Information Security Cultures of Four Professions: A Comparative Study

Sriraman Ramachandran, Srinivasan V. Rao, Tim Goles
Department of Information Systems and Technology Management
The University of Texas at San Antonio
sriraman.ramachandran@utsa.edu, chino.rao@utsa.edu, tim.goles@utsa.edu

Abstract

Differences in cultures across professions have been reported in the professional culture literature. An understanding of such differences is important to understand the effects of culture. We extend this argument to the area of information security. We argue that it is necessary to examine the information security cultures[1] of various professions to identify differences that may exist, so that they may be taken into account in formulating initiatives to enhance information security. In this article, we provide a comparative description of the security cultures of four professions -- information systems, accounting, marketing and human resources – based on semi-structured interviews of respondents from each of the professions. Our results confirm the existence of differences in security cultures across professions. In particular, they indicate that there are differences in beliefs about what constitutes information security, who is responsible for it, and the likelihood of their compliance with security under performance pressure.

1. Introduction

Literature in the area of culture includes studies both at the organizational level and professional or occupational[2] level [1]. Scholars of occupational cultures have established that distinct cultural beliefs can develop among members of a profession or occupation [1]. Further, researchers including IS scholars, have established that in an organizational setting, employee behaviors are influenced not only by cultural beliefs of the organizational system they are part of, but also by the cultural beliefs of the profession that they belong to [1, 2]. Thus, understanding the beliefs and behaviors of employees belonging to different professions requires an understanding of the cultures of the different professions. Similarly, in the domain of information security, it can be argued that an understanding of the information security cultures of different professional groups is necessary to understand the security-related beliefs and behaviors of their members in organizations. To date, information system scholars have limited the focus of the studies on information security culture to studies at the organizational level. There is no published study of information security culture at the professional level. Our longer term research program is to address this research niche, i.e., examine if differences are present in information security cultures across different professions, to identify the differences, and to research the effects of the differences. In the current study, we examine four different professions, -- information systems [IS], marketing, accounting and human resources [HR] -- and, provide a comparative description of their information security cultures.

Kroeber and Parsons [3, pp. 15] define 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 security related ideas, beliefs and values of the group, which shape and guide security-related behaviors. 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 information systems profession was chosen because, anecdotally, they are perceived as being responsible for security. The marketing profession was chosen because it was believed that they were less likely to be concerned about information security. The accounting and human relations professions were chosen because they have legal obligations with respect to confidentiality and privacy, and were perceived to be more likely to be concerned about information security.

The rest of the article is organized as follows. In the next section, we discuss relevant literature.

[1] We use the term security culture interchangeably with information security culture. In the current study, our focus is on safeguarding information.

[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 of different groups. We use the terms interchangeably.

1530-1605/08 $25.00 © 2008 IEEE

Following which, we outline the theoretical bases and methodological issues. Next, we discuss our findings. In the last section, we offer a discussion of the results.

2. Literature Review

2.1 Professional Cultures

The existence of distinct cultural characteristics unique to individual professions has been documented in literature (e.g., accountants [4], doctors [5] and engineers [6]). Accountants view themselves as rationalists [4], who believe that the primary reality is cold-blooded "bottom-line" [1]. The official culture of doctors is rooted in the Hippocratic Oath [7], which emphasizes the need to keep the good of the patient in mind. Kunda [6] describes the engineering culture in a high technology firm as being informal, where initiative and trust are important, and "working for money as a prime motivator will be abhorred" [6, pp. 75]. These descriptions support the idea that employees who practice the same profession tend to band together into communities, draw their identities from the work they do, and, proceed to share a set of values, norms and attitudes, which form a part of their occupational culture [8].

More recently, evidence for the existence of a distinct professional culture among IS professionals has been presented ([9], [10]). These studies have shown that the IS professionals have a converging cluster of characteristics, which reflect the technical nature of the occupation, the responsibilities of IS personnel associated with technology, the use of technical jargon of IS personnel and so on. Guzman et al [9] also report that managers view IS professionals 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" [9, pp.79].

This brief review indicates that groups belonging to different professions have some distinct beliefs of their own. Our premise is that along the same lines different professional groups are likely to have distinct security cultures of their own.

2.2 Security Culture

Most of the existing literature discusses security culture in the context of organizations. Our study is centered round the security cultures of diverse professional groups outside the context of organizations, i.e., groups, in which individuals belong to the same profession but do not necessarily work for the same organization. Once factors related to organizational context are removed, the conceptualization of security culture in current literature is relevant and appropriate for understanding security cultures of professions. The literature on security culture is briefly reviewed here.

Dhillon [11] defines security culture as "the totality of human attributes such as behaviors, attitudes, and values that contribute to the protection of all kinds of information in a given organization." This generally accepted definition serves as a starting point for our research. Further conceptualization of security culture follows one of two paths. First, scholars, such as Schleinger and Teufel [12] and Zakaria and Gani [13], attempt to map the conceptualization of security culture to existing models of culture (e.g., Schein's [14] model). Second, scholars such as Chia et al.[15] and Tejay et al. [16] propose dimensions of security culture based on frameworks from the management and industrial psychology. We limit our review to the studies in the second category, in which researchers propose dimensions of security.

Chia et al [15], and, Tejay and Dhillon [16] have used theory-based approaches to propose dimensions for security culture. Chia et al [15] based their suggestions on the dimensions proposed in Detert et al's [17] framework for total quality management issues, while Tejay and Dhillon [16] base theirs on Hall's [18] classification of behavioral responses to the implementation of a new computer based system in an organization.

Chia et al [15] propose eight IS security topics that could be used to describe the security culture of an organization. These are: (i) the basis of truth and rationality that security is important, (ii) the balance between short term and long term security goals in an organization (iii) rewards, punishment and motivation structure in the organization installed to motivate employees behavior towards IS security, (iv) inclination towards risk by the management and employees of the organizations, (v) pervasiveness of IS security in the daily work practices of the employees, (vi) level of involvement of employees in managing IS security in an organization, (vii) empowerment of employees, so as to instill responsibility towards IS security related actions, and, (viii) level of balance maintained to satisfy external and internal influences on IS security. They develop a qualitative comparison along the security culture dimensions of two organizations. Their results indicate differences between the two organizations on several of the dimensions.

Tejay and Dhillon [16] base their development of constructs on Hall's [18] classification of behavioral responses to the implementation of a new computer based system in an organization. The responses or behavioral patterns are referred to as silent messages. Following Dhillon's [11] examination of the implications of the silent messages for information security, Tejay and Dhillon [16] have developed these further to propose constructs for information systems culture. The seven constructs that they have proposed are group cohesiveness, professional codes, informal work practice, empowerment, planning, information security awareness and organizational structure. Tejay and Dhillon [16] have developed items and demonstrated the validity of some of the factors.

Some of the factors identified by Chia et al [15], and Tejay and Dhillon [16] to describe security cultures in organizations overlap with each other, even though they originate in different fields. Some of the common factors in their conceptualizations of security culture are: the existence of proper planning of security related initiatives, empowerment of the employees to independently take security actions, existence of organizational structures like rewards, and, the level of balance between external and internal factors influencing the employees' behaviors. There are additional factors in the each of the studies which don't have corresponding factors in the other study. Thus, it would appear that the factors or dimensions that contribute to the conceptualization of information security culture are still evolving.

In summary, literature on professional cultures indicates that cultural differences exist between professions. Literature in the area of security shows that research on information security culture is still in its early stages of development. Issues are still being identified, and, conceptualizations being explored. To date, most articles on security culture examine security culture in the context of an organization. We know of no study that examines the security cultures of professions. We believe an understanding of security cultures at a professional level is important because they have to be accounted for in understanding security culture in an organization.

3. Theoretical Basis

The current study attempts to compare the information security cultures across different professions. The theoretical conceptualization of security culture is derived from the Chia et al [15] conceptualization based on Detert's [17] taxonomy, and, the Tejay and Dhillon [16] conceptualization based on Hall's taxonomy. Since neither is fully established and validated, we have chosen to draw from both these perspectives to include factors that would help us describe the security cultures of different professional groups. We have included those factors that made sense only in a professional context. We have focused on understanding the groups' beliefs about the following: 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. Each of these factors is directly or indirectly related to factors proposed by Chia et al [15] or Tejay and Dhillon [16].

In addition, we include factors that identify the groups' perceptions of their identities and other relevant beliefs. We argue that a group's identity addresses its own perception of who they are and what their role is – and that this perception will shed light on its security-related beliefs. Similarly, a group's general beliefs about risk taking, and, complying with rules and regulations may help us understand the group's beliefs about security risks, rules and regulations.

Thus, the comparison of the information security is strongly rooted in prior theoretical bases used by Chia et al [15] and Tejay and Dhillon [16], and, includes additional factors to develop a better understanding.

4. Methodology

We employ qualitative methods. Interview protocols were developed, based on various issues identified from pilot interviews, and also from issues suggested by Chia et al [15], Tejay and Dillon [16], and, Stanton et al. [19]. The standard structure of the questionnaires focused on identifying the following three sets of beliefs -- beliefs about their identity of the profession, general beliefs, and, beliefs about information security – for each of the professions. Respondents were asked questions only about their profession.

Subjects 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 1.

The interviews were transcribed, identifiable information removed, coded, and analyzed using the

techniques suggested by Miles and Huberman [20]. Inter-rater reliability of coding was 0.92.

	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.

Table 1: Demographics

5. Results

Our interest is in comparing the security cultures of different professions. This section includes discussions of the identities, the general beliefs and the security-related beliefs of the professional groups to enable the reader to observe the relationship among the three categories.

5.1 Identities of Professions

The identity of a professional group is its perception of itself, formed from its core values, and, its perception of what the occupation contributes to society and organizations. In our study, the core values of the different groups have common threads, i.e., honesty, integrity, service to the organization and society. However, each group's perception of its role in the organization is quite distinct. The role is embodied in their belief that they bridge the organization and another entity, the entity being related to their special area of expertise. For instance, IS professionals view themselves as moderating the relationship between the organization and information technology. They believe they are the experts in the realm of information technology and that it is their charge to develop and maintain the technical infrastructure and solve user problems, and thus provide value to the organization. Marketing professionals view themselves as the group, which bridges the organization and its customers. They believe that they provide value by enabling organizations to understand the market and the customers, by effectively disseminating information about the organization's products to the market, by increasing market share, and being competitive. Accountants see themselves as the bridge between the owners (shareholders) and the agents (the managers).

> *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.*

Accounting professionals believe that they provide value by generating reports that helps managers make the correct decisions.

> *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. Accountants provide the feedback for decision makers.*

HR professionals mediate the relationship between the organization and its employees. They believe that their role is to ensure the equal treatment of all

employees, as required by federal regulations and / or organizational policies. Further, they provide value by helping 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.*

It can be seen that IS and marketing professionals identify more with productivity responsibilities. IS professionals view their role as increasing organizational efficiency and effectiveness, and, marketing professionals view their role as increasing sales and profitability. In contrast, both accounting and HR professionals believe their roles to be more of control than productivity, i.e., ensuring that the organization is staying within some designated parameters. Accountants are concerned about the correctness of the financials, i.e., they monitor and control reporting activities. HR professionals monitor and control the treatment of employees.

5.2 General Beliefs

The general beliefs of interest to us are beliefs of professionals about risk, their beliefs about the observation of rules and procedures, and, their beliefs about hierarchy and managerial guidance. These are relevant because we believe groups prone to taking risks are also likely to take chances with security. In a similar vein, security needs are met by formulating rules and regulations 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 also. Lastly, their beliefs about hierarchy and managerial guidance provide a basis for understanding how they may react to managerial initiatives about security.

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. IS professionals are risk averse, but seem somewhat resistant to the idea of rules. They acknowledged the need for hierarchy, but saw a limited role for managerial directives. 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.

The similarities between the accounting and HR professionals are understandable. Both professions are rooted in rules and regulations. Accountants are bound by generally accepted accounting principles (GAAP) and federal and state regulations that govern record keeping; HR professionals are bound by organizational policies, and, federal and state regulations governing treatment of employees.

> HR professional[3]: *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'. Its 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. In contrast to marketing professionals who see taking risks as the path to success, both accountants and HR professionals see it as important to avoid risk.

> Accounting professional: *They* [accounting professionals] *are very skeptical towards taking risk because underlying principle for accountants is conservatism. If you are ever skeptical about an event or transaction or you feel that it is risk then you lean more towards conservatism.*
>
> HR professional: *I would say that they are risk averse. Because large part of our job is to ensure that organization and employees are meeting certain regulations, certain standards set by the federal state local governments. So, we are in the mode of compliance. So, taking risk is kind of going outside of that.*

Accountants further extend their risk-aversion to other beliefs that reduce organizational risk. Their work deals financial data. Accuracy of such data is critical, and thus they consider it best to ratify work done at the lower levels by managers. This is consistent with their beliefs about the need for hierarchy in organizations, which delineates responsibilities and allows for managerial guidance and supervision.

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*

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

nature. There was an emphasis of you always knowing your place in the machine.

Thus, accountants and HR professionals present a coherent picture in their beliefs related to risks, rules and regulations, and, need for hierarchy.

In contrast, IS professionals present a somewhat confused picture with respect to their beliefs on the same issues. They believe that they are risk averse.

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.

But with respect to selected activities, IS professionals they see risk as unavoidable. For instance, they believe that software development is risky because of the ongoing innovations in technology.

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 the group should have the freedom to get their tasks accomplished without micromanagement.

Thus, IS professionals present a mixed picture. The group recognizes the criticality of the information infrastructure under their charge and this causes them to be risk averse. On other fronts, their beliefs reflect a group that wants independence, and does not want to be shackled by rules or managerial directives.

Marketing professionals present a consistent picture of a group prone to taking risks, with an open disregard for rules, and a relative disconcern 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 possible.

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 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.'*

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

In terms of general beliefs, accountants and HR professionals are at one end, with marketing at the other. 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.

5.3 Security-related Beliefs

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.

In our 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 is information security, 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.

Respondents from accounting pointed out that professional associations, like American Accounting Association, American Institute of Certified Public Accountants (AICPA) and so on, 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 term information security. They view it as including the safeguarding of all the information in the organization, and, the associated information infrastructure. The information encompasses accounting information, sales information, employee information and so on, and, infrastructure protection includes actions like locking server rooms, protection of physical files and so on. Consistent with this, they believed that all employees and departments shared the responsibility for information security in the organization. However, a few of them acknowledged that IS professionals had a special responsibility to lead on security issues, and, that accountants had 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. 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. Thus, it is clear that 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 reported that the laptops were stolen. I took mine when I was on vacations.*

Overall, the accounting profession appears to have cultivated a strong culture in terms of information security. Their mindset of observing rules aligns with the rule-oriented behaviors needed to enhance security.

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 individual have access to various levels of information such as social security numbers, birthdays, marital status things like that.*

Their awareness of information security risks was also limited. Their perception of their limited role in information security is complemented by a belief that it is the responsibility of IS professionals to deal with security. However, they were quite willing to comply with security rules and regulations.

> *...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.*

Presumably, 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 reason for the willingness to follow security rules unquestioningly.

HR professionals, similar to their accounting counterparts, have been subject to privacy and confidentiality laws in the recent past. 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.*

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.

IS professionals get most of their information about information security from professional sources. In particular, they did not see either the organization or the media as a useful source. Both these sources were considered reactive, and thus too late with any relevant information. In fact, IS professionals believed that they are the 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 structure, which includes the computers, networks, and the software applications. They believe that they are highly aware of the risks associated with information security. They also believe that they are responsible for information security in the organization. As those primarily responsible for security, they said they would not violate security rules. In their opinion, the potential negative consequences of violating security rules were very high and not worth the risk. However, they readily admitted that under performance pressure, they would favor performance and productivity over security related issues.

> *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 it's 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, if they had to choose 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.

Marketing professionals said that most of their knowledge about security came from within the organization, little from outside. They have a very limited perspective of information security. They viewed information security to be the protection of information on customers, for which they believed that they were responsible. 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.*

They did however say that they would observe security regulations. 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. 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, i.e., performance needs seem to take precedence over security.

5.4 The Information Security Cultures

The security-related beliefs of professionals taken together with their 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, and the marketing profession a weak security culture, with the IS and HR professions lying between the two.

Accounting professionals have a holistic view of security. 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. Once again, these security-related beliefs are in keeping with their primary culture of rule compliance and willingness to follow directives.

Marketing professionals view security as the responsibility of management and IS professionals, and, follow rules that are formulated only to the extent such rules do not get in the way of their productivity or performance. These beliefs about security are consistent with their general beliefs that they need to take risks to accomplish goals, and rules can be bent in the accomplishment of the goals, even as management directives can be sometimes ignored.

HR and IS professionals seem to fall in between accounting and marketing professionals. IS professionals view themselves as responsible for security and are more aware of the risks associated with security. HR professionals accept responsibility for the data under their jurisdiction, but appear to be less aware of the technical risks, viewing those as the responsibility of IS. But under performance pressure, HR professionals are more security conscious, whereas IS professionals tend to focus more on their performance goals.

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

6. Discussion and Contributions

The professional culture literature reports that there can be major differences in cultures across professions [21]. This study shows that security cultures can also differ across professions. Much of the literature on security culture has focused on conceptualizing security culture, i.e., defining the term and identifying dimensions [15, 16], 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 when formulating security initiatives.

We have also shown that security-related beliefs in different professions correlate well to the identity of the profession and other related general beliefs, e.g., risk propensity and rule compliance. Thus, in understanding the security culture of a group, professional or otherwise, it is worthwhile to simultaneously examine the group's identity and other related beliefs.

Semi-structured interviews examining self-reported beliefs and behaviors are likely to suffer from social demand bias in the answers of the respondents. It would be politically incorrect for subjects to indicate that they believed that security was unimportant, or that they would violate security rules. Further, they would have to be discreet about any security violations that they may have engaged in or observed. Either in keeping with these, or responding truthfully, subjects belonging to all professions said that they believed that security rules should not be violated. IS and marketing professionals readily admitted their bias to production-related objectives over security expectations. 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. Thus, there are differences between stated beliefs and actual practices. Martin [22] defines this inconsistency as action inconsistency in her discussions of differentiated culture, i.e., a culture in which inconsistencies exist. Such inconsistencies seem more likely in security culture, when groups believe that their primary responsibility is to enhance organizational performance. In our study, both marketing and IS professional groups viewed their primary responsibility as contributing to organizational performance. Guzman et al [9] reports that senior managers view the role of IS as improving efficiency and effectiveness. Thus, in spite of their beliefs that they will observe security rules, their actions may sometimes be different.

Our results indicate the IS group is seen as a key player, if not the leading player, in security initiatives. This reflects a techno-centric view of security. Accounting professionals appear to have a more holistic perspective, but still see a significant role for the IS group. Researchers have emphasized the dangers of viewing security as a technical problem [23, 24]. Earlier researchers have mentioned that managers also tend to view information security as a technical issue that is the responsibility of IS professionals [see 9]. 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.

Literature emphasizes the importance of information security awareness of users. For instance,

Siponen [24] indicates that information security awareness plays a crucial role in effective interpretation and use of information system policies, procedures and technologies by the end-users. Our study suggests that a rule compliant mindset may be more important than security awareness. The HR professionals did not claim awareness, but were willing to follow security rules even under performance pressure, with few exceptions. IS professionals, on the other hand, claimed a sufficiently high enough 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 rule compliance. This comparison of HR and IS professions suggests that while security awareness is important, a willingness to comply with rules may enhance security more.

In conclusion, using a theory-based view of security culture [15, 16], we have developed insights into the information security culture of four professional groups. These insights provide a good basis to understand and predict security related beliefs and behaviors of the groups, under different conditions.

7. References

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

[2] E. Karahanna, J. R. Evaristo, and M. Srite, "Levels of Culture and Individual Behavior: An Integrative Perspective," *Journal of Global Information Management,* vol. 13, 2005.

[3] A. L. Kroeber, and Parsons, T., "The Concept of Culture and of Social System," *American Sociological Review,* vol. 23, pp. 582-583, 1958.

[4] L. R. Pondy, "Union of Rationality and Intuition in Management Action " in *The Executive Mind* S. Srivasta, Ed. San Francisco: Jossey-Bass 1983, pp. 169-189.

[5] A. C. Smith and S. Kleinman, "Managing Emotions in Medical Schools: Students' Contacts with the Living and the Dead," *Social Psychology Quarterly* vol. 52 pp. 56-69, 1989.

[6] G. Kunda, "Engineering Culture: Control and Commitment in a High-Tech Corporation " *Organization Science,* vol. 6, pp. 228-230, 1995.

[7] Wikipedia, "http://en.wikipedia.org/wiki/Hippocratic_Oath," 2007.

[8] J. Van Maanen and S. R. Barley, "Occupational Communities: Culture and Control in Organizations," in *Research in Organizational Behavior*. vol. 6, B. M. Staw, and L. Cummings, Ed. Stamford, CT: JAI Press, 1984, pp. 287-365.

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

[10] S. Ramachandran and S. V. Rao, "An Effort Towards Identifying Occupational Culture Among IS Professionals," in *SIGMIS-CPR*, 2006.

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

[12] T. Schlienger and S. Teufel, "Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture," in *14th International Workshop on Database and Expert Systems Applications*, 2003.

[13] O. Zakaria and A. Gani, "A Conceptual Checklist of InformationSecurity Culture," in *2nd European Conference on Information Warfare and Security*, Reading, UK, 2003.

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

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

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

[17] J. R. Detert, "A Framework for Linking Culture and Improvement Initiavtives in Organizations," *Academy of Management Review,* vol. 25, pp. 850-863, 2000.

[18] E. T. Hall, *The Silent Language*. Garden City, NY: Anchor Books, 1959.

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

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

[21] H. Trice, *Occupational Subcultures in the Workplace*. Ithaca, NY: ILR Press, 1993.

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

[23] G. Dhillon, *Managing Information System Security*. London: Macmillan, 1997.

[24] M. T. Siponen, "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security,* vol. 8, p. 31, 2000.