufficient to observe artifacts (such as rituals) or analyze beliefs to characterize cultures.

In published research, empirical studies of culture, which attempt to characterize or measure dimensions of culture, have done so by observing behaviors or by eliciting beliefs (which may include beliefs related to values or beliefs related to assumptions) through questionnaires or interviews. For instance, Robey and Markus [1984] adopted a cultural approach to understanding the information systems development (ISD) process by analyzing rituals. In other words, they viewed the cultural process through the lens of the artifacts, since rituals are an observable form of artifacts. In contrast, Iivari and Abrahamsson [2002] examined the cultural differences between managers, software engineers, and user-centered design specialists by identifying their beliefs with respect to user-centered design (UCD). Thus, although culture includes both visible manifestations (artifacts) and beliefs (values and assumptions), a characterization of culture can be based on one or the other or both, regardless of the fact that the definition of culture includes artifacts and the beliefs that constitute values and assumptions.

It should be noted that the term "belief" is used broadly in the literature on culture. This is best seen in this hypothetical example. A respondent could say, "All men are created equal," which can be seen as a statement of value. Alternately, the respondent may say, "I believe 'all men are created equal,'" which can be seen as a statement of belief. But the two statements lead to the same characterization of culture. Thus, in efforts to characterize culture,

the distinction between the terms such as "values" and "beliefs" are not critical. We use the term "belief" broadly to include statements or responses about values, assumptions, ideas, morals, customs, and so on.

## Professional Cultures

The culture of specific professions has long been a subject of study for organizational scholars (e.g., night watchmen [Trice, 1993]; police [Van Maanen, 1973]). The existence of distinct cultural characteristics unique to individual professions has been documented. For example, accountants view themselves as rationalists [Pondy, 1983] who believe that the primary reality is a cold-blooded "bottom-line" [Trice and Beyer, 1993]. The culture of doctors is rooted in the Hippocratic Oath, which emphasizes the primacy of 'do no harm' [Smith and Kleinman, 1989]. The engineering culture in a high technology firm is described as being informal, where initiative and trust are important, and "working for money as a prime motivator will be abhorred" [Kunda, 1995, p. 75]. These findings support the idea that individuals who practice the same profession tend to band together into communities, draw their identities from the work they do, and share a set of values, norms, and attitudes, all of which form a part of their occupational culture [Van Maanen and Barley, 1984].

More research has found evidence supporting the existence of a distinct occupational culture among IS professionals [Guzman et al., 2004; Guzman, Stam, and Stanton 2008; Rao and Ramachandran, 2011]. These studies have shown that IS professionals have a converging cluster of characteristics, reflecting such attributes as the technical nature of the occupation, the responsibilities of IS personnel associated with technology, and the use of technical jargon. Managers view IS professionals as responsible for not only the technology, but also "to help serve their staff so they can be the most efficient and productive, while at the same time protecting the organization from outside threats" [Guzman et al., 2004, p. 79].

As mentioned earlier, differences in cultures across professions are often the source of differences in thinking, reasoning, and priorities [Hansen, 1995], which can lead to conflicts and dysfunctions. For instance, Iivari and Abrahamsson [2002] showed that managers believed that user-centered design (UCD) was theoretical and complicated, software engineers considered UCD as unimportant, while UCD specialists considered it important and useful. Rao and Ramachandran [2011] showed that IS personnel believed that technical jargon was essential for precise communication, while managers believed that technical jargon just confused non-technical people. Such differences in cultural beliefs can be readily seen to be potential sources of problems in the context of interactions between professional groups. This brief review indicates that groups belonging to different professions can have distinctly different beliefs, and such differences have the potential to cause dysfunctional interactions between the groups. Consequently, our premise is that different professional groups are likely to have distinct beliefs that would constitute distinct security cultures of their own. These differences need to be identified and understood to avoid dysfunctions in the design and implementation of information security initiatives.

## Security Culture

In this sub-section, we discuss the importance of security cultures, the diverse conceptualizations of security culture in literature, and the efforts to identify the dimensions of culture. Lastly, we include a section on alternate approaches to improve security-related behaviors.

The importance of security culture in the protection of information has been recognized for quite some time [e.g., Andress and Fonseca, 2000; Beynon, 2001; Breidenbach 2000; Schwarzwalder, 1999; Von Solms, 2000]. Proponents argue that the development of a security culture in organizations would influence employee behavior over and beyond technological and managerial controls [Dhillon, 1995; Ruighaver et al., 2007; Vroom and Von Solms, 2004]. It has been argued that company policies alone are not adequate to ensure appropriate security behavior, but must manifest in a culture to produce the desired effects [Von Solms and Von Solms, 2004]. Furthermore, it has been pointed out that while culture is expected to have a significant effect on security, such effect could be positive or negative [Vroom and Von Solms, 2004].

The acknowledgement of the importance of security culture has spawned a keen interest in research in this area. Notwithstanding the high level of interest, the concept of security culture is still evolving. In some early studies, security culture is left undefined [e.g., May, 2003]. In others, the definition is near circular. For instance, Gaunt [2000, p. 152] views security culture in a health environment as "a culture in which personal health care information is processed securely." Still others [e.g., Knapp, Marshall, Rainer and Ford, 2006] measure security culture using survey items, such as, "Employees value the importance of security" and "A culture exists that promotes good security practices," from which items the reader could infer the researchers' conceptualization of security culture.

A sampling of the definitions of security culture suggests diversity in thinking. Dhillon [1997] defines security culture as "the totality of *patterns of behaviour* [our italics] in an organization that contribute to the protection of information

of all kinds." Martins and Eloff [2002, p. 205] see information security culture "as a set of information security characteristics. These characteristics such as *integrity and availability of information* [our italics]…. Information security culture is also seen as an *assumption* [our italics] about what is and what is not acceptable in relation to information security." Helokunnas and Kuusisto [2003, p. 191] view security culture as "a system consisting of *interacting framework and content category components* [our italics] of information security," where content includes "people attitude, motivation and knowledge including mental models about information security." Others use Schein's three-layer model as the basis and include artifacts and creations, collective values, norms and knowledge, basic assumptions and beliefs [e.g., Schlienger and Teufel, 2003]. Schlienger and Teufel use a questionnaire with ten items, which are not specifically classified as values, norms, or beliefs. The diversity of characterizations of security culture can be seen in these definitions. What is evident is that some researchers focus on behavior, while others focus on values and beliefs. Each of these belongs in one of the layers of the Schein [1985] model for culture. In other words, researchers base their definition and conceptualization of information security culture on the Schein model, which was originally proposed for culture.

In the current study, we also view Schein's model [Schein, 1985] as a basis for conceptualizing information security culture (i.e., information systems culture includes behaviors, values, and assumptions/beliefs that inform on the topic of security). Further, as we stated earlier, we use the term "belief" broadly to include all responses about knowledge, ideas, values, beliefs, assumptions, and so on. Also, as we have shown, it is usually adequate to examine a single aspect such as rituals or beliefs to characterize culture. In the current study, we will elicit beliefs from respondents in interviews to characterize information security cultures of professionals.

Researchers who have delved a little deeper into conceptualizing security culture have drawn on two perspectives, primarily in an effort to propose methods or frameworks to improve organizational security culture. The first perspective is that of Schein [1985]. For example, Schlienger and Teufel [2003] attempt to assess the gap between employee perceptions at all three levels and the actual state in an organization. They do not explain how they arrived at the items that they use. Further, the items range from low level items, such as "Passwords should always have a length of at least eight characters and contain at least two alphanumeric characters in the middle," to high level items such as, "Every employee should be trained in the information security controls he/she is supposed to use in his/her work."

Zakaria and Gani [2003] use the Schein model to create a checklist. They use elements underlying each of the three layers and intuitively propose specific items of interest in information security. For instance, for the artifacts (surface manifestations) layer, they consider the element, norms, and propose the item, "Never open any suspicious attachment file of e-mail or always update antivirus databases online," for the checklist. Effectively, the items on the checklist reflect a do or don't, which collectively are argued to improve security culture in an organization. The process by which items are generated is not discussed.

Both articles [Schlienger and Teufel, 2003; Zakaria and Gani, 2003] are focused on enhancing information security in organizations by detailing low level behaviors that employees should comply with (e.g., using passwords with some characteristics or not opening suspicious attachments). Admittedly, these behaviors will improve information security and help develop a stronger information security culture in organizations. However, they are not useful in characterizing the information security culture of a group.

In the second perspective, researchers have attempted to identify dimensions of security culture [e.g., Chia, Maynard and Ruighaver, 2002; Tejay and Dhillon, 2005] based on different theories. Chia et al. use Detert, Schroeder, and Mauriel's framework [Detert, Schroeder and Mauriel, 2000], and Tejay and Dhillon used Hall's classification of behavioral responses to the implementation of a new computer-based system in an organization [Hall, 1959].

Chia et al. [2002] use the eight dimensions that Detert et al. [2000] proposed to characterize culture associated with the success of total quality management in organizations. The eight dimensions are: (1) the basis of truth and rationality, (2) the nature of time and time horizon, (3) motivation, (4) stability versus change/innovation/personal growth, (5) orientation to work, task, co-workers, (6) isolation versus collaboration/cooperation, (7) control, coordination, and responsibility, and (8) orientation and focus—internal and/or external. Chia et al. [2002] adapted these for the context of information security culture in organizations. Thus, for example, under the category of the basis of truth and rationality, they examine employee beliefs about the truth and rationality of what information security is and the importance of information security.

A point to note is that the dimensions are not completely orthogonal, and instances of partial overlap can be identified. For example, under the dimension orientation to work, task, and co-workers, the authors include one statement that "employees should be made to feel responsible for security in the organizations," and under the

dimension isolation versus collaboration/cooperation, they include that, “Every member of an organization should be involved in some way with maintaining security.” There is little, if any, distinction between the two statements, so this is a point of overlap between the two dimensions. There are other elements to each dimension that are different from each other. For example, the first dimension states that education of employees about security is important, while the second dimension emphasizes the importance of including all employees in the development of security policies.

Chia et al. [2002] developed a qualitative comparison of two organizations along these dimensions. Their results indicate differences between the two organizations on several of the dimensions. For instance, organization A believed security to be very important, adopted a longer-term view, and had strict security policies in place. In contrast, organization B believed security to be less important, adopted a shorter-term view, and did not have strong security policies in place. In sum, the framework is useful in characterizing and comparing information security cultures of organizations.

Tejay and Dhillon [2005] base their development of dimensions on Hall’s [Hall, 1959] classification of behavioral responses to the implementation of a new computer-based system in an organization. The responses or behavioral patterns are referred to as silent messages. Following Dhillon’s [1995] examination of the implications of the silent messages for information security, Tejay and Dhillon [2005] have developed these further to propose dimensions for information systems culture. The seven constructs that they have proposed are group cohesiveness, professional codes, informal work practice, empowerment, planning, information security awareness, and organizational structure. Tejay and Dhillon [2005] have developed multi-item scales for each dimension and argue that the dimensions are useful in assessing the information security culture of an organization.

There are some issues worthy of note. First, both frameworks are focused on information security culture in organizations. Second, they are both prescriptive in nature (i.e., trying to suggest ways in which information security culture in organizations can be strengthened). For instance, Chia et al. [2002] indicate that “Employees *should* [our italics] …” in some of their statements, implying prescriptive suggestions. An example from Tejay and Dhillon [2005] would be their hypothesis “Lack of planning would have impact on information security culture of an organization,” implying prescriptively that planning is necessary. Lastly, there are overlapping aspects to the points underlying both sets of dimensions. The overlaps are not relevant to the current study, so they are not discussed further.

Based on our literature review of the information security culture, we believe that research in the area is still at an early stage. Our review points to three significant issues. First, the concept of security culture draws on the concepts developed for culture in general (e.g., Schein’s model). Second, diverse approaches are being used to assess information security culture. Third, security culture has been studied in an organizational context and viewed from an integrated perspective (i.e., security culture is seen as uniform throughout the organization, with minor exceptions). An example of the exception would be the study by Ruighaver et al. [2007], who examine the differences in security beliefs of IT managers and end-users [Ruighaver et al., 2007]. No study exists that examines differences in security cultures across professions.

In the next sub-section, we briefly discuss alternate approaches to improve security-related behaviors.

### Alternate Approaches to Improve Security-Related Behaviors

The development of security culture is one approach to improving security-related behaviors. Other approaches are possible. Published literature on alternate approaches includes both descriptive and prescriptive studies. Descriptive studies focus on identifying factors that influence security-related behaviors, while prescriptive studies propose and test methods to improve security-related behaviors. For instance, descriptive studies have shown that social influence [e.g., Herath and Rao, 2010; Johnston and Warkentin, 2010; Lee and Larsen, 2009], self-efficacy [e.g., Bulgurcu, Cavasoglu and Benbasat, 2010], perceived threat characteristics (e.g., threat severity [Johnston and Warkentin, 2010], and threat appraisal [Lee and Larsen, 2009]), neutralization [Siponen and Vance, 2010], awareness [Bulgurcu et al., 2010], and so on, influence attitudes and intentions to comply with security policies.

It is possible to infer prescriptive measures from the descriptive studies. For instance, the finding that awareness increases compliance suggests that organizations should implement initiatives to increase awareness of security-related issues among employees. Prescriptive studies recommend mandatory compliance [Boss, Kirsch, Angermeier, Shingler and Boss, 2009; Kwon and Johnson, 2011; Smith, Winchester, Bunker and Jamieson, 2010], deterrence [D’Arcy and Herath, 2011], fear appeals [Johnston and Warkentin, 2010], training [e.g., Puhakainen and Siponen, 2010], user participation [Spears and Barki, 2010], and so on.

The long list of explanatory factors is overwhelming initially, but a deeper examination shows two points. First, the prescriptive factors tend to work over different temporal frames. Second, the factors, while distinct in some ways, have overlapping characteristics. Each of these points is discussed next.

Viewing the factors from the temporal frame, prescriptive methods to improve security-related behaviors can be classified as short term or medium term. Mandatory compliance may seem to be the method with the most potential for effecting immediate changes in the short term. Monitoring [Boss et al., 2009] and auditing [Kwon and Johnson, 2011] enhance the perception that compliance is mandatory, and thereby improve adherence to security-related rules, policies, and procedures. Boss et al. [2009] report that mandatory compliance rules lead to actual compliance, but Smith et al. [2010] report that only 33 percent of organizations complied with mandatory policies. It is interesting to note that Kwon and Johnson [2011] did not find a correlation between compliance and security performance. Further, mandatory compliance programs include deterrence to motivate employees to observe rules. The effectiveness of deterrence remains to be established conclusively. A review published by D'Arcy and Herath [2011] shows that deterrence is not uniformly effective across published studies. Thus, it would appear that short-term initiatives may need to be supplemented with medium and longer term initiatives.

Medium-term initiatives include fear appeals [Johnston and Warkentin, 2010], user participation [Spears and Barki, 2010], training [e.g., Puhakainen and Siponen, 2010], and similar measures. Results from such initiatives have been mixed. Johnston and Warkentin [2010] have shown that fear appeals can influence behavioral intentions to comply with security requirements, but the effect is not uniform across all end-users. Spears and Barki [2010] have shown that user participation in the formulation of legally mandated compliance programs leads to greater awareness of security, better alignment of security management to the business environment, and improved control processes for ensuring security. Puhakainen and Siponen [2010] report the effective implementation of training programs based on two theories—the universal constructive instructional theory and the elaboration likelihood model. Key findings of the study were that it was necessary to stimulate cognitive processing of material presented during training sessions, and a continuous communication process is needed to improve compliance. In examining the medium-term initiatives, it may be observed that the primary focus of each of these initiatives is different, but there are some overlapping aspects between them. For instance, training can be a forum to communicate three elements of a fear appeal—severity, susceptibility, and the appropriate response to a security incident—and to provide the employee with the fourth element of the fear appeal (i.e., the ability to perform the recommended response). Also, one goal of training is to increase awareness. User participation in formulating policies also serves to increase awareness.

Even as the medium-term initiatives have different foci, but share some commonalities, security culture, while distinct from these medium-term initiatives, also shares some commonalities with them. A comparison of security culture to each of the alternate approaches is possible. As an exemplar, we will compare security culture to one alternate factor, security awareness, to highlight commonalities and differences.

Schein's model [Schein, 1985] of security culture includes values, norms, beliefs, assumptions, and so on. There are different ways to develop or change culture. They include setting examples by senior executives [e.g., Leach, 2003], education [e.g., Von Solms and Von Solms, 2004], and so on. In particular, it is generally accepted that culture is built over a longer period of time and is deeply ingrained. Awareness, on the other hand, is typically defined as "the extent to which organizational members understand the importance of information security; the level of security required by the organization and their individual security responsibilities" [Albrechtsen, 2007, p. 280]. Education and repeated reminders are seen as the primary ways to raise and maintain awareness [e.g., Thompson and Von Solms, 1998].

The overlap between the two terms is that education is seen as a means to develop strong security culture and increase security awareness. Security awareness is seen as a contributor to the development of security culture [Da Veiga and Eloff, 2010; Lim, Ahmad, Chang and Maynard, 2010]. The distinction between the two terms is that high awareness does not necessarily equate to strong culture. Groups may be highly aware of security-related issues but choose not to comply with security requirements for various reasons. By definition, the lack of compliance implies weak security culture. Thus, it is possible to have high security awareness but weak security culture.

In sum, the literature review emphasizes the complexity of the culture construct, as well as the importance of examining differences in professional cultures and diverse aspects of information security culture. In the section on information security culture, current thinking about the importance of security culture is mentioned, definitions are examined, and the existing frameworks to study security culture in organizations are articulated. Lastly, we provide a brief overview of the various factors discussed in the security literature to explain security-related behaviors, and various methods suggested to enhance the behaviors; this overview also includes an exemplar comparison of security culture and security awareness, to illustrate the overlapping and distinguishing characteristics of that security culture from other initiatives.

## III. THEORETICAL FRAMEWORK

In the current study, our goal is to characterize the information security cultures of different professions, and examine the differences across them. Information security cultures of professions is an understudied phenomenon. For this reason, we elected to conduct a qualitative study (i.e., conduct interviews of professionals from selected professional groups to develop a descriptive characterization of the information security cultures of their respective professions). Miles and Huberman [1994] categorize qualitative studies as tight or loose, and discuss the trade-offs between them. They refer to tight designs as those that use a preexisting conceptual framework, and to loose designs as those in which the conceptual framework emerges during the course of the study. They recommend loose designs for understudied phenomena. They also recognize that even in loose designs the researcher comes to the study with some orienting ideas. Eisenhardt [1989] recommends that some *a priori* description of conceptualizations, constructs, and dimensions can help develop a study's initial design.

In the current situation, there is no preexisting conceptual framework for the study of information security cultures of professional groups. However, there are frameworks proposed by Chia et al. [2002] and Tejay and Dhillon [2005] for the study of information security cultures in organizations. These frameworks are not directly applicable in their original formulation for two reasons: (1) the frameworks are for information security cultures of organizations, while our interest is on the information security cultures of professions (the examination of information security cultures at the level of the profession), and (2) the frameworks are prescriptive in nature, while our interest is in developing descriptions of the information security cultures of the different professions. Nonetheless, the two frameworks contain features that can help in formulating a starting point for our study.

The two frameworks have been used to generate issues to address in the characterization of information security culture (see Tables 2 and 3). The process followed to arrive at the issues is as follows. The points discussed by Chia et al. [2002] and Tejay and Dhillon [2005] under each of their respective dimensions were first listed. The points are shown in the tables. If we considered them useful in identifying issues relevant to the information security cultures of professionals, then appropriate issues were noted. If a dimension was focused on an organizational aspect, and did not include any points that were useful for characterizing information security cultures of professionals, then it was excluded. For instance, Tejay and Dhillon [2005] include planning as a dimension based on the logic that planning was important to improving the information security culture of organizations. Planning does not help in understanding or describing the information security culture of professional groups. So, no issue is derived from this dimension. The reasons for excluding other dimensions are indicated in Tables 2 and 3.

In effect, by the Miles and Huberman [1994] discussion of tight and loose designs, our approach falls between the two extremes. In the absence of preexisting frameworks for characterizing the information security culture of professionals, we have adapted previous frameworks for the information security culture of organizations to generate issues relevant to characterizing the information security culture of professionals. The process of generating the issues and the subsequent questions for the interviews is loosely guided by the adapted frameworks and is researcher-driven. As Miles and Huberman [1994] put it, ". . . as researchers, we do have some background knowledge. … We know some questions to ask, … Not to 'lead' with our conceptual strength can be simply self-defeating" [p. 17]. In keeping with this theme, we use our intuition and common sense to generate the questions.

In reviewing the issues generated, it was clear that almost all issues focused on the information security-related beliefs of the professional groups. So, we created a category called security-related beliefs. Only two issues did not fit neatly into the category of security-related beliefs: beliefs about willingness to take risks in general, and beliefs about professional codes. Since these two issues were quite disparate, we created two separate categories: general beliefs and professional identity beliefs. General beliefs include beliefs about risk and compliance, and professional identity beliefs subsume issues related to professional codes. There are two reasons why we have included these two categories in the overall conceptualization of the information security culture of professionals. First, the issues related to these categories are derived from prior conceptualizations of information security culture. In the interest of building on prior research, they should be retained in the conceptualization of the information security cultures of professionals.

Second, while each of the two categories is not limited to security, they do encompass security and can inform us on the issue of information security culture. For instance, the unwillingness to take risks is likely to manifest in a tendency to comply with rules and regulations. It is reasonable to argue that groups that are risk averse are likely to carry over that aversion to the area of information security, and comply with rules and regulations regarding security, resulting in a stronger security culture in the group.

When we consider professional codes, the codes incorporate the profession's core values. The core values in turn are rooted in the profession's perception of who they are, what their role is, and their value to organizations.

| Table 2: Identification of Issues for Interview Guides | |
|---|---|
| Chia et al. [2002] | Listing of preliminary issues to develop interview questions |
| The nature of time and time horizon<br>• Short-term vs. long-term perspective of security | This relates to how organizations should view security to improve the information security culture in organizations. *This is not relevant to characterizing security cultures of professional groups.* |
| Motivation<br>• Are employees intrinsically motivated to accept security?<br>• Rewards and punishment? | This relates to how organizations should motivate employees to improve the information security culture in organizations. *This is not relevant to characterizing the security cultures of professional groups.* |
| Stability versus change/innovation/ personal growth<br>• Stability is safe; change has risks<br>• Willingness to take risks<br>• Willingness to take security risks | We have split this into two: Limited it to members of profession (compares to employees in organization)<br>• Beliefs about risks in general<br>• Beliefs about security risks<br>• Their propensity to take security risks under performance pressure<br><br>Risks are generally controlled by formulating rules and procedures or having direct guidance from management. Beliefs regarding these are related to beliefs about risk:<br>• Beliefs about complying with rules and procedures<br>• Beliefs about organizational hierarchy and complying with managerial guidance |
| Orientation to work, task, co-workers:<br>• Employees should be made to feel responsible for security.<br>• Is security an impediment to the daily operations of an employee?<br>• Education of employees about security is important. | • What is the role of the professional in security?<br>• What conflicts exist between work and security?<br>• What are sources of information about security? |
| Isolation versus collaboration/cooperation<br>• Every member of an organization should be involved in some way with maintaining security.<br>• Security policy should be created collaboratively. | • Who is responsible for information security?<br>• What role does the professional group play in ensuring information security? |
| Control, coordination, and responsibility<br>• Balance between risk and control: empowerment versus enforcement<br>• Alignment of organizational and security goals<br>• Tone for security must be set from the top<br>• Security awareness should be instigated right from the top<br>• Need for security team | Some issues in this category are not relevant to professions. For example, alignment of organizational and security goals is an organizational issue.<br><br>Other issues lead to possible questions:<br>• Beliefs about organizational hierarchy and complying with managerial guidance<br>• Who is responsible for security? |
| Orientation and focus<br>The internal and external focus driving the security activities | In organizations, there may be external forces dictating security behavior. *This is not relevant to characterizing security cultures of professional groups*. |
| The basis of truth and rationality<br>• Importance of security?<br>• What is good/bad security?<br>• What is the effectiveness of security? | • What is security?<br>• What is the importance of security? |

| Table 3: Identification of Issues for Interview Guides | |
|---|---|
| Tejay and Dhillon [2005] | Listing of preliminary issues to develop interview questions |
| Planning<br>• Security requirements should be analyzed. | This is a prescription to improve information security culture in organizations. *It does not relate to security beliefs of professional groups.* |
| Organizational structure<br>• Order of elements in an organization (hierarchical structure)<br>• Assigns authority and responsibilities | • Beliefs about organizational hierarchy and complying with managerial guidance |
| Information security awareness<br>• Awareness of security policies, procedures, controls; role of employee<br>• Attained through education and training | • What is security?<br>• What is the importance of security?<br>• Who is responsible for security?<br>• What are sources of knowledge about security? |
| Informal work practice<br>• Daily operations of how things are done | • What are conflicts between security and work performance? |
| Empowerment<br>• Power<br>• Responsibility (personal accountability)<br>• Authority | • What is the responsibility of the profession for security? |
| Professional codes<br>Ethics<br>Codes of conduct | • Core value of profession<br>• Role of profession<br>• Contribution to organization/society |
| Group cohesiveness<br>• Threatening group cohesiveness will threaten security culture. | This relates to improving the information security culture in organizations by increasing cohesiveness of working groups in organizations. So *this is not relevant to characterizing security cultures of the professional context*. |

Collectively, the core values of the profession, as well as the perception held by members of the profession of who they are, what their role is, and their value to the organization, reflect the beliefs about the identity of the professional group. It can be seen that these perceptions can shed light on security-related beliefs. For example, a group that sees its role as maintaining the integrity of organizations may pay more attention to security-related issues than a group that sees its role as improving the innovativeness of organizations.

In sum, the issues that have been identified to help characterize information security cultures of professionals can be parsimoniously classified into three categories: beliefs about the identity of the profession, general beliefs about risk taking and compliance, and beliefs about security. Each of the issues being considered to characterize security culture of professional groups can be included in one of these three categories. So, no additional category is necessary. Our framework contains the key dimensions applicable to professional security culture from both prior conceptualizations.

## IV. METHODOLOGY

Our qualitative study is based on interviews of respondents from different professions on issues identified in the section on theoretical framework as relevant to the characterization of information security cultures of professions. In this section, we elaborate on the demographics of the respondents in our study, the data collection process, and finally explain the analytical procedures used.

### Respondents

Our goal was to characterize the information security cultures of different professions and compare them. We elected to study four professions, because that number seemed sufficiently large to afford us an opportunity to detect diversity in security cultures, while at the same time keeping the scope of the study to a manageable size. The accounting profession was chosen because its work requires compliance with specific rules and policies, such as those specified by the Generally Accepted Accounting Principles (GAAP) and the Sarbanes-Oxley Act. Additionally, accounting data includes confidential organizational and client information, and must therefore be handled securely. The human relations (HR) profession was chosen because it has the primary responsibility for handling confidential employee information, which is subject to various laws, such as the Equal Employment Opportunity (EEO) Act, the Americans with Disabilities Act (ADA), and the Health Insurance Portability and Accountability Act (HIPAA). The marketing profession was chosen because of the general perception that marketers are relatively less likely to be concerned about information security. For example, Puhakainen and Siponen [2010] conducted an action research study in an organization to improve employee compliance through information

systems security training. In assessing the effectiveness of the training initiative, the researchers recorded "four issues that still needed to be addressed," of which the first one was "The *sales team* [our italics] in particular still took advantage of the permitted exceptions to e-mail encryption" [p, 770]. Such a finding is an exemplar of the relatively lower level of concern about information security among marketing personnel. The information systems profession was chosen because of the general perception that it is responsible for information security.

Respondents were recruited on the basis of their current full time work experience or prior full time work experience in their respective professions. At the time of data gathering, they were enrolled as graduate students at a large public university in the United States of America. Demographics of the respondent pools for each profession are shown in Table 4. The respondents for each profession were from different organizations. Thus, any cultural commonality that is identified can be attributed more to professional influences than to organizational influences.

**Table 4: Demographics of Respondents**

| | IS professionals | Marketing professionals | HR professionals | Accounting professionals |
|---|---|---|---|---|
| No. of respondents | 12 | 7 | 7 | 11 |
| Male:female ratio | 4:1 | 5:2 | 1:6 | 3:8 |
| Age range (years) | 23–45 | 21–43 | 24–37 | 22–55 |
| Experience (years) | 2–25 | 1.5–20 | 1–14 | 3 months–30 |
| Job titles (examples) | Programmers, network admin., database admin., Web developers. | Marketing research analyst, retailer, marketing assistant, property manager. | HR representative, compensation analyst, recruiter. | Staff accountant, tax accountant, auditor, public accountant. |
| Association with profession | Members of IS professional associations like ACM, ISSA, ISC2, and so on, and attended professional conferences. | Attended professional conferences, referred to professional websites and forums, constantly interacted with members of their profession. | Members of HR professional associations like SHRM, AMA-HR, Society of Training & Development, and so on, and attended professional conferences. | Members of accounting professional associations like AAA, attended professional conferences, and referred to professional websites. |

## Data Collection

The data collection method used in the current study was semi-structured, face-to-face interviews to elicit the beliefs underlying the information security culture. As we have mentioned earlier, we use the term "beliefs" broadly to refer to responses on values, beliefs, assumptions, and so on; based on prior research, these are usually considered sufficient to characterize culture. The structured questions were generated based on the issues related to the categories identified in the theoretical framework (see Tables 2 and 3 for issues on which interview questions are based). A detailed interview guide (see Appendix A) was prepared. The guide consists of questions for inclusion during the interview. In some cases, the issue listed in the table is already in the form of a question. In other cases, the issue was expanded into more than one question in the interview guide.

The follow-up unstructured questions were aimed at eliciting clarifications, details, and richness. Responses from interviewees were not limited in any way. The interviews focused on identifying the following three sets of beliefs—beliefs about their identity of the profession, general beliefs, and beliefs about information security. Respondents were asked questions only about their profession (e.g., accountants were asked about the beliefs of the accounting profession only). A sample of the questions used in the study is shown in Table 5.

The unit of analysis for the study is the professional group level, so the respondents were asked to state their respective professional group's beliefs and behaviors, not their own personal beliefs and behaviors. Toward the end of the interviews, respondents were allowed to also ask questions and add comments.

The interviews were conducted over a period of three months. Interviews were recorded and transcribed. In addition to the transcription, additional notes were taken during the course of the interview and were also made after the interview. Following every interview, the recordings were reviewed to ensure proper preparation for subsequent interviews.

| Table 5: Sample Questions Used in Interviews | |
|---|---|
| Category | Sample questions[2] |
| Membership in profession | What profession do you consider yourself to be a part of?<br>To what extent do you participate in activities or groups associated with your profession?<br>Do you attend professional group meetings, gatherings, or conferences? |
| Identity: | |
| Core value of profession | What would your profession's members say the values of your profession are? |
| Role of profession | What do members of your profession believe is the primary role of their profession? |
| Contribution to organization/ society | If you had to describe what your profession contributes to society, what would you say? |
| General beliefs: | |
| Beliefs about risks | Generally speaking, how do members of your profession feel toward risk-taking? |
| Beliefs about complying with rules and procedures | Among the members of your profession, what is the general belief about abiding by rules and procedures? |
| Beliefs about organizational hierarchy and complying with managerial guidance | Do members of your profession subscribe to the idea of hierarchy?<br>What would the response of members of your profession be if upper management tried to specify details on how to do the task? |
| Beliefs about information security: | |
| What is information security? | Can you describe what the term "information security" or "IS security" means to members of your profession? |
| Who is responsible for information security? | Who do the members of your profession think should be responsible for information security? |
| What role does group play in ensuring security? | What role do the members of your profession think they play with respect to information security? |
| Beliefs about taking security risks | Do members of your profession believe in taking information security-related risks? |
| Beliefs about taking security risks under performance pressure | How do members of your profession handle choices/trade-offs between getting the job done and information security measures? |

It would be appropriate to mention that a pilot study with twelve respondents from diverse professions was conducted. Pilot studies help the researchers get familiar with the phenomenon of interest and test the questions. The pilot study indicated no major problem with the interview scheme.

## Analytical Procedures

The interviews were transcribed, identifying information removed and coded. The Qualitative Data Analysis (QDA) software Atlas.ti was used to code the transcripts. A total of thirty-nine codes were generated. A sample of the codes is shown in Table 6.[3] In qualitative studies, coding is part of the analysis process—"coding is analysis" [Miles and Huberman, 1994, p. 56]. Thus, the first author was the primary coder. To ensure the reliability of the coding process, we followed procedures used in Pare [1995]. An external coder is provided with a list of codes, an explanation of each code, and a sample chunk for each code. The external coder is instructed to use the list to become familiar with the codes. Then the external coder is provided with a test set of textual chunks from the interviews. The external coder and the researcher code these chunks independent of each other. Intercoder reliability is calculated using Holsti's code of reliability (CR) [Holsti, 1969]. The formula for calculating the coefficient of reliability is CR = 2M/(N1 + N2), where M = number of coding decisions on which the coders agreed, and N1 and N2 are the number of coding decisions made by the first and second coders, respectively. The coefficient of reliability for the test set was 0.83. The external coder and the researcher discussed the codes on which the two disagreed. On the basis of the discussion, the researcher was able to confirm his understanding of the code or correct his understanding of the code for further coding of the remaining transcripts. Inter-rater reliability was checked only once. It can also be seen that the inter-rater reliability was done for the overall coding scheme and not for individual codes.

[2] The full list of questions is included in Appendix A.
[3] The full set of codes with number of instances and sample segments are shown in Appendix B.

| Table 6: Sample of Codes | |
|---|---|
| Description of individual codes | Codes |
| Beliefs about taking risks | Bel_Risk |
| Beliefs about complying with hierarchy in organizations | Bel_Comp_Hier |
| Beliefs about complying with rules and procedures | Bel_Comply_Rules |
| Beliefs about amount of responsibility generally preferred | Bel_Pref_Responsibility |
| Beliefs about taking information security risks | Bel_InfoSec_Risks |
| Beliefs about taking information security risks, when taking such risks could help them in getting their jobs done and improve their efficiency or productivity. | Bel_InfoSec_Risk_Job_Done |
| Beliefs about amount of responsibility preferred on information security issues | Bel_Pref_InfoSec_Responsibility |
| Beliefs about the role members of their profession play in information security | Bel_Role_in_InfoSec |
| Beliefs about who is responsible for information security issues in organization | Bel_InfoSec_Responsibility_is |
| Beliefs about the connection between information security and productivity | Bel_InfoSec_Prod_Cnx |

Next, the process of generating a narrative is described. The software package (Atlas.ti) was used to extract clusters of quotes associated with one code from the interview transcripts. Sample responses for one cluster, "Who do IT professionals think is responsible for information security in an organization?" are shown in Table 7. Brief notes are made, and a summary of beliefs surfacing from the responses are noted. In Table 8, the development of a small part of the narrative from the summaries associated with three different codes is shown. A preliminary structure for a narrative fragment that could be generated from these summaries was first decided upon. Then the actual narrative fragment was developed. Using this process, the narrative shown in the results section was developed.

| Table 7: Sample Responses and Summary Notes for One Code | |
|---|---|
| Sample of responses and summary notes: Who do IT professionals think is responsible for information security in an organization? (Code: Bel_InfoSec_Responsibility_is) | |
| Question | Response |
| Who do IT professionals think is responsible for information security within organizations? | P3: IT professionals |
| Who do IT professionals think is responsible for information security within organizations? | P4: IT professionals |
| Who do IT professionals think is responsible for information security within organizations? | P5: Everybody |
| Who do IT professionals think is responsible for information security within organizations? | P6: Themselves [IT professionals] |
| Who do IT professionals think is responsible for information security within organizations? | P7: CIO at the very end. But, it comes down to IT professionals themselves including the security staff and IT professionals that you have. |
| Who do IT professionals think is responsible for information security within organizations? | P11: The trend today is that you have an actual security team. |
| What if they don't have an actual one? | P11: Whoever they happen to have working in IT, if they don't have a security team. But, most large organizations have a security team. |
| Notes for "Who do IT professionals think is responsible for information security within organizations?" | |
| Keywords/phrases | Individuals mentioned: IT professionals; security teams; CIO; everybody. |
| Summary | The primary belief is that IT professionals are responsible for security. A couple of respondents believed that the security team should be responsible. One or two respondents stated that management or the CIO is ultimately responsible for security. Only one respondent viewed information security as everyone's responsibility. |

The narratives generated following this systematic process are used to create segments of the descriptive characterization of the information security cultures of the four professions. The descriptions are presented in the next section on results. The empirical basis or empirical support for the descriptions are the narratives generated. The quotes included are exemplars to illustrate issues, and are not meant to be the sole basis on which the descriptions are developed.

| Table 8: Generation of Narrative from Summaries | |
|---|---|
| Development of narrative from summary notes for multiple codes | |
| Notes for "Who do IT professionals think is responsible for information security within organizations?" | |
| Individuals mentioned | IT professionals, security teams, CIO, everybody |
| Summary | The primary belief is that IT professionals are responsible for security. A couple of respondents believed that the security team should be responsible. One or two respondents stated that management or the CIO is ultimately responsible for security. Only one respondent viewed information security as everyone's responsibility. |
| Notes for "What does the term 'information security' mean for IT professionals?" | |
| Key phrases from responses | Protecting data, keeping it from going public, protection from hackers. Making sure data is not tampered with.<br>Protecting technology resources: network, infrastructure, networks, computer systems, and applications.<br>Securing lines of transmission |
| Summary | IT professionals view information security as protecting data and the technology resources, which include: computers, networks, and applications. |
| Notes for "What activities/issues do IT professionals associate with information security?" | |
| Keywords/phrases from responses | Planning, passwords, encryption, rules and procedures, audits.<br>Passwords, physical security, authorized access.<br>Intrusion detection, role-based access, passwords; confidentiality, integrity, availability. |
| Summary | IT professionals associate technical issues and activities with information security, such as intrusion detection, passwords, encryption, and role-based access. They acknowledge the need for higher level managerial activities, such as planning, and development of rules and procedures to guide the technical activities. |
| Preliminary structure for narrative | IS professionals view information security as protection of information and information infrastructure. Activities associated with information security—passwords, encryption, and so on, as well as planning and development of rules and policies. They view themselves as responsible for security. |
| Narrative generated from these summaries[4] | IS professionals view information security primarily in terms of safeguarding the information residing in the information technology infrastructure, which includes the computers, networks, and the software applications. Some of the tools that they associate with information security include passwords, intrusion detection systems, firewalls, and role-based access control systems. Thus, it would appear that they view information security primarily as a technical problem. This, presumably, leads to the belief that the IS group is and should be the group responsible for information security in organizations. They believe that members of other professional groups, such as accounting, marketing and human relations, view IS professionals as responsible for security, a charge that they feel capable of fulfilling. IS professionals further believe that while management may have the ultimate responsibility for security, it is the responsibility of the IS group to guide management on security issues, both by educating managers and by proposing security initiatives. They also believe that they are responsible for developing security policies and implementing them. Further, IS professionals believe that they are aware of security issues (i.e., what the dangers are and how to minimize them). |

## V. RESULTS

Our focus was on identifying and examining the security cultures of different professions. This section examines the identities, general beliefs, and security-related beliefs of each of the four different professional groups. This is followed by a brief comparison of the information security cultures of the four professional groups. The information security culture of a group is viewed as the security-related beliefs taken in conjunction with the group's beliefs about its identity and its general beliefs about risk and compliance.

### Identities of Professions

The identity of a professional group is its perception of itself, formed from its core values, and its perception of the profession's contribution to society and organizations. In our study, the core values of the different groups have

[4] This narrative is part of the description of the Security Beliefs of IS Professionals in the body of the article.

common threads, including honesty, integrity, and service to the organization and society. However, each group's perception of its role within an organization is quite distinct. The role is embodied in their belief that they bridge the organization and another entity, that entity being related to their special area of expertise.

### Identity of Accounting Professionals

Accountants believe that their role is to ensure the validity and accuracy of financial statements of organizations, and to keep track of money and other assets in organizations. They view themselves as the bridge between principals (the shareholders) and agents (the managers). To quote one respondent:

> *"They* [accounting professionals] *are the people that assure the correctness of financial statements. They are the people that say the financial statements are correct. They play a big role between the principals which are shareholders and the agents which are the managers. They are the middle man between them i.e. to make sure that this is your money and this is what is being done with your money."*

Accountants further believe that their work contributes to the efficiency and profitability of organizations. The accounting and financial reports that they produce are used to assist the organizations in making decisions on budget allocations, predicting future performance, and ensuring compliance with regulations. Valid accounting data leads to good decisions, which in turn lead to efficiency and profitability. In the words of one respondent:

> *"Because that* [financial reports] *is what all the other departments will utilize when making decisions about the firm, if they should invest in the project or discontinue a line."*

Accounting professionals believe that they play an integral part in the protection of the wealth of people in society. When queried about the contribution that accountants make to society, one of the respondents with three decades of experience in the profession put it this way:

> *"Sort of like 'A guard at the door'. We* [accounting professionals] *offer an area of security, confidence to the users of the financial information. Accountants are a form of security to the users of financial information."*

Accounting scandals have reinforced the belief that there is a need to uphold their core values even in the event of conflict with management. They believe that the emphasis on core accounting values is higher today than before the notable corporate accounting scandals (e.g., Enron, Worldcom) when corporate values clouded the accounting profession's values of integrity and accuracy. Respondents noted that corporate accounting scandals have resulted in regulatory standards and penalties for not upholding the values of the profession.

### Identity of HR Professionals

HR professionals mediate the relationship between the organization and its employees. On one hand, they believe they maximized the value of the organization by aligning employees with the strategic direction of the organization.

> "[the core value of HR professionals is] *to achieve the strategic objectives of the organization through the accomplishments of people and so, the alliance would be first with strategic intent, and, then aligning the people vertically and horizontally with what direction the company wants to go."*

They provide support to the strategic goals of the organization by playing an active role in the recruitment, development, and retention of employees.

> *"Developing people, celebrating their success and working with them to improve their shortcomings."*

On the other hand, they view themselves as champions of the employees, ensuring equal treatment of all employees, and advocating for their causes, which sometimes involve standing up to management on behalf of employees. One HR manager said:

> *"You know we always have to fight different things for employees and managers. That fight means bringing up the issues to the management, providing support, going outside and doing research and saying this is why we have to do this."*

They also viewed their role as ensuring that the organization complied with federal and state laws and internal policies.

While professing that the core values are very important to them, HR professionals were clear on how they would respond to a conflict between the values of their profession and the values of the organization. For issues related to legal procedures and laws, they would stand up for the values of the profession, even when doing so may entail their job. However, for other issues, they would concede to management. In the words of one recruiter:

> *"They* [HR professionals] *are going to go with the values of the organization. Because, that gives them their bread and butter. Unless against the law that would be an exception."*

In effect, HR professionals view themselves as the mediators between an organization and its employees, trying to help the organization gain the maximum from its employees, while simultaneously ensuring that employee rights and privileges are not ignored.

### Identity of Marketing Professionals

Marketing professionals view themselves as the group that bridges an organization and its customers. They believe that they provide value by enabling organizations to understand the market and the customers, and by effectively disseminating information about the organizations' products to the market. To quote one marketing research analyst on the issue of helping organizations understand customers,

> *"They* [marketing professionals] *play a major role overall in the organization because, if the organization did not know who their customer is then they wouldn't know what to sell."*

Marketing professionals believe that they play the critical role of bringing information about products to those who need it (including organizations and consumers) and of enabling them to make informed decisions about the products. In the words of one of the respondents with sales and advertising experience from the pharmaceutical industry:

> *"..it* [marketing profession] *brings information to consumers that otherwise may not have been conveyed. Because, marketing basically brings out information to those who need it about new products."*

They view this role as important because they believe that society as a whole lacks the ability to pursue relevant information about products and services available, because of information overload.

Thus, the marketing professionals have the identity of meeting societal needs for products by informing the organization of the consumer needs and the consumer of products available from the organization.

### Identity of IS Professionals

IS professionals view information systems as a key factor in making organizations more efficient and effective. They view their role as helping organizations and society derive the benefits of using information technology. In this role, they believe that it is their charge to develop and maintain the technical infrastructure and solve user problems. The solutions to the complex problems associated with these tasks demand that IS professionals be innovative. Thus, their primary identity is that of an innovative group dedicated to the task of making society and organizations more efficient and effective through the use of information technology. An illustrative quote:

> *"[Information Systems] Delivers the infrastructure that our culture or society has grown to depend upon. If you removed all the technology it will be back to Stone Age exactly. So, as a society we have grown to depend on the technology. The IT* [information technology] *professionals themselves are the ones that continue to develop and implement that technology. Quality of living ultimately depends on IT professionals who continue to keep up our quality of living."*

While they see themselves as the primary personnel who are experts in the realm of technology, they recognize their role has to be relevant to organizations. In this context, they encounter conflicts between their views and that of other groups, either users or managers. In such situations of conflict, they are reluctant to surrender technology-related decisions to others. They will assert their viewpoints, almost to the point of appearing recalcitrant. But they recognize that managers bear the ultimate responsibility for the well being of the organization. Hence, once they believe that the managers have heard and taken their views about technology into consideration, they will concede to managers. In short, when there are conflicts between the values of the IS personnel and those of the organization, IS personnel will ultimately fall in line with organizational values. To quote one respondent:

> *"I would say that the values of the organization win over. Because its [IT professional's] whole goal is to support the overall organization. So, I would say IT would have to bow down to organization."*

In effect, IS professionals view themselves as the technical experts who help an organization realize the benefits of technology.

### Summary of Identity of Professions

The interviews indicate that members of the Accounting and HR professions are focused on control functions. Accountants are bound by the rules governing accounting practices, and they exert control over others by demanding behavioral compliance with the rules. Similarly, HR professionals are bound by rules and regulations from federal and state agencies, and they exert control over the other groups in the organization by demanding compliance with employee-related regulations. In contrast, IS and marketing professionals identify more with productivity responsibilities. IS professionals view their role as increasing organizational efficiency and effectiveness by leveraging information systems and technology. Marketing professionals view their role as facilitating two-way traffic between the organization and its customers, engaging in activities that increase sales and profitability.

## General Beliefs of Professions

The general beliefs of interest to us are beliefs of professionals about risk, compliance with rules and procedures, and the importance or relevance of hierarchy and managerial guidance. We consider these relevant because groups with a proclivity toward risk-taking are also likely to take chances with security. Similarly, security safeguards are enhanced by formulating policies and procedures that employees must observe. A group that fails to observe rules and regulations, in general, may be more likely to transgress rules and regulations related to security. Finally, beliefs about hierarchy and managerial guidance provide a basis for expectations regarding how groups may react to security-related managerial initiatives.

### General Beliefs of Accounting and HR Professionals

The general beliefs of the accounting professionals and HR professionals are very similar, so they are discussed together. Both professions are rooted in rules and regulations. In the accounting profession, the Generally Accepted Accounting Principles (GAAP) provide the framework for preparing financial statements. Professional associations such as the American Accounting Association (AAA) and the American Institute of Certified Public Accountants (AICPA) have published codes of ethics. The passage of the Sarbanes-Oxley Act has further defined expectations of accounting professionals. Collectively, the internal standards, code of ethics, and laws governing accounting place a strong demand on accounting professionals to comply with rules and regulations.

> Accounting professional:[5] *"I think they* [accounting professionals] *are more and more familiar with it* [ethics and rules]*. Not to say that they were not but, it is getting more …After Sarbanes and Oxley, it has been really emphasized in the accounting world and the accounting profession. If you are really on the job, you would be really careful about things like that."*

HR professionals are likewise bound by organizational policies, as well as federal and state regulations governing treatment of employees.

> HR professional: "*Because a lot of the rules that are in place in HR [are] not like 'Oh you can take a short cut and get away with it'. It's like this is the rule and you know its legality."*

This need to be in compliance with laws and regulations appears to extend to other rules and procedures that may exist. Accountants see legal liabilities involved with taking risks, feel the need to take personal responsibility for actions, and believe that in the accounting profession there is much to lose by taking risks, thus making them a conservative group, overall.

> Accounting professional: "*They* [accounting professionals] *are very skeptical towards taking risk because the underlying principle for accountants is conservatism. If you are ever skeptical about an event or transaction or you feel that it is a risk then you lean more towards conservatism."*

HR professionals, with a few exceptions, identified themselves as a *"risk-averse group."* They attributed their risk aversion to the expectation of their job and profession to be compliant to various rules, regulations, and procedures, and the eventual risk of litigation. To cite one of the respondents:

> HR professional: "*I would say that they are risk averse. Because a large part of our job is to ensure that the organization and employees are meeting certain regulations, certain standards set by the federal state local governments. So, we are in the mode of compliance. So, taking risk is kind of going outside of that."*

[5] We have explicitly identified the profession of the respondent in some instances to avoid confusion.

Accountants further extend their risk-aversion to other beliefs that reduce organizational risk. Their work revolves around financial data. Accuracy of such data is critical, and thus they consider it advisable to verify work done at levels below them. This is consistent with their beliefs about the need for hierarchy in organizations, which delineates responsibilities and allows for managerial guidance and supervision. But managerial guidance is expected to be consistent with professional guidelines.

The beliefs of HR professionals on the issue of hierarchy are best reflected in the group's view that they are the keepers of organizational charts.

> HR professional: *"In my experience, you know, HR people are pretty quick to, you know, bring out the organization chart to show, you know, here is where you are and here is where your boss is and here is how your boss fits in to the hierarchy above you. All these organizations that I worked for was very hierarchical in nature. There was an emphasis of you always knowing your place in the machine."*

Their acceptance of a hierarchy is consistent with their willingness to comply with managerial directives. When they disagree with managers, they will express the disagreement, but comply when directed to do so. To cite one of the respondents on this issue:

> HR professional: *"They are going to share their perspectives on the issue. But, at the end of the day they are going to do what they are told to do."*

Thus, accountants and HR professionals present a coherent picture in their beliefs related to risks, rules, and regulations, as well as the need for hierarchy. They believe in minimizing risk and complying with rules and regulations. They believe that a hierarchical structure is necessary for the orderly functioning of a system.

### General Beliefs of Marketing Professionals

Marketing professionals present a consistent picture of a group more prone to taking risks, with a lower regard for rules, and a relatively lower level of concern for managerial directives. They view taking risks as important to their success.

> *"Generally they* [marketing professionals] *would think that 'There's nothing to gain if you don't take risk' so, they are above average in terms of taking risks."*

Consistent with that, marketing professionals will circumvent rules when necessary. Marketing professionals view rules and procedures as guidelines rather than inflexible directives. Marketing professionals reserve the right to bend the rules, and do so, when the rules are time consuming, or problematic, or impede the flexibility of their work schedules. In the words of one of the respondents:

> *"They* [marketing professionals] *see rules and procedures as guidelines as they can be bent a little… and if there is a loophole you can go through it. But, if it is not bendable or a loophole they will not do it."*

Marketing professionals further seem to believe that supervision and reporting requirements are not the road to success.

> *"It* [what marketing professionals expect from management] *is more like 'When there is a problem I will call you or ask you. In the mean time tell me I am doing a great job.'"*

Overwhelmingly, marketing professionals want very little influence from management. They believe that managers should provide high level guidance and allow the marketing professionals to decide on the details of how to get the work done.

> *"You [management] do not have to tell us [marketing professionals]. [I'd] rather have you guide me through the process than … you tell me what to do. Unless I ask you or I do not know what … it is."*

This belief stems from the feeling that non-marketing managers do not have adequate marketing expertise, and should therefore stick to what they know best (i.e., management). There is also the associated fear that managerial involvement will curtail the freedom necessary to get their job done. Further, they believe that influence from management may also skew the outcome of their work. In the words of one marketing researcher,

> *"Very little* [influence from management]*. From [a marketer's] perspective they are trying to produce data for these managers to answer, to make the decision. Sometimes they get too involved, they*

*kind of skew that data or kind of push the answer or the question to another question, when you are trying to work on this question."*

Marketing professionals believe that a hands-off style of management will foster creativity and provide an environment where they can perform effectively.

Overall, marketing professionals come across as willing to take chances, ignoring rules when possible, and wanting to assert their independence at every chance.

### General Beliefs of IS Professionals

IS professionals present a somewhat confused picture. They believe that they are risk averse. Their risk aversion stems from the belief that organizations are highly dependent on information systems. Quote from a respondent:

> *"IT professionals are generally averse to risk because they are charged with maintaining the organization's information resources, and, they can't afford risk because if they take a risk and information resources are compromised, there is no way to get it back. So, the potential loss is too high and they don't want to take risk."*

This conservative view applies to the maintenance of the technical infrastructure, as well as the day-to-day operations of the technology. On the other hand, the frequent changes in technology present risks related to the choice of new technologies to adopt, and timing risks related to when to upgrade to or adopt new technologies. In such situations, a certain degree of risk is unavoidable. In this case, their attitudes became:

> *"They would think risk is part of IT and specifically software development. I think they believe that it has to be managed."*

Given their primary belief about being risk averse, surprisingly, IS professionals are reluctant followers of rules. They concede the need for rules and procedures, but tend to question them frequently. In particular, they seem to believe that rules with respect to information systems are for others and not for themselves.

> *"They* [IS professionals] *will be happy to make rules and procedures but, following other people's rules and procedures would probably be seen by them as stupid sometimes."*

Their beliefs about managers and hierarchy are consistent with their reluctant observance of rules and regulations. IS professionals believe that managers should provide broad goals and facilitate access to resources. Other than that, they believe that IS professionals should have the freedom to accomplish tasks without micromanagement.

Thus, IS professionals present a mixed picture. The group recognizes the criticality of the information infrastructure and routine processing under their charge, causing them to be risk averse. On other fronts, their beliefs reflect a group that wants independence, without being shackled by rules or managerial directives.

### Summary of General Beliefs of Professions

Our analysis indicates that accounting and HR professionals are risk averse and rule compliant, and believe strongly in the role of hierarchy and managerial initiatives. Marketing professionals came across as almost rebellious—believing that their success as marketers depended on their willingness to take risks, that rules can be bent when necessary, and that managers should help when called upon, but otherwise stay away. IS professionals are schizophrenic: risk averse on basic functions, but risk tolerant when it comes to new technology. They believe in the value of rules for others, but do not see the need to follow them themselves ("do as I say, not as I do"). They acknowledged the need for hierarchy, but saw a limited role for managerial directives.

In terms of general beliefs, accountants and HR professionals are at one end of a "general beliefs" spectrum (beliefs about risk, compliance with rules and procedures, and the importance of hierarchy), with marketing at the other end. Accountants and HR professionals are conservative, compliant with rules, and desirous of an organized structure with clear delineation of responsibilities. Marketing professionals believe in taking risks, circumventing rules, and asserting their independence, all in the search for success. IS professionals fall between these two extremes, believing it necessary to be risk averse in discharging their duties with respect to the information infrastructure, but otherwise wanting to be independent of rules and managerial guidance.

## Security-Related Beliefs

The security-related beliefs of relevance are: what is information security, who is responsible for it, what role does the group play in ensuring security, what is their awareness of security issues, what is their propensity to take security risks in general, and what is their propensity to take security risks under performance pressure?

### Security Beliefs of Accounting Profession

Respondents from accounting pointed out that professional associations, like the American Accounting Association and the American Institute of Certified Public Accountants (AICPA), provide courses, seminars, workshops, online self-study courses, and training on information security issues. This education may account for the fact that accountants have the most comprehensive view of information security. They view it as including the safeguarding of all the information in the organization, along with the associated information infrastructure. This encompasses accounting information, sales information, employee information, and so on. Infrastructure protection includes actions like locking server rooms, protection of physical files, and restricting access to other sensitive areas and material. The following quotes, first from a respondent who has worked as a staff accountant, and then from a respondent who has worked as an external auditor, highlight this.

> Respondent 1: "[For an accounting professional, the definition of Information Security means] *Protection of the company's information that is internal information.* [company's internal information refers to] *Any of the company's internal information, any of the accounting, all the sales data, the customer's information."*
>
> Respondent 2: *"From one standpoint it would be the information that I have gotten from my client that it is secured from passing on [to] somebody else. The information that I have in my company files is secured from passing on to anybody outside such as…."*

Consistent with this, they believed that all employees and departments shared the responsibility for information security in the organization. However, a few of the accounting respondents went on to state that IS professionals had a special responsibility to take the lead on security issues, and that accountants had a special responsibility with respect to accounting information.

Accountants were fairly cognizant of information security risks. They were firm in their belief that they would not violate security procedures. Their mindset was to observe rules.

> *"Their* [accounting professionals] *belief is that even the non-accounting related rules and procedures are still meant to protect their own work.* [They would follow non-accounting rules and procedures] *to the full extent."*

Their willingness to follow rules and their cognizance of security issues makes them unwilling to violate security rules, even in the pursuit of performance.

> *"I think it depends on what the risk is. I think in every profession, there is cost benefit and so, I think you weigh the risk of breach of security with, you know, the benefit of doing it. So, would I say never No…I wouldn't say we would never ever breach that. But I would say that we are fairly conservative about wanting to ever breach that."*

This tendency is further reinforced by the enactment of laws related to privacy and confidentiality. Certain nuances are worth noting. While security rules are observed, beliefs favor productivity when no rule exists. Also, while they have strong beliefs about observing security rules, they are not above circumventing those rules at times.

> *"You took your laptop wherever you went. We had several instances reporting that the laptops were stolen. I took mine when I was on vacations."*

Overall, accounting professionals have a good deal of knowledge about information security issues. They are willing to accept responsibility for keeping information secure, and treat security tasks on par with their accounting tasks. The profession is based on standards and rules, and encourages a conservative mindset. The willingness to comply with rules aligns well with the beliefs and behaviors necessary to enhance security. Thus, the accounting profession presents a strong security culture oriented toward the protection of information assets in organizations.

### Security Beliefs of HR Professionals

HR professionals indicated that their beliefs about information security come more from within the organizations that they work for than the profession itself. Their belief about information security is limited to the protection of information pertaining to employee records.

> *"For the most part it* [information security for HR professionals] *relates to employee management i.e. making sure that every aspect of [the] employee file is kept confidential and only certain individuals have access to various levels of information such as social security numbers, birthdays, marital status [and] things like that."*

In addition to their own role in keeping such information safe, they believed it was necessary to communicate to other employees the importance of keeping such information secure and confidential. Their awareness of information security risks was limited. While accepting the major responsibility for keeping employee information secure, almost all respondents in the study said they believed that it is the responsibility of IS professionals to ensure information security as a whole within organizations.

In line with their reluctance to take risks in general as part of their job, HR professionals had strong beliefs about not taking information security risks. To quote a compensation analyst:

> *"I do not think that they [HR professionals] would take that risk for two reasons. 1. Because of their code of ethics and their general way of being risk averse, and, 2. I don't think they would know how to do it because, we don't understand information technology."*

When it came to rule compliance, HR professionals did not make a distinction between general rules and procedures and specific rules and procedures for security. They believed it was necessary to comply with all sets of rules.

> *"…in general I think there is a strong sense of responsibility in obligation just to follow all the rules and procedures. Because, we* [HR professionals] *know there is a reason for them. A lot of times we are enforcing a lot of reporting deadlines and rules, procedures, and, people don't understand them. So, we are always having to communicate the reason why—if it's state, federal, or local laws. So, there is a general awareness and kind of this tendency to comply and follow along with the rules."*

Their general belief in observing rules and regulations extends to their willingness to observe security rules and regulations. HR professionals also admitted that their lack of expertise in the area of security was part of the reason for their willingness to follow security rules unquestioningly. For similar reasons, they were willing to comply with managerial directives about security.

> *"They* [HR professionals] *would give 100% weight* [to managerial directives]*. If it's not your domain or you know nothing about it and if the management does, then you listen to them."*

HR professionals, similar to their accounting counterparts, are subject to privacy and confidentiality laws. This reinforces their tendency to comply with rules. It also inhibits any tendency to violate security under performance pressure. But subtle exceptions to this are acknowledged.

> *"I* [HR professional] *have to get a notification because, [if] a kid is very badly hurt and he needs medical assistance then, I am not going to care about security. Those are high pressure situations for me that are very, very unique."*

Overall, HR professionals are a rule-compliant group, who are risk averse and follow managerial directives on all issues including security issues. They believe it is necessary to avoid violating security policies even under performance pressure except under extreme circumstances. HR professionals have strong beliefs about their role in and responsibility for maintaining the security of confidential information about employees. However, the same beliefs do not clearly extend to all aspects of security, or other types of information. In particular, while they accept the responsibility for the security of employee information, they believe that the responsibility for overall information security lies with information system professionals. HR professionals' beliefs of information security are less holistic than that of the accounting professionals. But they seem to be strongly rooted in the concept of abiding by rules, including those related to security, even in situations of high performance pressure. Thus, it would appear that their contribution to the protection of information assets can be equally effective.

### Security Beliefs of Marketing Professionals

Marketing professionals said that most of their knowledge about security came from within the organization, little from outside. They have a very limited perspective on information security. Marketing professionals viewed information security as the protection of three types of information: (1) confidential information pertaining to products that they market, (2) confidential information about clients for whom they market the products, and (3) information about customers to whom they market the products. The protection of confidential information about the products is considered part of their responsibility to safeguard the intellectual knowledge of the organization that they work for.

The protection of confidential information about clients (organizations for whom they market the product) and customers (individuals or organizations that buy the product) is considered necessary to maintain the trust of the clients and customers. As one of the respondents with experience in advertising puts it:

> *"Well, in order to segment, target position or perform other marketing activities we need to know names, addresses or sometimes personal information if it is internal, purchasing experiences. So, it's [a] lot of information that the customers would not be happy if someone else got their hands on…."*

They also understood that they should protect their computers (although their concept of protecting their computer was primarily limited to "don't lose your laptop") and not give out their passwords. They considered all other aspects of information security as the responsibility of senior management and IS professionals.

> *"The IT department* [is responsible for information security issues in organizations]*… Because, we* [marketing professionals] *perceive ourselves being experts in duties that we perform. In the same line we view information security as information technology…within their domain."*

Marketing professionals do not believe in taking information security risks, in contrast to their willingness to take other forms of risks. This belief is rooted in the knowledge of the importance of information they possess, the importance of ensuring the confidentiality of that information, and the consequences of not ensuring the confidentiality of the information. Further, marketing professionals accept that there are issues of information security that they do not understand, making it more dangerous to take chances. A quote from a respondent:

> "[taking information security risks] *That is different. Because, that is not like being risky on your own terms. That is being risky with company security and you do not want to do that. So, I probably think they wouldn't be as comfortable as being risky with that kind of information."*

This translated to a willingness to observe security regulations. Once again, this willingness is primarily rooted in their lack of knowledge about security.

> *"I think there isn't a lot that they* [marketing professionals] *could do about it. I think they would be much more accepting. I don't think we really have a lot of understanding about some other departments."*

But marketing professionals acknowledge that, under performance pressure, performance would take precedence.

> *"It would be just getting the job done first of all. Because, you know information security really does not impact their job. It is not their* [marketing professionals'] *responsibility."*

Overall, marketing professionals seem to have minimal knowledge or awareness about security. They view security as the responsibility of others, and their only concession appears to be a willingness to observe security rules. But this also seems a limited willingness, based on their perspective that performance needs should take precedence over security.

### Security Beliefs of IS Professionals

IS professionals receive most of their security-related knowledge from professional sources. In particular, they did not view either the organization or the online and print media as a useful source. These sources were considered reactive, and thus failed to provide relevant information in a timely manner. In fact, IS professionals believed that their group educates senior management on security issues and develops security initiatives, policies, and procedures.

IS professionals view information security primarily in terms of safeguarding the information residing in the information technology infrastructure, which includes the computers, networks, and the software applications. Some of the tools that they associate with information security include passwords, intrusion detection systems, firewalls, and role-based access control systems. Thus, it would appear that they view information security primarily as a technical problem. This, presumably, leads to the belief that the IS group is and should be the group responsible for information security in organizations. They believe that members of other professional groups, such as accounting, marketing, and human relations, view IS professionals as responsible for security, a charge that they feel capable of fulfilling. IS professionals further believe that while management may have the ultimate responsibility for security, it is the responsibility of the IS group to guide management on security issues, both by educating managers and by proposing security initiatives. They also believe that they are responsible for developing security policies and implementing them. Further, IS professionals believe that they are aware of security issues (i.e., what the dangers are and how to minimize them).

Consistent with their beliefs about the importance of security in organizations, they express an unwillingness to take security risks or violate meaningful security rules and regulations. Violations of rules have serious consequences, including the possibility of being dismissed from the job. However, such attitudes toward compliance are challenged when the group is confronted with the need to meet productivity or performance objectives. Most of the respondents in our study indicated that IS professionals strongly believed that security and productivity issues could be at odds with each other. When the respondents were specifically asked how IS professionals handle trade-offs between getting the job done and information security issues, most of them said that getting the job done will come first, and security issues will take a back seat. The reasons IS professionals provide for the emphasis on job demands over security include pressure from the management to be productive, and their belief that they get paid for getting their job done, not for taking care of security issues within the organization.

> *"I think, in the end, if they* [IS professionals] *had to choose between the two, they would get the job done. Because that's what they get paid for, that's their job, task and its number one."*

In sum, IS professionals exhibit an awareness of the technical aspects of information security, and claim a leadership role in IS information security issues. They seem willing to observe security rules because of the risks associated with violating them, but their stand changes when faced with the choice between security and performance. Thus, in spite of their belief that they have superior knowledge about security issues, they are vulnerable to the demands of performance.

### Summary of Information Security Beliefs

Currently, accounting professionals express a set of beliefs that are most reflective of a strong security culture. HR professionals were not quite as holistic as accountants in their beliefs about what information security is, and who is responsible for it. Further, their awareness of security risks seemed less comprehensive than that of IS professionals. However, IS professionals appeared more likely to pursue productivity at the expense of security. Marketing professionals believed that their role in security was limited to safeguarding confidential information regarding customers and following security rules and regulations put in place by others. We elaborate on our findings further at this stage.

The common theme that runs through the security beliefs of different professions is that the IS group is the primary arbiter of information security issues, which reflects a techno-centric view of security. Each profession appears to accept responsibility for a particular niche of information security. The groups acknowledge a role in protecting the core information that they handle: accountants for accounting information, HR for employee information, marketing for customer information, and IS for information residing in the computers and networks. The awareness of information security issues related to the technological infrastructure is limited in most non-IS groups, consistent with their belief that security is the primary responsibility of the IS group. The non-IS groups state that they will comply with security rules, if there is no other competing demand. Surprisingly, even the IS professionals believed that their professional cohorts would favor getting the job done over complying with security regulations.

## A Brief Comparison of Information Security Cultures

Summary comparisons of the information security cultures of the four professions are shown in Tables 9 and 10 (parts 1 and 2). The security-related beliefs of professionals taken together with their group identities and other relevant beliefs provide an overview of the security cultures of different professional groups. Our premise that there will be differences in the security cultures of different professions has been borne out. Our data suggest the accounting profession has a strong security culture, the marketing profession a weak security culture, with the IS and HR professions falling somewhere between the two.

Accounting professionals have a holistic view of security that is consistent both with their professional identity and their general beliefs about rules and compliance. Their professional identity is that of a group charged with ensuring the accuracy of financial statements, the discharge of which requires clear procedures, and strict adherence to rules. Ensuring security also requires compliance with security policies, procedures and rules. Thus, compliance with security rules is in line with their normal propensity to comply with rules. They tend to view security as everyone's responsibility, even if IS is assigned the lead role. They are aware that information security includes the protection of all the information in the organization and the information infrastructure. They believe strongly in complying with security rules. They do not believe in violations of security rules to meet performance requirements, except under extreme circumstances. It is clear that their security-related beliefs are in keeping with their primary culture of rule compliance and willingness to follow directives.

The marketing profession's identity is that of a group that improves an organization's competitiveness and profitability by helping the customers understand the organization's products and helping the organization understand the customers' needs. Increasing sales and profitability involves a willingness to take risks to accomplish

| Table 9: Summary Comparison of Information Security Cultures of Professions (Part 1 of 2) | | | | |
|---|---|---|---|---|
| | Profession | | | |
| Category | Accounting | Human resources | Marketing | Information systems |
| Identity | | | | |
| Role 1 | Ensure validity and accuracy of financial statements | Help recruit employees that fit into the organization | Educate customers about the organization's products; inform the company about the customer's needs | Offer technical expertise and guidance |
| Role 2 | Bridge between shareholders and managers | Bridge between employees and organization | Bridge between customers and organization | Bridge between technology and organization |
| Contribution to organization | Improve efficiency and profitability of organization | Contribute to strategic goals by recruiting correct employees | Improve profitability by meeting customer needs | Help organization use technology to its benefit |
| Contribution to society | Provide confidence in corporations; protect shareholder interests | Ensure employees are treated in compliance with the law | Help society meet its consumption needs | Help society use technology to its benefit. |
| General Beliefs | | | | |
| Compliance with rules and laws | High | High | Low | Reluctant follower of rules |
| Propensity to risk | Low | Low | High; taking risks is considered necessary for success | Mixed. Want stable operations because of organizational dependency on technology; have to be willing to be innovative (i.e., willing to take risks) when new advances come |
| Hierarchy | Need to comply with instructions from higher levels | Need to comply with instructions from higher levels | Lower level of concern for managerial directives | Would like guidance to be limited to broad directions |

goals. The risks taken are sometimes associated with a deviation from rules and managerial directives. Thus, there is a general belief that rules can be ignored if the circumstances demand it. This spills over into their belief system about security rules and regulations. While there is a willingness to abide by security rules in normal times, there is a readiness to ignore them when they get in the way of fulfilling their primary responsibilities. This value system is consistent with their belief that they have a small role to play in information security, due to their perception that the primary responsibility for security belongs to management and IS professionals. Marketing professionals follow rules only to the extent such rules do not get in the way of their productivity or performance.

HR and IS professionals seem to fall in between accounting and marketing professionals. HR professionals view their role as ensuring the equal treatment of all employees, which is tied in with the need to comply with federal and state statutes and rules. They believe in avoiding risks. Thus, similar to the accounting profession, their beliefs about complying with rules and avoiding risks in general carry over to complying with security rules and not taking risks with respect to security. Where they differed from the accounting profession was that they had a narrower view of what information security is—their beliefs restricted information security to the safeguarding of employee records. Also, there was a lower level of awareness of risks associated with technology. Thus, while their beliefs about complying with security rules strengthened security culture, their narrow definition of security and reduced awareness of technical issues related to security indicated vulnerabilities.

IS professionals view their primary role as enhancing organizational efficiency and productivity through the use of information technology. Frequent changes in technologies require that they be willing to take risks in their pursuit of

| Table 10: Summary Comparison of Information Security Cultures of Professions (Part 2 of 2) | | | | |
|---|---|---|---|---|
| | Profession | | | |
| Category | Accounting | Human resources | Marketing | Information systems |
| Security beliefs | | | | |
| Source of beliefs | Profession | Mostly from their organization | Mostly from their organization | Profession |
| Primary focus | Accounting focus on accounting information | HR focus on employee information | Client-related information | Information stored in technology |
| Who is responsible | Mostly everyone; IS personnel have special responsibility; accounting personnel have special responsibility for accounting info | IS department responsible for information security | Primarily IS department | IS believes that everyone else holds them responsible; IS believes that they have to guide management on security issues; IS believes they have to come up with security policies |
| Awareness | Aware that risks exist | Limited awareness | Limited awareness | High awareness of technical risk |
| Security risk taking | Low | Low | Don't understand security; don't mess with it | Low |
| Compliance with security rules | Prone to comply | High | Willing to follow security rules | Yes, on issues that IS group considers important |
| Security vs. productivity | Sometimes have to violate security rules | For the most part, security wins; make exceptions in special cases | Performance needs take precedence | Getting job done takes precedence |

higher efficiencies. On the other hand, they need to ensure the integrity and reliability of the technology infrastructure on a day-to-day basis, which leads to the belief that they should not take risks. In spite of the latter, overall they come across as risk takers. This applies to their beliefs about information security. So while they are knowledgeable about information security, they tend to believe that it is permissible to ignore security policies in pursuit of productivity (perhaps because they view themselves as cognizant of risks and consequences).

Comparing the security cultures of HR professionals to IS professionals, it can be seen that HR professionals are less prone to take risks, more compliant with security rules and managerial directives, but have a narrower awareness of security issues. IS professionals, on the other hand, are more aware of security issues, but more prone to take risks and circumvent security rules.

Overall, while professional groups may share individual characteristics of security culture, the aggregate security culture of each professional group appears to be relatively unique.

## VI. DISCUSSION AND CONTRIBUTIONS

Based on the preceding analysis of the data gleaned from our interviews, and an understanding of the literature that is available, we have developed a set of propositions to illuminate the interplay and interrelationships between differentiated professional cultures and security cultures, including inconsistencies between culturally related beliefs and subsequent behavior under conditions of performance pressure. In the absence of hypotheses to confirm or disconfirm, these propositions constitute part of the contributions of this research. In addition, these propositions also provide direction for future research.

### The Conceptualization of Security Culture

Our proposed theoretical framework is that security culture is a composite of the three dimensions: beliefs about the identity of the profession, general beliefs about risk and compliance, and security-related beliefs (see Figure 1).

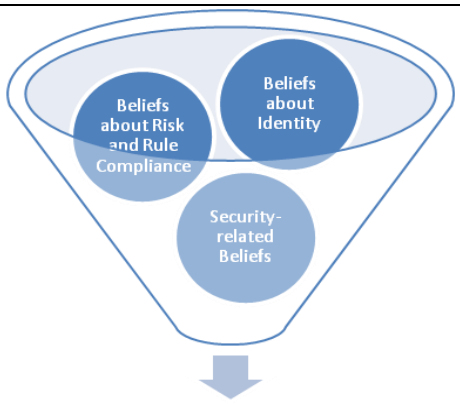


**Figure 1. Conceptualization of Information Security Culture**

Thus, our work provides a parsimonious set of dimensions to characterize information security cultures of professional groups. As discussed in the section on Theoretical Framework, the three dimensions are derived from the frameworks proposed by Chia et al. [2002] and Tejay and Dhillon [2005]. The results in the current study show a consistency between the three categories of beliefs: beliefs about identity, beliefs about rule compliance, and beliefs about security. The idea that factors that influence behaviors in non-security domains can influence security-related behaviors has been suggested by others. For instance, Bulgurcu et al. [2010] argue that the motivation to follow rules and regulations in general can be extended to "expect that similar motivations exist in the context of ISP (Information Security Policy) compliance" [p. 526]. Thus, in understanding the security culture of a group it is worthwhile to simultaneously examine the group's identity and other related beliefs. This leads to Proposition 1.

> Proposition 1: The information security culture of a profession is rooted in its beliefs about its identity, its general beliefs about risk and compliance, and its security-related beliefs.

This is important because it points out that cultural characteristics of professions outside the immediate realm of security can also help inform on the information security cultures of professions. In particular, the identity of the profession and the general beliefs about risk and compliance are useful in understanding the security cultures of professional groups.

### Security Cultures of Professions

Research on security culture to date has focused on conceptualizing security culture: that is, defining the term and identifying dimensions [Chia et al., 2002; Tejay and Dhillon, 2005], or describing security cultures at an organizational level [e.g., Ruighaver et al., 2007]. There is no prior study definitively reporting differences in security cultures across professions, although it has been suggested that IS security has different meanings for different occupational communities [Vaast, 2007]. The Vaast study was conducted in a hospital, and examined the views of doctors, nurses, clerical staff, technicians, managers, and so on. Further, Zakaria and Gani [2003] have shown that managerial perceptions of security are different from end-user perspectives of security, and Smith et al. [2010] also indicate differences between managerial and employee perceptions of information security. The professional culture literature reports that there can be major differences in cultures across professions [Trice, 1993; Mills and Tsamenyeni, 2000]. Thus, differences in security cultures across professions should not be surprising. The current study has found support for the existence of differences in security cultures across professions. Thus, it can be proposed:

> Proposition 2: Information security cultures vary across professions.

This result is significant because the study provides preliminary empirical evidence for differences in security cultures across professions. The additional contribution is that, for these four professions, the information security culture has been characterized. It can form the basis of understanding what lapses in security behavior may occur in each group, and appropriate steps taken to avoid them.

## Action Inconsistency

In the discussion of differentiated cultures, action inconsistency has been defined as the differences that exist between beliefs and behaviors in a culture [Martin, 1992]. Differences between beliefs and behaviors have been reported by others. Smith et al. [2010] report that senior managers, while implementing a security compliance program, failed to allocate adequate financial resources for the initiative. Similarly, Puhakainen and Siponen [2010]

report that the CEO in their study, while arranging for security training for his employees, was perceived to be slack in complying with the company's information security policies. These two examples show that while management believed security to be important enough to implement security initiatives, their behaviors were not consistent with those beliefs. Similarly at the employee level, behavior has been reported to deviate from beliefs: "… four employees felt that work overload, hurrying, suddenly emerging situations and unplanned assignments hindered their compliance with the email policy" [Puhakainen and Siponen, 2010, p. 767].

The possible existence of similar inconsistencies between security-related beliefs and security-related actions has been identified in the current study. Interviews examining self-reported beliefs and behaviors are likely to suffer from social demand bias in the answers of the respondents. It would be inappropriate for respondents to indicate that they believed that security was unimportant, or that they would violate security rules. Further, they would tend to be discreet about any security violations that they may have engaged in or observed. Either in keeping with these, or responding truthfully, respondents belonging to all professions said that they believed that security rules should not be violated. However, under conditions of performance pressure, all groups appeared to believe, to a lesser or greater extent, that security rules may have to be ignored. Accounting and HR professionals try to incorporate security procedures into their normal work-routine, but still admitted that they were prone to occasional circumventing of security rules under pressure to complete tasks. IS and marketing professionals readily admitted their bias to productivity-related objectives over security expectations. Thus, there are differences between stated beliefs that security rules should not be violated, and actual practices of circumventing security rules under performance pressure. This leads to:

> Proposition 3a: There may be inconsistencies between security-related beliefs and security-related behaviors, particularly at times of performance pressure.

The conflict between security and productivity poses one of the biggest challenges. The interesting point to note is that even the more conservative and rule-compliant groups, such as accounting and human resources, confess to the circumvention of security at times of performance pressure.

## Functional Orientation of Professions

The categorization of functions in organizations has received scattered attention in management literature. Additionally, the categories and their definitions are not consistent across studies. We use the categorizations suggested by Thompson [1965] to categorize professions by their primary functions. Thompson (1965) states that conditions within a bureaucracy are determined by a drive for productivity and control. Productivity refers to the maximization of the goal(s) as set by the owner(s) of the organization. Control refers to the processes in place to achieve reliable and predictable behaviors. Based on these definitions, marketing and information systems can be seen to be predominantly production functions, and human resources and accounting to be predominantly control functions. Marketing is aimed at maximizing sales; information systems is aimed at using technology to maximize the efficiency of diverse functions as sales, production (manufacturing), record keeping, and so on. In contrast, human resources is focused on controlling processes to ensure consistent application of rules and compliance with governmental regulations across employees (i.e., achieve reliable and predictable behaviors in these areas). Similarly, the accounting function controls financial record keeping (i.e., applies GAAP rules to produce reliable and predictable records of financial performance).

Previous studies have not examined differences in security-related behaviors across professions. In the current study, we note that the two groups (accounting and HR) with a primary focus on control functions show a greater tendency to comply with rules and security than the two (marketing and information systems) with a primary focus on productivity, effectiveness, and efficiency, even under performance pressure.

> Proposition 3b: Production-oriented groups are more likely to have inconsistencies between security-related beliefs and security-related behaviors than control-oriented groups.

This proposition is important because it provides generalizable guidance on which groups are more likely to deviate from security-related behaviors. Further, there is the possibility that the pressures from production-oriented groups can spill over to other related groups. This is evident from the complaint of one respondent in the Puhakainen and Siponen [2010] study: "*Sometimes management and salesmen give us unusual, unplanned and urgent assignments. This makes us too busy even to think about IS security --…"* [p. 767].

## The Techno-centric View of Information Security

Our results indicate the IS group is seen as a key player, if not *the* key player, in security initiatives. This reflects a techno-centric view of security. Accounting professionals appear to have a more holistic perspective of security, acknowledging the security responsibilities of all individuals, but still seeing a significant role for the IS group.

Researchers have emphasized the dangers of viewing security as a technical problem [Dhillon, 1997; Siponen, 2000]. Other researchers have determined that managers also tend to view information security as a technical issue that is the responsibility of IS professionals [Guzman et al., 2004]. The tendency of management to view information security as the responsibility of IT is also reported by Smith et al. [2010]. Interestingly, Vaast [2007] reported that IS professionals in a hospital setting viewed information security as a technical problem. Thus, the efforts of information security researchers to disseminate the idea that information security is a complex combination of technical, managerial, and behavioral issues have yet to bear fruit, as expressed in Proposition 4.

> Proposition 4: Information security cultures of all professions continue to be rooted in a techno-centric view of security.

The pervasiveness of this belief is surprising given that most security professionals have been preaching that information security should not be viewed as a technical problem alone, and should be addressed holistically (i.e., with behavioral, organizational, and technical controls). The greatest danger could occur when they see the responsibility for information security as belonging to others, and professional groups (primarily IS) fail to see their own responsibilities. Such misperceptions of professional groups may be further aggravated when top management also has a techno-centric view of information security.

## Security Awareness

Information security awareness plays a crucial role in effective interpretation and use of information security policies, procedures, and technologies by the end-users [Siponen, 2000]. In our study, the HR professionals did not claim security awareness, but were willing to follow security rules, with few exceptions. IS professionals, on the other hand, claimed a sufficiently high awareness level to stake a leadership role in security, but admitted a bias toward performance over security under pressure. IS professionals also did not believe strongly in complying with the rules. This comparison of HR and IS professions suggests that while security awareness is important, it could prove of little value unless it is accompanied by a strong willingness to comply with rules. This results in Proposition 5.

> Proposition 5: Security awareness is a necessary but not sufficient condition to build a strong information security culture.

This proposition challenges one line of thinking currently present in the area of security (i.e., that security awareness is the key to improving information security) [Albrechtsen, 2007; Siponen, 2000]. It is true that security awareness is necessary, but our research suggests that that is not sufficient. Puhakainen and Siponen [2010] made similar observations. They report in their study that despite "a high level of employee awareness of IS security issues …. the IS security manager saw violations of information security policies and procedures, especially the e-mail policy." [p. 765]. We argue that culturally, the group has to be willing to engage, and translate that awareness into action to result in a strong information security culture.

## Contributions and Implications

The contributions of the study, along with the theoretical and practical implications of the findings, are discussed next. First, we have proposed a framework to conceptualize the security culture of a profession based on the identity, the general beliefs, and the security-related beliefs of the professional members. In line with this framework we have logically developed and provided a preliminary qualitative empirical basis for a set of propositions to inform and guide future research. There is consistency in the beliefs related to the three categories. Both theoretically and practically, this implies that a cogent understanding of the security culture of a profession can be greatly enhanced by simultaneously examining the three sets of beliefs.

Second, our study suggests that while there are overlaps between the security cultures of different professions, there are also differences. The existence of differences may not be surprising. However, the finding is important for two reasons. One, in an organization, employees are influenced both by organizational and professional cultures [Trice, 1993]. Thus, in attempting to establish a strong security culture in an organization, managers must understand the influences of the professional security culture, and either leverage or compensate that influence based on whether the professional influence is beneficial or not. While this may seem obvious, none of the published literature [e.g., Leach, 2003; Tejay and Dhillon, 2005; Von Solms and Von Solms, 2004] on the development of information security culture in organizations recommends customized approaches for different groups in an organization. Two, the identification of specific differences in information security cultures between professions will be helpful in the formulation of customized approaches for different professions. For example, accounting groups are more risk averse while marketing groups are less risk averse. Thus, it is more necessary to help the marketing group internalize the idea that taking risks in marketing is different from taking security-related risks.

Third, during times when task demands increase performance pressure, there appears to be a greater willingness to circumvent security if it presents barriers to the efficient execution of the tasks. Our study indicates that the readiness with which a professional group surrenders security in favor of productivity varies across groups. Production-oriented professional groups (such as marketing and IS) seem to be more willing to favor productivity over security than control-oriented professional groups (such as accounting and HR) in our study. There is the potential to develop theoretical explanations why this is so, which we will leave to future research. From a practical perspective, the implication is to seek ways to reduce the conflict between productivity and security. In today's corporate environments, where the constant refrain is "do more with less," management may wish to step back and examine the effects that this perennial focus on productivity has on security. Alternatively, in a security-conscious organization, management may wish to focus more education and monitoring efforts on those groups that exhibit a tendency to favor productivity over security.

Fourth, our study suggests that while all professional groups acknowledge some responsibility for information security, there is a near unanimous belief that information security is the bailiwick of IS professionals. This is consistent with a techno-centric view of information security, and in contrast to a growing belief among most researchers and many practitioners that information security is everyone's responsibility. From an academic perspective, this highlights a disconnect in the IS literature between the theoretical and prescriptive acknowledgement that information security is a socio-organizational issue [e.g., Von Solms, 2006] and empirical findings that "information security research has primarily focused on technical issues" [Siponen and Oinas-Kukkonen, 2007, p. 73]. From a practitioner perspective, this highlights an opportunity to improve information security by recognizing that although human behavior is a significant problem in implementing effective information security practices [Siponen and Oinas-Kukkonen, 2007], group members are often unaware of this, and think that a combination of technology and the IS function is sufficient to safeguard organizational information assets. Focused outreach initiatives might educate individuals on this issue and make them more aware of their own security responsibilities.

Lastly, in comparing the security awareness and beliefs about compliance of the HR and IS groups, there can be a disassociation between awareness and compliance. We have noted that IS professionals are more aware of security, but show a greater willingness to deviate from security rules, while HR professionals who are less aware of security risks are more willing to comply with the security rules. Thus, it is possible for a group to have high awareness of security issues, but to be willing to deviate from security policies. Conversely, another group may have low awareness but be less willing to deviate from security policies. From a theoretical standpoint, it raises the issue of which of the two forces leads to greater information security, and under what circumstances. From a practical point of view, security training must focus both on increasing awareness and encouraging compliance.

## Limitations and Further Research

Prior to our research, there was no well established conceptualization of information security culture for professional groups; what was available were only two proposed conceptualizations with some preliminary validation for organizational security culture. We have adapted the existing frameworks to characterize the information security cultures of professional groups, and provided qualitative evidence to support our conceptualization.

Our study is subject to all the limitations of studies that use qualitative techniques. Qualitative studies have limited generalizability. Generalizability is best established by conducting large scale surveys. Thus, future research will have to focus on large scale surveys to test the robustness of our results. A second limitation is that the respondents were all from one part of the United States. Thus, care must be taken when generalizing the results to groups in other parts of the United States or other parts of the world. Future research will have to replicate the study and conduct more surveys to expand the generalizability to professional groups in other geographical areas.

The research agenda surfacing from the current study is presented next along with suggestions for future steps. First, we have examined information security cultures independent of organizations (i.e., respondents worked in different organizations). It would be interesting to examine whether the observed differences persist across professional groups working in a single organization. Trice [1993] reports that cultures of professional groups in organizations are subject to the influences of the culture of the professional group and the culture of the organization. Thus, it could be anticipated that the information security culture of professional groups in organizations will show the influences of the security cultures of the professions and that of the organization. At the level of probing for differences in security cultures across professions within an organization, a study parallel to the current study using interviews can be conducted. At a more complex level of identifying the relative influences of the profession and the organization, it would require the study of two professions (one stronger in security culture [e.g., accounting], and one weaker in security culture, perhaps marketing) in two organizations that have reportedly stronger and weaker security cultures at the organizational level. Case methodology would be best to address such a question.

Second, the primary goal of all security-related research is to help identify factors that will promote information security. The belief that security culture will enhance information security is based in demonstrated relationships between culture and performance in other areas such as organizational excellence. Comparable evidence for the area of information security culture needs to be gathered at two levels. The first level of study would examine the influence of culture on the compliance behavior of employees and the reduction in vulnerabilities. Such studies can be either in-depth case studies of organizations with varying strengths of security cultures, or surveys using self-report data from key respondents in organizations. The second level of study would examine the relationship between security culture and the actual incidence of security breaches. Such a study is probably best approached using survey methodology using key respondents from organizations.

Third, another challenge for researchers is to develop profession-specific techniques to improve information security cultures. Several researchers have put forth generic proposals for improving information security cultures in organizations [e.g., Von Solms and Von Solms, 2004]. More targeted approaches are necessary. Generic profession-independent proposals include the formulation of clear policies and procedures, awareness and education programs, and the implementation of rewards systems. Targeted profession-specific proposals would require differential emphasis on these factors based on the profession. For instance, marketing professionals have lower levels of awareness than other professionals. Security culture development for the marketing group should include a heavy emphasis on increasing awareness. In contrast, IS professionals have a high level of awareness to begin with, but come across as overconfident in their ability to be secure. For the IS group, improving awareness will need less emphasis than the issue of not being overconfident. In effect, an understanding of the differences in security culture across professions can help tailor efforts to improve the security culture of each profession. Studies requiring observations of change in cultures are necessarily longitudinal studies extending over periods of years. Cultures are embedded deeply, and are not likely to change in the short span of a year or two. Thus, efforts to study the effectiveness of approaches to change culture present the greatest challenges in terms of patience, time, and resources. Essentially, such studies need pre- and post-treatment measures of security cultures, in one or more organizations, to assess the effectiveness of the treatments.

The fourth and final suggestion relates to the observation in our study that even groups that are aware of information security issues do deviate from recommended information security practices. This points to the need to understand why such deviations from good practices are engaged in. The deviations range from simple ones at a low level (e.g., sharing passwords with others to expedite work), to more complex ones, in which top management makes simultaneous demands of productivity and security without allocating sufficient resources to achieve both goals. Research would have to focus on identifying the complete range of the deviations based on observations, interviews, and surveys, and then classifying them into a parsimonious set. Subsequently, efforts will have to focus on finding ways to reduce the deviations. The specific research projects would depend on the nature of the deviations. Simple deviations at the individual level will need to conduct survey-based studies to elicit the role of individual characteristics, task-based variables, and organizational level constraints. Study of deviations at a more complex level, such as budget allocation issues, would need surveys to understand the demands on top management.

In sum, the work in the area of information security culture has just begun. Clearly, much work remains to be done.

## VII. CONCLUDING REMARKS

In an organizational setting, employee behaviors are subject to the influences of organizational culture and professional culture. Based on this, it is necessary to gain an understanding of professional culture to understand employee behaviors in organizations. In the current study, we focused on developing a characterization of information security cultures of four different professions. We have provided preliminary evidence that there are differences in the security cultures across the professions. Based on these and other findings, we have put forth propositions related to information security cultures of professions. In essence, the results of the study support our argument that the security cultures of different professions need to be examined more closely as a part of the field's attempts to improve the security culture in organizations.

## ACKNOWLEDGEMENTS

We thank Prof. Dianna L. Stone for her feedback on an earlier draft of this article. We thank all the participants in the study for their help and cooperation. We owe a special debt of gratitude to Carlos Dorantes for his painstaking work associated with coding. We thank the seminar participants at the Indian Institute of Management, Bengaluru, for their feedback. We thank the reviewers for their thoughtful comments and suggestions, and the associate editor for the clear directions concerning the revisions needed. We thank the Chief Editors for their thoughtful guidance. The help of the copy editor to improve the presentation of the article is gratefully acknowledged. We thank the Dean of

the College of Business, University of Texas at San Antonio, for supporting the participation of the second author in the study through summer research grants.

## NOTE

An earlier version of this article was published in the Proceedings of the 41st Hawaii International Conference on Systems Sciences.

## REFERENCES

*Editor's Note*: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Albrechtsen, E. (2007) "A Qualitative Study of Users' View on Information Security", *Computers and Security,* (26), pp. 276–289.

Andress M. and B. Fonseca (2000) "Manage People to Protect Data", *InfoWorld,* (22)46, p. 48.

Beynon, D. (2001) "Talking Heads", *Computerworld*, (24)33, pp.19–21.

Boas, F. (1930) "Anthropology" in *Encyclopedia of the Social Sciences*, New York, NY: The Macmillan Company pp. 73–110.

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.

Breidenbach, S. (2000) "How Secure Are You?" *Information Week*, (800), pp. 71–78.

Bulgurcu, B., H. Cavasoglu and I. Benbasat (2010) "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness", *MIS Quarterly,* (34)3, pp. 523–548.

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

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

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

D'Arcy, J. and T. Herath (2011) "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings", *European Journal of Information Systems,* (20), pp. 643–658.

Deshpande, R. and F.E. Webster (1989) "Organizational Culture and Marketing: Defining the Research Agenda", *Journal of Marketing*, (53)1, pp. 3–15.

Detert J., R. Schroeder and J. Mauriel (2000) "A Framework for Linking Culture and Improvement Initiatives in Organisations", *The Academy of Management Review*, (25)4, pp. 850–863.

Dhillon, G. (1995) *Interpreting the Management of Information Systems Security*, London, England: London School of Economics and Political Science.

Dhillon, G. (1997) *Managing Information System Security,* London, England: Macmillan.

Eisenhardt, K.M. (1989) "Building Theories from Case Study Research", *Academy of Management Review*, (14)4, pp. 532–550.

Gaunt, N. (2000) "Practical Approaches to Creating a Security Culture", *International Journal of Medical Informatics,* (60), pp. 151–157.

Geertz, C. (1973) "Religion as a Cultural System" in *The Interpretation of Cultures*, New York, NY: Basic Books.

Gordon, G.G. and N. DiTomaso (1992). "Predicting Corporate Performance from Organizational Culture", *Journal of Management Studies,* (29)2, pp. 783–798.

Gregory, K.L. (1983) "Native-View Paradigms: Multiple Cultures and Culture Conflicts in Organizations", *Administrative Science Quarterly,* (28), pp. 359–376.

Guzman, I.R., J.M. Stanton, K.R. Stam, V. Vijayasri, I. Yamodo, N. Zakaria and C. Caldera (2004) "A Qualitative Study of the Occupational Subculture of Information Systems Employees in Organizations" in *Proceedings of the ACM–SIG MIS-Computer Personnel Research Conference*, Tucson, AZ, pp. 74–80.

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, p. 33.

Hall, E.T. (1959) *The Silent Language*, Garden City, NY: Anchor Books.

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

Helokunnas, T. and R. Kuusisto (2003) "Information Security Culture in a Value Net" in *Proceedings. of IEEE International Engineering Management Conference*, Albany, NY, pp. 190–194.

Herath, T. and H.R. Rao (2010) "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations", *European Journal of Information Systems,* (18), pp. 106–125.

Holsti, O. (1969) *Content Analysis for the Social Sciences and Humanities*, Menlo Park, CA: Addison-Wesley Publishing Co..

Iivari, N. and P. Abrahamsson (2002) "The Interaction Between Organizational Subcultures and User Centered Design—A Case Study of an Implementation Effort" in *Proceedings of the 35th Hawaii International Conference on Systems Sciences,* (8), pp. 245–254.

Jermier, J.M., J.W. Slocum, L.W. Fry and J. Gaines (1991) "Organizational Subcultures in a Soft Bureaucracy: Resistance behind the Myth and Façade of an Official Culture", *Organizational Studies*, (2), pp.170–194.

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

Kluckhohn, C. (1949) *Mirror for Man*, New York, NY: McGraw-Hill Book Co, Inc..

Knapp, K.J., T.E. Marshall, R.K. Rainer and F.N. Ford (2006) "Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness", *Information Management and Computer Security,* (14)1, pp. 24–36.

Kroeber, A.L. and C. Kluckhohn (1952) *Culture: A Critical Review of Concepts and Definitions,* New York, NY Vintage Books.

Kroeber, A.L. and T. Parsons (1958) "The Concept of Culture and of Social System", *American Sociological Review*, (23)5, pp. 582–583.

Kunda, G. (1995) "Engineering Culture: Control and Commitment in a High-Tech Corporation", *Organization Science*, (6)2, pp. 218–230.

Kwon, J. and M.E. Johnson (2011) "The Impact of Security Practices on Regulatory Compliance and Security Performance" in Thirty Second International Conference on Information Systems, Shanghai.

Leach, J. (2003) "Improving User Security Behavior", http://www.jlis.co.uk/Papers/Improving_Security_Behaviours_030903.pdf (current Dec. 25, 2011).

Lee, Y and K.R. Larsen (2009) "Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-malware Software", *European Journal of Information Systems,* (18), pp. 177–187.

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.

Lim, J.S., A. Ahmad, S. Chang and S. Maynard (2010). "Embedding Information Systems Culture: Emerging Concerns and Challenges", http://www.pacis-net.org/file/2010/S11-03.pdf (current Dec. 20, 2011).

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

Martins, A. and J. Eloff (2002) "Information Security Culture" in *SEC '02 Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives*, Kluwer, B.V. Deventer, The Netherlands, pp. 203–216.

May, C. (2003) “Dynamic Corporate Culture Lies at the Heart of Effective Security Strategy”, *Computers, Fraud and Society*, (2003)5, pp. 10–13.

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

Mills, J. and M. Tsamenyeni (2000) “Communicative Action and the Accounting/Marketing Interface in Industry”, *Journal of Applied Management Studies,* (9)2, pp. 257–273.

Pare, G. (1995) “Understanding the Dynamics of Information Technology Implementation: The Case of Clinical Information Systems”, Unpublished Dissertation, Florida International University, Miami, FL.

Pondy, L.R. (1983) “Union of Rationality and Intuition in Management Action” in Srivasta, S. (ed.) *The Executive Mind*, San Francisco, CA: Jossey-Bass, pp. 169–189.

Puhakainen, P. and M. Siponen (2010) “Improving Employees’ Compliance Through Information Systems Security Training; An Action Research Study”, *MIS Quarterly,* (34)3, pp. 757–778.

Rao, V.S. and S. Ramachandran (2011) “Occupational Cultures of Information Systems Personnel and Managerial Personnel: Potential Conflicts”, *Communications of the Association for Information Systems,* (29) Article 31, pp. 581-604.

Robey, D. and M.L. Markus (1984) “Rituals in Systems Design”, *MIS Quarterly,* (8)1, pp. 5–15.

Ruighaver, A.B., S.B. Maynard and S. Chang (2007) “Organizational Security Culture: Extending the End-user Perspective”, *Computers & Security*, (26), pp. 56–62.

Schein, E.H. (1985) *Organizational Culture and Leadership,* San Francisco, CA: Jossey-Bass Publishers.

Schein, E. (2004) *Organizational Culture and Leadership, 3rd edition*, San Francisco, CA: Jossey-Bass Publishers.

Schlienger, T. and S. Teufel (2003) “Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture” in 14th International Workshop on Database and Expert Systems Applications, Prague, Czech Republic.

Schwarzwalder R. (1999) “Intranet Security”, *Database and Network Journal*, (22)2, pp. 58–62.

Siponen, M.T. (2000) “A Conceptual Foundation for Organizational Information Security Awareness”, *Information Management and Computer Security*, (8)1, p. 31.

Siponen, M.T. and H. Oinas-Kukkonen (2007) “A Review of Information Security Issues and Respective Research Contribution”, *ACM SIGMIS Database*, (38)1, pp. 60–80.

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

Smith, A.C. and S. Kleinman (1989) “Managing Emotions in Medical Schools: Students’ Contacts with the Living and the Dead”, *Social Psychology Quarterly*, (52), pp. 56–69.

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.

Spears, J.L. and H. Barki (2010) “User Participation in Information Systems Security Risk Management”, *MIS Quarterly,* (34)3, pp. 503–522.

Straub, D., K. Loch, R. Evaristo, E. Karahanna and M. Strite (2002) “Toward a Theory-based Measurement of Culture”, *Journal of Global Information Management*, (10)1, pp 13–23.

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

Thomson, M.E. and R. Von Solms (1998) “Information Security Awareness: Educating Your Users Effectively”, *Information Management and Computer Security,* (6)4, pp. 167–173.

Thompson, V.A. (1965) “Bureacracy and Innovation”, *Administrative Science Quarterly,* (10)1, pp. 1–20.

Thurnwald, R. (1950) *Der Mensch Geringer Naturbeherrschung: Sein Aufstieg Zwischen Vernunft and Wahn*, Berlin, Germany: Walter de Gruyter.

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

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

Tylor, E.B. (1871) *Primitive Culture*, London, England: John Murray.

Vaast, E. (2007) "Danger Is in the Eye of the Beholders: Social Representations of Information Systems Security in Healthcare", *Journal of Strategic Information Systems,* (16), pp. 130–152.

Van Maanen, J. (1973) "Observations on the Making of Policemen", *Human Organization,* (32)4, pp. 407–418.

Van Maanen, J. and S.R. Barley (1984) "Occupational Communities: Culture and Control in Organizations" in Staw, B.M. and L. Cummings (eds.), *Research in Organizational Behavior,* Stamford, CT: JAI Press, pp. 287–365.

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

Von Solms, B. (2006). "Information Security—The Fourth Wave?" *Computers and Security,* (25)3, pp. 165–168.

Von Solms, R. and B. Von Solms (2004) "From Policies to Culture", *Computers and Security,* (23), pp. 275–279.

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

Zakaria, O. and A.A. Gani (2003) "Conceptual Checklist of Information Security Culture" in *2nd European Conference on Information Warfare and Security*, Reading, England: MCIL.

## APPENDIX A: INTERVIEW GUIDE

This is (interviewer name) interviewing _(respondent name)_ on __(date)_____.

- For the record, can you give your consent for audio taping the interview for research purposes?

→ Some of the following questions may be very obvious, but I have to ask those questions for the sake of completeness.

Work Experience

- Can you briefly explain your work experience (including profile of the organization, department, the responsibilities of the department, and responsibilities of the job)?

Questions Tapping Professionally Based Beliefs

*Extent of Association with Profession*

- What profession do you consider yourself to be a part of?
- Do you have any professional certifications (Example certifications with IS profession like MCSE, MCSP, CCNP)? – [ *WILL CUSTOMIZE THE CERTIFICATIONS DEPENDING ON THE PROFESSION/DISCIPLINE OF THE RESPONDENT]*
    a. If yes, which ones?
- To what extent do you participate in activities or groups associated with your profession?
- Are you a member of any professional associations? (Example: ACM, IEEE for IS)? – *[WILL CUSTOMIZE THE PROFESSIONAL DEPENDING ON THE PROFESSION/DISCIPLINE OF THE RESPONDENT]*
    a. If yes, which ones?
- Do you attend professional group meetings, gatherings, or conferences?
    - How often do you attend these meetings, gatherings, or conferences?
    - Have you attended national meetings?
    - Are you currently or have you previously been an office bearer of professional bodies associated with your profession?
- Do you regularly visit any professionally oriented websites or listservs?
    a. If yes, which ones?
- Do you subscribe to any industry trade magazines or journals? (Example: *PC Magazine*, *Computers and Security*, *IEEE Spectrum*, *Communications of the ACM*, *IEEE Computer for IS Professionals*)? *[WILL CUSTOMIZE THE MAGAZINES DEPENDING UPON THE PROFESSION OF THE RESPONDENT]*

- Do you interact with members of your profession away from work?
    a. Is this interaction primarily with co-workers or with people from other firms? *
- *If the respondent answered YES for the previous question* then ask the following:* Please answer the following questions based on your perception of what your profession expects from you. Your answers should be based on what you have read in trade magazines, heard in professional meetings, and think other professional members in general believe.
    b. *If the respondent has answered NO for the previous question* then ask the following:* Please answer the following questions based on your perception of what members of your profession inside your organization believe, and which you think could be applicable to members of your profession in general (including outside the organization).
- Do the professional societies you are associated with have a formal code of ethics?
    - How familiar are you with the code of ethics?
    - How familiar do you think others are with it?
- Generally speaking, how do members of your profession feel toward risk-taking?
- Are members of your profession optimistic or pessimistic, in general?
- Can you describe what the term "information security" or "IS security or computer security" means to members of your profession?
- In your opinion, do members of your profession believe in taking information security-related risks to get a job done?
- To what extent do members of your profession seek validation of their actions from their professional peers:
    - External to their organizations?
    - Internal to their organizations?
- *Expectations toward complying with hierarchy, rules, and procedures*
    - Do members of your profession subscribe to the idea of hierarchy?
    - If yes, do members of your profession *like* subscribing to the idea of hierarchy?
    - What is the belief of members of your profession about appropriate styles of management?
    - What is their belief about the level of detail that a manager should get involved in?
    - Among the members of your profession, what is the general belief about abiding by rules and procedures?
    - What is the belief of the members of your profession on the extent to which people should abide by rules and procedures?
- *Loyalty*
    - Are they loyal to the profession?
        - What would your profession's members say the values of your profession are?
        - To what extent do members of your profession believe in the values of the profession?
            - Would members work on upholding it whatever it takes?

In case of conflict between the values of the profession and the values of the organization, what would happen?

- *Responsibility/Accountability Factors*
    - When it comes to decisions, what level of guidance do members of your profession need from upper management?
    - What would be the response of members of your profession if upper management tried to specify details on how to do the task?
    - What would their response be if upper management tried to specify details of actions outside the domain of your profession (e.g., Security)?

- What would their response be if upper management entrusts responsibility to members of your profession in doing any task?
    - Will that have any effect on their beliefs/actions (in regards to the task in hand)?

- *Expectations About the Need for Rewards*
    - What motivates the members of your profession?
    - How do tangible rewards (such as money, promotion) compare to intangible rewards (such as satisfaction and appreciation of professional peers)?

*Security-Related Issues*

- Who do the members of your profession think *is* responsible for information security within organizations they work in?
- Who do the members of your profession think *should* be responsible for information security within organizations they work in?
- What role do the members of your profession think they play with respect to information security in an organization?
- Do members of your profession view information security as a serious problem for organizations?
    - Why?
- Does your professional association have continuing education about IS-related security?
    - Like what? (E.g.., training sessions/workshops on security organized by professional groups)
- Do members of your profession take IS courses as part of their education?
- Do members of your profession take IS security-related courses as part of their education?

*Productivity Issues*

- How do members of your profession define productivity?
- What do members of your profession believe is the primary role of their profession in an organization?
- How does this contribute to the overall performance of the organization?
- Does the professional organization arrange for continuing education on improving the performances?
- Do members of your professional association take part in continuing education on performance-related issues?
- How do members of your profession handle choices/trade-offs between getting the job done and information security measures?
- What kind of a connection do members of your profession see between “activities to secure information” and “activities to be done to be productive”?

*Professional Attributes*

- If you had to describe the “culture” of your profession, how would you describe it?
- If you had to describe what your profession contributes to society, what would you say?
- Who influences the security-related beliefs of the members of your profession?—the profession, each individual’s organizational management?

*<u>If the Respondents Are IT Professionals Then Ask the Following Additional Questions</u>*

Influence of members of the IT professional group <u>within organizations</u> on security-related beliefs of members of other professional groups within organizations

- What is the level of interaction IT professionals have with members of other professional groups within organizations?
- Do you think that the information security-related beliefs of IT professionals tend to influence the security-related beliefs of members of other professions within organizations?
    - *If the respondent answered YES,*

        - Why do you think IT professionals influence the security-related beliefs of members of other professions within organizations?
        - How do you think members of the IT profession are influencing the security-related beliefs of other professionals within organizations?
    - *If the respondent answered NO,*
        - Why do you think IT professionals do not influence the security-related beliefs of members of other professions within organizations?
        - How do you think members of the IT profession can do better to influence the security-related beliefs of other professionals within organizations?
- Do you think IT professionals in general influence security initiatives within organizations (set the tone for it) or follow what management has planned?
    - What makes you think so?

## APPENDIX B: SAMPLE CODES

**Table B–1: Sample Codes**

| Definition | # of instances | Sample |
|---|---|---|
| Beliefs about the need for validation of their action by others including their peers | 37 | Interviewer: To what extent do IT professionals seek validation of their actions from other people including peers?<br>Respondent: I think they seek it out frequently.<br>Interviewer: Why do they seek it out?<br>Respondent: On the personal level, you know, for egos. I think individuals like to be special technology professionals. Again, the personalities that wind up in our particular area like those challenges but, at the same time, they solve those challenges. Also, you know they like to represent it. I think from a personal standpoint from human nature they just like to. |
| Beliefs about hierarchy and complying with hierarchy in organizations | 38 | Interviewer: Do HR professionals subscribe to the idea of hierarchy in organizations?<br>Respondent: Yes. It allows that validation that we just talked about. They are very big on hierarchy. There is the vice president of HR, and there is the HR director, HR manager, then HR representative. Only as you get to certain levels are you given access to more information and ability to make more and more substantial decisions. |
| Belief about information security rules and procedures, and the need to comply with them | 24 | Interviewer: What do they believe about following security rules and procedures?<br>Respondent: If you are talking about IT security staff, they tend to put themselves above them.<br>Interviewer: I am talking about information security.<br>Respondent: I think they tend to put the rules in place and then don't think they apply to themselves.<br>Interviewer: Why do they think that it does not apply to them?<br>Respondent: Because they are ones that created it. They want to control it. |
| Belief about rules and procedures, and the need to comply with them | 51 | Interviewer: Among HR professionals, what is the belief about abiding to rules and procedures?<br>Respondent: It is very important that you must abide by the rules and procedures.<br>Interviewer: What is the extent to which they would follow these rules and procedures?<br>Respondent: I would say very strong again. If it's a tactical action, they will not abide by as much because there probably aren't any functional aspects on that. But, for strategic action they would. |
| General belief about ethics | 28 | Interviewer: Does the professional society that you are associated with have a formal code of ethics?<br>Respondent: Yes. We have several courses. |
| Belief about familiarity with the ethical standards | 27 | Interviewer: How familiar are others with the code of ethics?<br>Respondent: Strongly familiar, because you go through training for that. |

| Table B–1: Sample Codes – Continued | | |
|---|---|---|
| Professionals' familiarity of information security issues | 11 | Interviewer: How familiar do you think HR professionals are with information security issues?<br>Respondent: I would say that their understanding is relatively general. General in the sense they know what they are told to do by their management. I don't think most people know the broader scope of U.S. law or Texas law for that matter. I have heard a lot of people say that they don't know the difference between company policy and the U.S. or state policy. |
| Beliefs about whether information security is a cause for concern in organizations | 38 | Interviewer: Do members of your profession [marketing] view IS security as a serious problem for the organization?<br>Respondent: Yes, but they ignore it.<br>Interviewer: Why do they think it is a serious problem?<br>Respondent: If you are designing a system for security, it comes with more cost and is difficult to set up… that's the reason. |
| Beliefs about the connection between information security and productivity issues | 36 | Interviewer: How do HR professionals handle choices of trade-off between getting a job done and securing information?<br>Respondent: I would say 5 or 10 years ago it would be like just get it done. It does not matter if you have to break into that system. Today it's a different game. People might slide a little bit on keeping passwords real crazy and that kind of thing. But, the trade-off wouldn't be acting as a trouble for the whole system. |
| Beliefs about who has responsibility for information security in organizations | 39 | Interviewer: Who do members of your profession [marketing] think is responsible for information security within the organization they work for?<br>Respondent: The computer information officer or the IT people. |
| Beliefs about who should have responsibility for information security in organizations | 36 | Interviewer: Who do members of your profession think should be responsible for IS security within the organization they are working for?<br>Respondent: I would say the CIO again, but maybe with more input from the HR management team. |
| Beliefs toward taking information security risk | 16 | Interviewer: How do accounting professionals feel toward taking information security risk?<br>Respondent: I think it depends on the level of information that you have access to.<br>Interviewer: What do you mean by that?<br>Respondent: For example—I give you a live system or a system that has historical data. The company that I currently work for had just acquired another company and we would never share passwords for the actual accounting system, but we had access to historical data for research purposes in the other accounting system that they were using and we shared passwords for that. But, it was a dead system. We could not make entries or change anything. It was strictly read only. |
| Beliefs toward taking information security risks to get a job done | 33 | Interviewer: How do marketing professionals feel toward taking information security risks to get a job done?<br>Respondent: They might bend the rules.<br>Interviewer: Why?<br>Respondent: Because, as far as I am concerned, in my area sometimes you have to take risks to get the information that you need. |
| Beliefs about what motivates the professionals | 37 | Interviewer: What motivates HR professionals?<br>Respondent: Being acknowledged as a credible legitimate partner. Not being held responsible for problems outside the control of an HR person. An example of that would be—I am trying to get this young kid stationed in Florida because his mom and dad are both dying there and there is a special situation that requires that. Well, that is not enough of an action in order to move a kid to Florida. We have systems where you say we have to work within these rules and you have to follow them. |
| Beliefs about the level of responsibility that professionals prefer for information security issues | 15 | Interviewer: What kind of responsibility would they [marketing professionals] prefer for doing tasks related to information security?<br>Respondent: I would say full responsibility and be treated like an adult. |

| Table B–1: Sample Codes – Continued | | |
|---|---|---|
| Beliefs about the preference of the level of guidance needed from management | 37 | Interviewer: When it comes to making decisions, what level of guidance do IT professionals need from upper management?<br>Respondent: I don't think they need guidance as much as they just need enabling. Give me the resources and equipment, time, and the money to do the things that I need to do. |
| Belief about the level of influence that the professionals want the manager to exercise | 35 | Interviewer: What is the belief about the level of detail that a manager should get involved in?<br>Respondent: Lots of it depends upon subordinates and the subordinates' ability and skill level, their experience. When I first started as a salesperson, my boss would always help me with the sales call. Then later, whenever my boss wanted to come with me I was always wondering why? So, at the beginning whenever I needed help I was very happy to have it.<br>Interviewer: But, in general, what is the belief?<br>Respondent: Autonomy is very big for salespeople. |
| Belief about the style of management that would be preferred by professionals | 38 | Interviewer: What style of management do marketing professionals generally prefer?<br>Respondent: They kind of prefer decentralized. I mean, they just like to have an open management style. |
| Beliefs about the level of responsibility that professionals generally prefer | 31 | Interviewer: When it comes to doing any task, what level of responsibility do IT professionals need or want management to entrust to them?<br>Respondent: They want to rely on shared responsibility in case there is a problem that comes on the line that is caused by the misinformation on the requiring data. |
| Belief about the primary role that professionals play in organizations | 37 | Interviewer: What do HR professionals believe is the primary role their profession plays in organizations?<br>Respondent: Several roles; for example, we are advocates and leaders because we represent employee issues and concerns, as well as organizational issues and concerns. We have to be good communicators. We have to be masters of the business. We have to understand what our company does. We should also facilitate change. We have to always promote and facilitate change. |
| Belief about how the primary role that professionals play in the organization contributes to the overall performance of the organization | 36 | Interviewer: How does this [the role of the profession] contribute to the overall performance of the organization?<br>Respondent: I think people are the most important part of the company. If you have a work force that is motivated or relatively satisfying, you know you are going to realize benefits in terms of the profitability of the company. |
| Beliefs about the relative importance of tangible and intangible rewards for the professionals | 37 | Interviewer: How do tangible rewards such as money or promotions compare to intangible rewards such as enjoyability and challenge, which they supposedly should be seeking?<br>Respondent: I think the majority of IT professionals are in the profession because they believe that it pays better than the other. But, there are other IT professionals who will enjoy the relative popularity associated with it. |
| General belief about taking risks as part of the job | 38 | Interviewer: How do accounting professionals feel toward risk taking?<br>Respondent: I would say they are risk averse, especially from an audit perspective. Accountants are very stringent on how money is being categorized because they have to be more conservative on those guidelines. |
| Beliefs about the role played by their professionals with respect to information security in organizations | 38 | Interviewer: What role does a marketing professional think he or she plays (i.e., information security in organizations)?<br>Respondent: I think we view it as a very minimal role. We view ourself as the customers of the IT department. |

| Table B–1: Sample Codes – Continued | | |
|---|---|---|
| Beliefs about the sources that influence the information security-related beliefs of members of their profession | 38 | Interviewer: Who influences information security-related beliefs of HR professionals? Would that be your profession, each individual's organization, or some other factors?<br>Respondent: I think organization plays a role and management.<br>Interviewer: What about their profession?<br>Respondent: I don't think so.<br>Interviewer: Why?<br>Respondent: I think it's one of the routine things they do to comply with company policy and legal policy. They just view it as part of their job. |
| Beliefs about whether their profession offers continuing professional education courses in information security | 37 | Interviewer: Do professional associations in your knowledge have security-related training or awareness programs or workshops? Do they conduct these things?<br>Respondent: I would think they would. It's a major aspect today. If you look at any journal in security that's up there just about every major category of business is concerned. |
| Beliefs about whether their profession offers continuing education courses to improve productivity-related skills | 35 | Interviewer: In your understanding, do professional associations arrange for continuing education courses on improving performance?<br>Respondent: Yes they do. They have training programs and conferences (They have several conferences a year.) where marketers come together and learn. |
| Profession's definition of information security | 37 | Interviewer: What does the term "information security" mean for HR professionals?<br>Respondent: For the most part, it relates to employee management (i.e., making sure that every aspect of the employee file is kept confidential). Only certain individuals have access to various levels of information such as social security numbers, birthdays, marital status, and other things like that. |
| Issues that professionals would identify with the term "information security" | 4 | Interviewer: When HR professionals talk about information security, what actions come into their mind?<br>Respondent: Controlled access files. They think in terms of filing cabinets and making sure that they are locked, they think in terms of computer systems where electronic employee data is kept. |
| The overall outlook toward job and profession—optimistic or pessimistic | 37 | Interviewer: In your opinion, do you think members of the accounting profession think optimistically or pessimistically?<br>Respondent: Optimistic.<br>Interviewer: Why?<br>Respondent: Because they assume that is the way to do it. So, you just go ahead and do whatever. They make their own assumptions. |
| Profession's definition of productivity | 35 | Interviewer: What does the term "productivity" mean to accounting professionals in organizations?<br>Respondent: Effective use of time and money to produce a product. |
| Beliefs about what their profession contributes to society | 36 | Interviewer: If you had to describe what the accounting profession contributes to society, what would you say?<br>Respondent: Again, it plays a middle man role between the managers and shareholders, banks, and different stakeholders. If there is no accounting or auditing, then no information can be verified; thus, you cannot rely on information to make a decision. Therefore, banks cannot trust financial statements to issue loans and lots of things like that. |
| Beliefs about the culture that members of their profession share | 36 | Interviewer: If you had to describe the culture of the marketing profession, how would you describe it?<br>Respondent: The culture is somewhere in the middle between salespeople and (Pauses) I do not know. We have to use some techniques like the salespeople; for example, gaining confidence, being liked by the people whom we speak to, being a good listener. Also, marketing culture is very outspoken. I have to make my point and give my opinions. |
| Belief about the core values that constitute the profession | 37 | Interviewer: What would you say the core values of the accounting profession are?<br>Respondent: Honesty, integrity, conservatism (I am not sure if that's a value). |

| Table B–1: Sample Codes – Continued | | |
|---|---|---|
| Belief about how much the professionals will fight to uphold the values of the profession | 36 | Interviewer: To what extent do marketing professionals believe in the value that you stated?<br>Respondent: They would fight for these values. Many times you have to go out and get the information that you need. You have to speak to people and you have to let them know that this is confidential. I will not disclose this information and this is just for me to learn about the market. I am trying to put that all together and get a big picture of what I am doing, such as researching. If you let that information slip, then you lose your face value on your clients. |
| Belief about how professionals will respond to detailed instructions from management | 37 | Interviewer: What would be the response of IT professionals if upper management tried to specify the details of actions regarding how to do the task within the domain of expertise of IT?<br>Respondent: It would be counterproductive and risk going back to micromanagement. A person of management dictating how to do something may not be the best way to do it. |
| Belief about how professionals will respond to detailed instructions (in information security issues) from management | 37 | Interviewer: What would be the response if management tried to specify the details of actions outside the domain of expertise of accounting, like information security?<br>Respondent: I think that is probably a little bit different, because that is something that the individual may not be familiar with. |
| Beliefs about whether members of their profession take information security courses as part of their education | 37 | Interviewer: Do HR professionals in your opinion take information security-related courses as part of their education?<br>Respondent: I am sure they have some credits they have to fill, but I don't know if it is related to security. |
| Belief about what happens when there is a conflict between the values of the profession and the values of the organization | 37 | Interviewer: In case of a conflict between the values of the HR profession and the values of the organization that they work in, what would happen?<br>Respondent: They are going to go with the values of the organization, because that gives them their bread and butter unless it is against the law—that would be an exception. |

## ABOUT THE AUTHORS

**Sriraman Ramachandran** is currently employed at Dell Inc. as a Global Program Manager managing their Sales Transformation initiatives. He obtained his PhD from the University of Texas in San Antonio in 2007. His areas of research interests include information systems, professional culture, and security culture. His work has appeared in the *Journal of Information Systems Security* and *Communications of the Association for Information Systems* and has been presented at international conferences.

**V. Srinivasan (Chino) Rao** is a Professor of Information Systems at the University of Texas at San Antonio. He obtained his PhD from the University of Texas at Austin. His areas of research interest include electronic commerce, behavioral issues in computer security, and professional cultures. He has published in leading academic journals, such as *MIS Quarterly*, *Management Science, Communications of the Association for Information Systems,* and *Group Decision and Negotiation.*

**Tim Goles** earned his PhD in MIS from the University of Houston. Prior to that, he was employed for over fifteen years in the information technology field. His industry experience includes outsourcing contract management, information systems security, and evaluating, developing, and implementing strategic and operational information systems. His scholarly work has appeared in numerous journals and has been presented at national and international conferences.

**Gurpreet Dhillon** is a Professor of Information Systems in the School of Business, Virginia Commonwealth University, Richmond, USA. He holds a PhD from the London School of Economics and Political Science, UK. His research interests include management of information security and ethical and legal implications of information technology. His research has been published in several journals including *Information Systems Research, Journal of Management Information Systems, Decision Support Systems, Journal of Strategic Information Systems,*

*Information Systems Journal, European Journal of Information Systems, Information & Management, Communications of the ACM,* and *Computers & Security,* among others. Gurpreet has authored seven books including *Principles of Information Systems Security: Text and Cases* (John Wiley, 2007). He is also the Editor-in-Chief of the *Journal of Information System Security*. Gurpreet's research has been featured in various academic and commercial publications and his expert comments have appeared in the *Knowledge@Wharton*, *New York Times*, *USA Today*, *Business Week*, and *NBC News*, among others.

Communications of the Association for Information Systems

ISSN: 1529-3181





Communications of the Association for Information Systems