THE UNIVERSITY OF TEXAS AT SAN ANTONIO, COLLEGE OF BUSINESS

Working Paper SERIES

Date May 9, 2012

WP # 0021IS-19-2012

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

**Sriraman Ramachandran**
**Dell, Inc.**

**V. Srinivasan (Chino) Rao**
**University of Texas at San Antonio**

**Timothy Goles**
**Texas A&M International University**

**Gurpreet Dhillon**
**Virginia Commonwealth University**

UTSA COLLEGE OF BUSINESS KNOWLEDGE FOR A NEW WORLD

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

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

**Sriraman Ramachandran**
**Dell, Inc.**

**V. Srinivasan (Chino) Rao**
**University of Texas at San Antonio**

**Timothy Goles**
**Texas A&M International University**

**Gurpreet Dhillon**
**Virginia Commonwealth University**

**Work-in-Progress**
**April 2012**

**JEL CODES: M14, M15, M19**

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

## 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. This study utilizes 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, when the professions are examined independent of organizations.

**Keywords:** Information Security Culture, Professional Culture

**JEL CODES: M14, M15, M19**

## 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 et al, 2006; Straub et al, 2002]), but there is general agreement that culture includes the shared set of assumptions, values, and beliefs that help shape subsequent behavior of a social group [Kroeber and Kluckhorn 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]. 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 et al, 2007, Vroom and Von Solms, 2004]. However, there is a paucity of

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

research on the topic of information security culture. So, an overarching goal of our research stream is to contribute to the body of literature in this area.

Culture is often treated as a monolithic construct. However, some researchers have proposed that organizations can have differentiated cultures [Chatman et al,et al, 1998, Jermier et al,et al, 1991, Martin et al,et al, 1983], and that one source of differentiation may be the diverse professions or occupations present within the organization [Trice, 1993]. Professional cultures exist independent of the organizational affiliation of individual members [Trice, 1994]. Consequently, within an organization, the cultural beliefs and behaviors result from a combination of the influences of organizational and professional cultures. In addition to the cultural differentiation that may exist as a result of the presence of diverse professional groups in organizations, organizations may also have cultures related to the goals of the organization. High tech organizations may seek to create an innovative culture, while companies selling undifferentiated products may strive to create a culture of customer service to gain an advantage over their competitors. In addition to these, organizations may strive to have an ethical culture or safety culture.

Our research is based on the premise that information security cultures in organizations will be differentiated, and that the differences must be accounted for to understand and improve information security cultures. The overall research is viewed as a two-step process. The first step is to empirically demonstrate that there are variations across the information security cultures of professions, when studied independent of organizations. The second step would be to examine if some or all of the differences persist when the information security cultures of the diverse professions are examined in a single organization. Empirical support for variations in information security culture across professions will confirm our premise and argue for the accommodation of these differences in future studies. In the current article, we focus on the first step, i.e., we report the results of our research on the variations in the security cultures of four professions, independent of organizations.

Empirical studies of culture have used both qualitative and quantitative approaches. Qualitative studies such as ethnographic studies are popular in anthropology, case studies are often employed to examine organizational culture. Such studies provide rich descriptions of culture. In contrast, other scholars have developed scales to characterize cultures, e.g., Hofstede's (1980) scales for national culture and the inventory of organizational culture [Cameron and Quinn 2006]. Such scales facilitate quantitative analysis. Our goal for the current study was to conceptualize and develop rich comparative descriptions of security culture for each of the professions considered[2]. Hence we have adopted a qualitative approach.

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.

## II. LITERATURE REVIEW

### Culture

The complexity and ambiguity associated with the study of culture has been acknowledged by scholars [Leidner et al, 2006, Schein 2004, Trice and Beyer 1993]. For purposes of this study, we adopt the Kroeber and Parsons (1958, p. 15) definition of culture as the ".. 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." Thus, information security culture involves identifying the ideas, beliefs and values of the group, which shape and guide security-related behaviors.

### 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

[2] The subtle distinctions between the terms profession and occupation are not relevant to the primary theme of this study, i.e., an examination of the security cultures.. We use the terms profession and occupation interchangeably.

share a set of values, norms and attitudes, all of which form a part of their occupational culture [Van Maanen and Barley, 1984].

More recent research has found evidence supporting the existence of a distinct occupational culture among IS professionals [Guzman et al, 2004, Guzman et al, 2008]. 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].

This brief review indicates that groups belonging to different professions can have distinct values and beliefs. Consequently, our premise is that different professional groups are likely to have distinct values and beliefs that would constitute distinct security cultures of their own.

## Security Culture

Of particular relevance to this study is the concept of security culture. This refers to the "behaviors, attitudes, and values that contribute to the protection of all kinds of information in a given organization [Dhillon 1995, p. 5]. 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]. A strong security culture can increase awareness of and commitment to an organization's security mission, and ingrain security-related behaviors into the day to day activities of employees [Siponen 2000, Von Solms 2000].

The study of security culture is in its infancy. Issues are still being identified and conceptualizations explored. Some researchers have attempted to map conceptualizations of security culture to existing models of culture [e.g., Schlienger and Teufel 2003, Zakaria and Gani 2003]. These efforts, however, are primarily at the organizational level of analysis. In general, they map organizational assumptions, values, and artifacts to behaviors and management actions. Since our focus is on the culture of professional groups across organizations (and not within), the organizational perspective is not a good fit.

Other scholars have drawn on frameworks from management and industrial psychology to propose dimensions of security culture [Chia et al, 2002, Tejay and Dhillon 2005]. This approach is more pertinent to our purposes, and so we utilize it to further our study. A comparison of the dimensions proposed in the two studies indicates that there is a loose overlap of some concepts underpinning various dimensions (see Table 1 in the Theoretical basis section), but there are also factors in each study that do not have corresponding factors in the other. This indicates that agreement on the dimensions or factors of security culture is still evolving, and that security culture does not fit neatly into a single framework. It has even been suggested that "the concept of a security culture is too complex to be covered by a single framework or model" [Ruighaver et al, 2007, p. 61].

To summarize, prior research on professional cultures suggests that different professional cultures have different beliefs, values, and associated behaviors. Research into security culture is still in its infancy, with no generally accepted frameworks or dimensions. Furthermore, the little published research that exists conceptualizes security culture in the organizational context. This study explores a hitherto unexamined aspect of security culture; that is, security culture in the context of professional groups. This is significant because organizational culture consists of various subcultures, including professional groups. Enhanced understanding and improvement of organizational security is likely to be facilitated by enhanced understanding of security culture at the professional group level.

## III. THEORETICAL BASIS

The current study describes and compares the information security cultures of different professions. To build such an understanding, existing theoretical conceptualizations of security culture have been used as a starting point. The *a priori* description of conceptualizations, constructs, dimensions and relationships can help develop a study’s initial design [Eisenhardt 1989]. In this research, due to the lack of theories on security cultures at the professional level, existing conceptualization of security cultures at the organizational level is used to help the initial understanding of the concept of security culture at the professional level and also to help design the study.

The theoretical conceptualization of security culture is derived from two earlier studies [Chia et al, 2002, Tejay and Dhillon 2005]. While the results of neither study are fully established and validated, they are the best available theoretical perspectives to use as a starting point. Further, these studies are focused on security culture in the context of organizations. So, we selected those factors that made sense in a professional context to create a framework that conceptualizes security culture at the professional group level.

The process of conceptualizing security culture was done as follows. The dimensions proposed in the two previous studies [Chia et al, 2002, Tejay and Dhillon 2005] were mapped to each other to the extent possible. Then for each of the dimensions, we created a list of issues that would help us create questions for the semi-structured interviews (See Table 1).

In reviewing the issues that we generated, we felt that they fit neatly into a framework of three categories: beliefs about professional identity, general beliefs about risk taking, and security related beliefs. A group's identity addresses its own perceptions of its core values, who they are and what their role is, and what their value to the organization is. These perceptions may shed light on security-related beliefs. For example, a group which 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. Similarly, a group's general beliefs about risk taking, and complying with rules and regulations may also help us understand the group's beliefs about security risks, rules and regulations. Groups that are risk averse in general are likely to carry over that aversion to the area of information security also.

Finally, security related beliefs have been categorized into: what is information security, importance and awareness of security issues, who is responsible for information security, the responsibility of the group for information security, existence of security risks, compliance with security rules and regulations, and, other responsibilities that may conflict with their responsibilities to security.

In effect, we have transformed the prior dimensions into a more parsimonious framework to conceptualize security culture. Our framework contains those key dimensions applicable to professional security culture from both prior conceptualizations.

**Table 1. Mapping of Dimensions of Security Culture**

| Chia et al (2002) | Tejay and Dhillon (2005) | Listing of Preliminary Issues to Develop Interview Questions |
|---|---|---|
| The balance between short term and long term security goals in an organization | Planning | This is relevant at an organizational level; not at a professional level. |
| Rewards, punishment and motivation structure in the organization installed to motivate employees behavior towards IS security | Organizational structure, Planning | This is relevant at an organizational level; not at a professional level. |
| Inclination towards risk by the management and employees of the organizations | Information security awareness<br>Information work practice | 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>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 |
| Pervasiveness of IS security in the daily work practices of the employees | Informal work practice | What are usual steps to be taken in complying with security? |
| Level of involvement of employees in managing IS security in an organization | Information security awareness | What is security?<br>What are steps in complying with security?<br>Who is responsible for information security?<br>What role does group play in ensuring information security? |
| Empowerment of employees, so as to instill responsibility towards IS security related actions, | Organizational structure, Planning | Not applicable at professional level; organizations empower employees; not relevant at professional level |
| Level of balance maintained to satisfy external and internal influences on IS security | | Not applicable at professional level |
| The basis of truth and rationality that security is important, | | What  is security?<br>What is responsibility of profession? |
| | Professional codes | Core value of profession<br>Role of profession<br>Contribution to organization / society |
| | Group cohesiveness | Not applicable at professional level |

## IV. METHODOLOGY

Given that neither of the prior conceptualizations [Chia et al, 2002, Tejay and Dhillon 2005] have strong empirical validation, it was considered appropriate to conduct a qualitative study. A qualitative study using semi-structured interviews permits the flexibility necessary to explore issues that emerge during the course of the study. Our efforts were guided by suggestions from other scholars for conducting qualitative studies [Dube and Pare 2003].

### Respondents

**Table 2. Demographics of Respondents**

| | IS Professionals | Marketing Professionals | HR Professionals | Accounting Professionals |
|---|---|---|---|---|
| **No. of Respondents** | 15 | 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. |

Using theory based conceptualizations of security culture, our goal is to identify ideas, beliefs and values on issues related to security for four different professions, and view them from a comparative perspective. The accounting and human relations professions were chosen because they have legal obligations with respect to confidentiality and privacy, and were perceived to be concerned about information security. The marketing profession was chosen because it has a relative lack of legal or regulatory security-related constraints, and hence is less likely to be concerned about information security. The information systems profession was chosen because of the general perception that it is responsible for information security. The study is based on qualitative methods, primarily semi-structured interviews of members from each of the professional groups.

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 United States of America. Demographics of the respondent pools for each profession are shown in Table 2.

## Data Collection

The primary method of data collection used in the current study was semi-structured face-to-face interviews. The structured questions focused on getting responses to issues identified in the conceptual framework. 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 3.

Interview guides containing detailed list of questions were developed and used. 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 on their own personal beliefs and behaviors. They were encouraged to illustrate general observations with examples, when possible. Towards 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 3. Sample Questions Used in Interviews**

| Category | Sample Questions |
|---|---|
| **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 or 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 towards 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 be 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 does the term "information security or IS security" mean to members of your profession? |
| What are steps in complying with security? | What does information security involve? |
| Who is responsible for information security? | Who do the members of your profession think should be responsible for IS security? |
| What role does group play in ensuring security | What role do the members of your profession think they play with respect to IS 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 problems with the interview scheme.

### Analytical Procedures

Generally accepted techniques [Miles and Huberman 1994] were used for analyzing the data. The interviews were transcribed, identifiable 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. Only a sample of the codes is shown in Table 4 because of space considerations[3]. Inter-rater reliability of coding was 0.83.

**Table 4: 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 issues in organizations | 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 issues | Bel_InfoSec_Prod_Cnx |

The process of generating a narrative is described. The software package (Atlas.Ti) was used to extract clusters of quotes associated with one or more codes from the interview transcripts. Sample responses for one cluster, "who is responsible for information security in an organization" are shown in

[3] Complete list of codes is available on request.

Table 5. Brief notes are made, and a summary of beliefs surfacing from the responses are noted. In Table 6, 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 5: Sample Responses and Summary Notes for One Code**

**Sample of Responses and Summary Notes**
**Who do IT professionals think is responsible for security?**
**(Code: Bel_InfoSec_Responsibility_is)**

Q: Who do IT professionals think is responsible for information security within organizations?

P3: IT professionals

-------------------

Q: Who do IT professionals think is responsible for information security within organizations?

P4: IT professionals

----------------

Q: Who do IT professionals think is responsible for information security within organizations?

P5: Everybody

---------------

Q: Who do IT professionals think is responsible for information security within organizations?

P6: Themselves [IT professionals]

------------------------------------

Q: Who do IT professionals think is responsible for information security within organization?

P7: CIO at the very end. But, it comes down to IT professionals themselves including the security staff and IT professionals that you have.

---------------------------------------------

Q: Who do IT professionals think is responsible for information security within organizations?

P11: The trend today is that you have an actual security team.

Q: what if they don't have an actual one?

P11: Who ever they happen to have working in IT, if they don't have a security team. But, most large organization has security team.

-----------------------------------------------------------------------

**Notes for "Who do IT professionals think is responsible for security?"**

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 state that management or CIO is ultimately responsible for security. Only one respondent viewed information security as everyone's responsibility.

## Table 6: Generation of Narrative from Summaries

### Development of Narrative from Summary Notes for Multiple Codes

**Notes for "Who do IT professionals think is responsible for security?"**

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 state that management or CIO are 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, protect from hackers. Making sure data is not tampered with.
Protecting technology resources: network, infrastructure
Networks, computer systems and applications
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
Passwords, physical security, authorized access.
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, 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, etc:, and, also planning, 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.

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

## 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 the four different professional groups, and explores the relationship among the three categories.

### 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 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.”*

Recent 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 corporate accounting scandals of recent years (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 viewed themselves as champions of the employees, ensuring equal treatment of all employees, and advocating for their causes, which sometimes involved 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 will 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 which 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.

**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 it's [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 towards 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 which 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, and federal and state regulations governing treatment of employees.

> HR professional: "*Because a lot of the rules that are in place in HR is 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 be 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 of 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*

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

> *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."*

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, and, the need for hierarchy. They believe in minimizing risk, and complying with rules and regulations. They believed that a hierarchical structure was necessary for the orderly functioning of a system.

**General Beliefs of Marketing Professionals:** Marketing professionals present a consistent picture of a group prone to taking risks, with an open disregard for rules, and a relative lack 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 it and if there is a loophole you can go through it. But, if it is not bendable or a loop hole 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 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 that 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 marketers 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 ‘cowboys’, 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 organizations 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, and 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 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**: 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 almost at will, 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 don't 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, their awareness of security issues, their propensity to take security risks in general, and 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 from 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 is 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 recent 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 towards the protection of information assets in organizations.

**Security Beliefs of HR Professionals:** HR professionals indicated that their beliefs about information security comes 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 employee file is kept confidential and only certain individuals have access to various levels of information such as social security numbers, birthdays, marital status 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 its 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, 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, its lot of information that the customers would not be happy if someone else got their hands on it."*

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 fail to provide relevant information in a timely manner. In fact, IS professionals believed that their group that 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 towards 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 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 Security Beliefs**: In this study, 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

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 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 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 what literature 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. These propositions will also serve to 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).

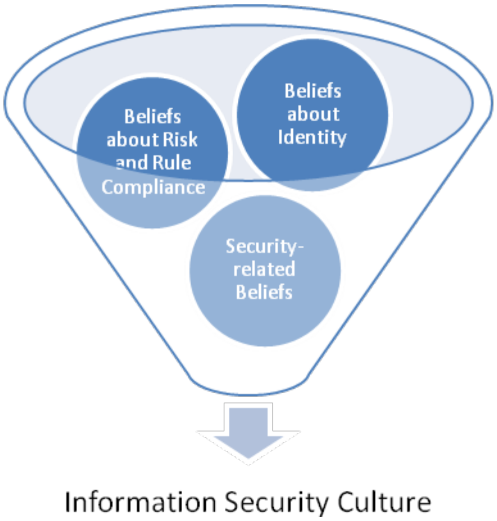
Beliefs about Risk and Rule Compliance
Beliefs about Identity
Security-related Beliefs
Information Security Culture

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

Thus, our work reframes the dimensions, particularly those relevant to professions, proposed in two earlier studies [Chia et al, 2002, Tejay and Dhillon 2005]. The results in this study show a consistency between the three categories of beliefs. Groups whose role requires generally rule compliant behaviors tend to believe in complying with security rules and procedures. 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.

**Security Cultures of Professions:** The professional culture literature reports that there can be major differences in cultures across professions [Trice 1993]. This study shows that security cultures can also differ across professions. Much of the literature on security culture has focused on conceptualizing security culture: that is, defining the term and identifying dimensions [Chia et al, 2002, Tejay and Dhillon 2005], and arguing for the development of strong security culture at the organizational level. Based on our finding that there are differences in security cultures across professions, it may be argued that when studying security culture in an organizational environment, attention should be paid to these differences. Hence Proposition 2.

**Proposition 2**: Information security cultures vary across professions.

**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]. 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 can be inconsistencies between security related beliefs and security related behaviors, particularly at times of performance pressure.

It is interesting to 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.

**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]. 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.

**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 towards 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.

## 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 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 preliminary qualitative empirical support 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, we have shown that while there are overlaps between the security cultures of different professions, there are also differences. The practical implication of this relates to the development of security culture 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.

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 arguments 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.

Fourth, our study shows that while all professional groups acknowledge some responsibility for information security, there is 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. The practical implication of this is that users need to educated more on their role in ensuring information security.

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

There was no well established conceptualization of security culture, only two proposed conceptualizations with some preliminary validation. This created a necessity to develop a proper framework to conceptualize security culture, which we have done in this study. The robustness of our conceptualization will have to be established in future research employing large scale surveys. Future research also needs to examine how to cultivate a strong security culture along with a culture of productivity, how to leverage security-related beliefs prevalent in professional groups to strengthen security culture in organizations, and, to understand why security-aware users continue to deviate from security policies and regulations.

## 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 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. The second author would like to thank the Dean of the College of Business for funding his participation in the research.

## REFERENCES

Cameron, K. S. and R.E. Quinn. (2006) *Diagnosing and Changing Organizational Culture*, San Francisco, CA: Jossey-Bass,.

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*, Japan.

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

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

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

Dube, L., and Pare, G. (2003) “Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations,” *MIS Quarterly,* 27(4), pp. 597-635.

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

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, Arizona, pp. 74-80.

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

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

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

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

Kroeber, A.L., and C. Kluckhohn (1963) *Culture: A Critical Review of Concepts and Definitions.* New York: Random House.

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

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.

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

Martin, J., Feldman, M., Hatch, M., & Sitkin, S. (1983) "The Uniqueness Paradox in Organizational Stories," *Administrative Science Quarterly*. 28, pp.438-453.

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

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

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. (2004) *Organizational culture and leadership* (3rd ed.). San Francisco: Jossey-Bass.

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, 2003.

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

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.

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, 2005.

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.

Van Maanen, J. (32) "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 *Research in Organizational Behavior,* B.M. Staw, and L. Cummings (ed.), Stamford, CT : JAI Press, 1984, pp. 287-365.

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

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 *2$^{nd}$ European Conference on Information Warfare and Security*, Reading, UK, 2003.