The Role of Strong Cultures to Information Security Management: A Goal Setting Perspective

Ioannis V. Koskosas
Department of Information and Communication Technologies Engineering
University of Western Macedonia, KOZANI, GREECE, 50100
Tel: +3 24610 56500 , Fax: Fax: +3 24610 56200
E-mail: ioanniskoskosas@yahoo.com

Georgia Charitoudi
Technological Educational Institute of West Macedonia
GREECE, 50100
Tel: +3 24610 40161, Fax: +3 24610 39682
E-mail: tok0039@kozani.teikoz.gr

Malamati Louta
Technological Educational Institute of Western Macedonia
Department of Business Administration
University of Western Macedonia
Department of Information and Communication Technologies Engineering
GREECE, 50100
Tel: +3 24610 38772, Fax: +3 24610 39682
E-mail: louta@kozani.teikoz.gr

ABSTRACT

The aim of this research is to investigate the role of strong organizational cultures in setting information systems security goals. In doing so, it explores and discusses the concept of strong culture within three financial organizations with different social organizational structures and seeks to demonstrate the importance of having a strong culture in setting efficiently information security goals. The determinants of a strong organizational culture are also discussed. This research contributes to interpretive information systems research with the study of strong culture and goal setting in a security management context and its grounding within an interpretive epistemology.

Complete Research Paper

1.“INTRODUCTION”

The research described in this paper is concerned with information systems (IS) security in a social organizational context. A number of major studies recently conducted in Europe, among these being the Andersen 2001 survey, the Ernst and Young 2001 survey, and the DTI study 2002, indicate a general upward trend in the number of security incidents in organizations. These studies further suggest, that organizations expressed less confidence about future security issues, noting that security incidents are increasing both in terms of number and complexity. In this research information systems security is viewed as the minimization of risks arising from unauthorised access to and possession of information (Dhillon, 1995). In the context of information systems, the asset under consideration is data and the main IS security foundations are the integrity, confidentiality and authenticity of such data (Forcht and Wex, 1996).

Over the years, a number of security approaches have been developed that help in managing IS security and in limiting the chances of an IS security breach. The majority of these approaches entail checklists, risk analysis, and evaluation methods. Although the value of these approaches to security management is evident, Hirschheim et al., (1995), Backhouse and Dhillon (1996), James (1996) and Siponen (2001) among others, suggest that these approaches focus on narrow-technically oriented solutions and they ignore the social aspects of risks and the informal structure of organizations.

In a similar vein, as the annual total of security-related incidents is on the increase, current means for managing information systems security have been unable to fulfil their promise. The application of various security risk management approaches seems inadequate in managing and controlling efficiently security risks and overall, the performance of an IS manager and group in managing risks efficiently, remains limited.

Following these trends, this research adopts a social organizational approach to information systems security and makes the consideration that although IS managers and groups may have a variety of security risk management methods, tools and techniques available, differences and/or weaknesses of the cultural context within which they work, do not allow them to make an efficient use of methods, tools and techniques, in the context of risk management activities. Hence, this research is based on the rationale that security risks may arise due to a failure to obtain some or all of the goals that are relevant to the management of the integrity, confidentiality, and authenticity of data through an organization's information systems. To this end, this paper intents to study the concept of goal setting in the context of information systems security management by exploring and discussing the role of strong cultures in the process of setting security goals. In the following sections, the research methodology is being discussed and the concepts of goal setting and strong culture are introduced. Then, the paper presents the empirical research findings and ends with some conclusions.

2."RESEARCH METHODOLOGY"

The objectives of this paper were to investigate:

- If IS managers and groups set, in particular, security goals in relation to the integrity, confidentiality and authenticity of data through the organizations' information systems
- What are the procedures based on which IS managers and groups set security goals in the context of information systems security management
- The role of a strong culture and its possible effect on the level of security goal setting
- The determinants of a strong culture

The ontology of this research with regards to security is that, security should not be treated as something tangible and concrete but also as a social, organizational issue.

To this end, a qualitative research approach having philosophical foundations, mainly in interpretivism, was deemed more appropriate for this research. Miles and Huberman (1994) describe qualitative research as simply, research based upon words, rather than numbers. A more generalised, but appropriate definition is: "Qualitative research is multimethod in focus, involving an interpretive, naturalistic approach to its subject matter" (Denzin and Lincoln, 1998). This definition implies that qualitative researchers study things in their natural environment and understand events in terms of the meaning people assign to them and this is the strategy applied to this investigation. The term 'interpretivism' is defined as "Studies that assume that people create and associate their own subjective and intersubjective meanings (inductive process) as they interact (processual) with the world around them (contextual) (Orlikowski and Baroudi, 1991).

Interpretivism was particularly useful when the results were being obtained. The respondents were providing their views from their interactions with the rest of the group in which goal setting was in process. For instance, when the respondents were asked questions regarding goals, it was difficult for them to provide a response without having been involved with the rest of the group.

The next issue under consideration was the research method to be used. Having considered the possible benefits of each available method e.g. action research, case studies, field studies, application descriptions, it was decided that the advantages offered by case studies were deemed more appropriate to this research. Cavaye (1996) and Yin (1994) cite a benefit of a case study as 'an investigation of a phenomenon within its real life context'.

However, the question was whether to employ single case studies or multiple case studies. Theorists support the view that a single case study should be employed, particularly when exploring a previously unresearched subject (Yin, 1994) or for theory testing by confirming or refuting theory (Markus, 1989). When a single case study is used, a phenomenon is investigated in depth, and a rich description and understanding are acquired (Walsham, 1995).

Conversely, multiple case studies enable the researcher to relate differences in context to constants in process and outcome (Cavaye, 1996). According to Miles and Huberman (1994) multiple case studies can enhance generalisability, deeper understanding and explanation. Herriot and Firestone (1983) point out that the evidence from multiple case studies is often considered more convincing, with the overall study being considered more robust. This research further asserts that although studying multiple cases may not provide the same rich descriptions as do studies of single cases, multiple cases enable the analysis of data across cases.

To this end, a case study approach has been followed within the IT departments of three financial institutions in Greece due to the investigator's availability of access. The institutions ranged from small (Alpha-Bank)[1] to medium (Delta-Bank) to large (Omega-Bank) financial institutions respectively, based on their financial assets. The reason for choosing these organizations according to their assets was to investigate the interrelationship and effect of different socio-organizational perspectives to different IT group structures. For example, the IT department of Alpha-Bank consisted of approximately 40 employees, while in Delta-Bank 150 employees, and in Omega-Bank 410 employees, respectively.

However, another issue to be resolved with the research approach used here concerns data collection. The design of this research employed multiple data collection methods as it is important in case research studies (Benbasat et al., 1987). In all cases data was collected through a variety of methods including interviews, archival records, documents, and observation and visits to the banks lasted for approximately three months. The total number of interviews within the three case studies, numbered to fifteen. The interviewees ranged from IT managers, deputy managers, auditors, and general IT staff. The interviews were face-to-face and when necessary telephone interviews followed up to confirm something about the data that was unclear.

Further, the use of multiple data collection methods makes triangulation possible and this provides stronger substantiation of theory (Eisenhardt, 1989). Triangulation is not

[1] The Three Case Studies in this article are described as Alpha-Bank, Delta-Bank, and Omega-Bank respectively, for confidentiality reasons

a tool or strategy, but rather an alternative to validation (Denzin, 1989; Flick, 1992). Thus, any finding or conclusion made from the cases is likely to be more convincing and accurate if it is based on several different sources of information (Yin, 1994). Five types of triangulation have been identified in the literature (Janesick, 2000): Data, Investigator, Theory, Methodological triangulation and Interdisciplinary. The present research used data triangulation, theory, methodological, and interdisciplinary.

Having discussed the research approach, the paper next will introduce the concepts of goal setting, and strong culture in order to provide a deeper understanding of the issues under concern.

3.”THE CONCEPT OF GOAL SETTING”

The theory of goal setting falls within the broad domain of cognitive psychology and its literature is extensive. The theory, as the name implies, is based on the concept of goals and is an essential element of social learning theory (Bandura, 1997), which has become increasingly influential through time (Mitchell et al., 2000). Goals, however, can be viewed as internal psychological representations of desired states, which can be defined as outcomes, events, or processes (Mitchell et al., 2000). A goal encompasses terms such as intention, aim, task, deadline, purpose and objective. It is part of the human condition, in the sense that almost all human activities are consciously or unconsciously directed by goals.

The importance of goals with respect to work behaviour is well documented by two main propositions, these are:

1. Increases in the difficulty of assigned goals (given goal acceptance) lead to increases in performance
2. Specific, difficult assigned goals result into higher performance than instructions of ‘do your best’ or no assigned goals.

In the first proposition, research shows that when individuals accept an assigned difficulty goal, task performance tends to increase. In particular, 90 percent of the

studies support this proposition with an effect size on performance being approximately 10-15 percent increase as a result of goal level (Locke and Latham, 1990). Likewise, in the second proposition research shows that when individuals are given goal specificity, task performance tends also to increase. Based on the same research findings, Locke and Latham (1990) report that 90 percent of those studies support the second proposition with an effect size on performance being approximately 8-16 percent increase as a result of goal specificity. In addition, Rodgers and Hunter (1991, 1994) using MBO programs and Pritchard (1995) with his PROMES system, confirm that specific goals have a positive impact on performance.

Although, the results of the above two propositions have been at an individual level, Locke and Latham (1990) based on a review of 41 independent studies on group level found that over 90 percent of those studies support these two main propositions. Similarly, O' Leary-Kelly et al., (1994) found strong effects of assigned groups goals on group performance and Crown and Rosse (1995) reported that when individual and group goals were congruent, group members were committed to increasing group performance. Shalley and Johnson (1996) found that when individual and group goals were incongruent, individuals gave priority to a specific goal over a more ambiguous goal. Weingart (1992) also asserted that goal difficulty and task component complexity influence group performance by affecting the group members' effort as well as the amount, quality and timing of their planning.

Some recent research results, however, show that the relationship between goal level-performance may not necessarily hold at a macro (group) level. For instance, Finnegan (1999) found that group goal commitment was not related to group performance, Seijts and Latham (2000) found different impacts of goal setting on performance based on group size, while Wegge (2000) found moderating effects from participation in goal setting, group cohesion and group conflict. The majority of the results, however, show that the two propositions hold for both individual and group levels in laboratory and field studies as well as in different types of tasks.

Following these trends, this paper takes a macro-goal level point of view and supports that an efficient goal setting process at a group level will improve the process of

information systems security management. Consequently, the main research question becomes:

- Do organizations set goals relevant to the management of the integrity, confidentiality and authenticity of data through an organization's information systems?

4."THE CONCEPT OF STRONG CULTURES"

Although relatively new as a concept in organizational behaviour, organizational culture is widely referenced in academic literature, and business journals, and has attracted the attention of researchers in recent years. A reason for such interest may be the belief that organizational cultures provide a sense of control, in terms of unifying the way employees process information and behave within the organization, which increases the predictability of organizational behaviour (Trice and Beyer, 1993).

However, most of the literature on organizational culture focuses on the hypothesis that strong cultures enhance organization performance (Deal and Kennedy, 1982; Burt et al., 1994). A strong culture is defined as "a system of shared values (which define what is important) and norms that define appropriate attitudes and behaviours for organizational members" [O' Reilly and Chatman, 1996, p.160] and this is the definition of culture strength applied in this research. This hypothesis, however, is based on the belief that organizations benefit from having highly motivated employees dedicated to common goals (Deal and Kennedy, 1982). It is also believed that having widely shared and strongly held norms and values lead to performance benefits such as: enhanced co-ordination and control within the organization, increased employee effort, and improved goal alignment between the organization and its employees (Sorensen, 2002). Thus, a culture can be considered strong if those norms and values are widely shared and strongly held throughout the organization (Kotter and Heskett, 1992; O' Reilly and Chatman, 1996).

Moreover, it is believed that strong cultures benefit organizations by allowing social control, which may provide an agreement on certain behaviours within the

organization; that means, any possible “breaches” of behavioural norms may be identified and corrected immediately (Krimsky and Plough, 1988). Similarly, in strong cultures employees are motivated to perform in high standards, as they feel free to participate in the organization’s activities (O’ Reilly and Chatman, 1996). In addition, strong cultures provide clarity of goal achievement as well as better co-ordination and control of activities, which in turn, provide a certain course of action by employees on the organizations’ business strategies (Cremer, 1993).

Although the assumptions of the effects of strong cultures have been considered in terms of the content of organizational values and norms (Sorensen, 2000), recent evidence shows also positive evidence of culture strength in terms of the degree of agreement and commitment to organizational values and norms (Kotter and Heskett, 1992). For example, Denison (1990) suggested that organizational effectiveness is increased as a result of agreement enclosing organizational values, using both qualitative and quantitative data. Burt et al., (1994), using Kotter and Heskett’s data, investigated the effect of culture strength on market context and came to the conclusion that the benefit of strong cultures was increased in highly competitive markets.

However, strong cultures may not always provide benefits for organizations and this might be the case in organizational learning, whereas some theorists believe organizational cultures conceptualize on (Weick, 1985; Schein, 1992). As an example, organizations with strong cultures may not recognize the need for change because such organizations are too focused in understanding the world and thus may be unable to observe changes in environmental conditions. Conversely, March (1991) suggests that organizations with cultural weaknesses and willingness to learn from their members (cultural exploitation) are better able to understand and cope with any changes in environmental conditions. Similarly, even if organizations with strong cultures are willing to respond to any changes in environmental conditions, the transfer of knowledge and fresh ideas becomes in a rather sluggish way (Tushman and O’ Reilly, 1997).

Given all these characteristics of strong cultures this research supports that a strong culture plays a significant role on the level of security goal setting. To this end, this research supports the rationale that a strong culture at a group level:

3. plays a significant role at the level of goal setting in the context of security risk management

5.”EMPIRICAL FINDINGS”

Goal Setting

It was imperative for this research that any organization used for the research should have followed goal setting procedures and particularly the organizations’ IS/IT group departments. Before the interviews commence the contacted organizations replied positively that goal setting was a consistent part of their overall business strategy. In fact, goal setting was a very important issue and it was seen as an integral part of the overall risk management process. All the interviewees within Delta and Omega-Bank argued that goals are being set on a regular basis within each banking unit respectively, and that goals represent the identity of the banks’ business activities plan. The goals within both organizations, like in the case of Alpha-Bank, are always business oriented and within the technology units the main goals are cost reduction, automation of processes, systems efficiency, and security. Likewise, goals within all of the three organizations, come in the form of projects which either originate from the top-management to the different banking units or from those units to the top-management, in the form of project proposals. The goal setting activities within the three organizations are shown in Figures 1,2, and 3 respectively. However, it is not in the scope of this article to describe in detail each step of the goal setting phases within the organizations but rather to give an overall view of how the selected organizations set security goals.

In saying so, the IT group within Delta-Bank distinguishes the monitoring phase into an independent phase instead of being part of the execution phase, like in the cases of Alpha- and Omega-Banks. Similarly, the first four steps at the goal initiation phase

within the organizations were identical although the IT group at Omega-Bank considers the level of security applications in internet banking and alternative networks as separate levels of security goal activities. The interviewees within Omega-Bank argued that the additional taxonomy of security levels gives a more clear insight into the different aspects of security

1st Phase: Goal Setting Initiation Phase
Step 1: Selection of members for the project group
Step 2: Explanation of the method to the members of the group and planning of the goal setting security risk activities
Step 3: Physical security goals (external)
Step 4: Systems security goals (internal)
2nd Phase: Goal Execution Phase
Step 1: Risk identification goals
Step 2: Selection of identified risks
Step 3: Final risk identification and further goal setting via a joint security project group meeting
Step 4: Control of goal setting activities
Step 5: Risk monitoring
3rd Phase: Evaluation Phase
Last step: Evaluation of security risk goal setting activities and compiling a report

Figure 1 The Goal Setting Process in Alpha-Bank

1st Phase: Goal Setting Initiation Phase
Step 1: Selection of members for the project group
Step 2: Explanation of the method to the members of the group and planning of the goal setting security risk activities
Step 3: Physical security goals (external)
Step 4: Systems security goals (internal)
2nd Phase: Goal Execution Phase
Step 1: Risk identification activities
Step 2: Risk estimation
Step 3: Final selection of security risks via a joint project group meeting
3rd Phase: Evaluation Phase
Last step: Evaluation of security risks and goal setting activities planned
4th Phase: Monitoring Phase
Last step: Monitoring of the risks selected

Figure 2 The Goal Setting Process in Delta-Bank

1st Phase: Goal Setting Initiation Phase
Step 1: Selection of members for the project group
Step 2: Explanation of the method to the members of the group and planning of the goal setting security risk activities
Step 3: Physical security goals
Step 4: Security of internal systems
Step 5: Security applications in relation to internet banking
Step 6: Alternative networks
2nd Phase: Goal Execution Phase
Step 1: Risk identification goals
Step 2: Selection of identified risks
Step 3: Final risk identification and further goal setting via a joint security project group meeting
Step 4: Risk monitoring
3rd Phase: Evaluation Phase
Step 1: Evaluation of goal security risk related activities
Step 2: Providing an evaluation report
Step 3: Security policies and procedures

Figure 3 The Goal Setting Process in Omega-Bank

At the goal execution phase all of the organizations exhibited similar patterns although at Delta-Bank the risk monitoring stage was assumed as an independent final phase from that of execution. Alpha-Bank, had also an additional step of controlling the goal activities planned, while Delta-Bank and Omega-Bank did not. At Alpha-Bank though this stage is considered as reactive since the IT group seeks feedback to ensure that the security goal setting plan until that stage, will actually accomplish its objectives. From the interviews, Delta- and Omega-Bank considered that such feedback is achieved at the evaluation phase while at Alpha-Bank the IT group members argued that although feedback is achieved at the evaluation phase, some of the goal activities planned may be 'jeopardised' before that phase. Thus, the control of goal setting activities planned is a 'premature' stage, which provides though more valuable information at the time needed.

The evaluation phase was also a significant stage of the overall goal setting process in the context of security risk management within all of the three IT groups. In the case of Omega-Bank, the IT group considered an additional activities step, that of security policies and procedures, based on which the IT group investigates whether there is a need to change any particular aspect. The difference in the case of Omega-Bank, as compared to the case of Alpha-Bank and Delta-Bank, is that the IT group makes a more frequent evaluation of the security policies and procedures after the implementation of security projects.

However goal setting within all of the three case studies was a significant and consistent part of the overall organizations' business activities plan and development. The procedures according to which the IT groups within the three organizations respectively set goals, in the context of security risk management, exhibit similar patterns although with a few minor differences in the implementation process, in terms of stage prioritisation.

The Role and Effect of a Strong Culture in Goal Setting

The culture within Alpha-Bank was believed to be a reason of having an efficient goal setting process. In particular, the majority of the interviewees agreed that the cohesive strong group culture within the IT department plays a significant role at the level of security goal setting. Given the meaning and definition of strong culture to the interviewees, it was stated that in strong cultures goal alignment is easy to achieve, which confirms the results originally found by Sorensen (2002), whereas goal alignment has an ultimate effect on the manner by which security goals are set.

Moreover, in the Alpha- IT group the members were motivated to perform in high standards as they felt free participate in the group's overall security risk activities. The strong culture of Alpha-Bank provided an efficient co-ordination and co-operation of group activities among IT members, which ultimately provided clarity in goal achievement (Cremer, 1993). The IT manager in particular expressed: *"When the culture within the organization is strong, the employees seem to accept the co-ordination of activities more efficiently, and consequently there is clarity in what*

we're trying overall to achieve. Certainly there are benefits of having a strong cohesive culture and I believe these benefits are reflected in project management".

Further, the majority of the interviewees within Alpha-Bank argued that in a strong culture the employees know a certain course of action, which ultimately has an impact on how the goals are set. Evidence shows that the strong culture of Alpha-Bank was a motivation for IT members to dedicate their efforts to common group goals (Deal and Kennedy, 1982; Kotter and Heskett, 1992).

Likewise, in the context of the effect of a strong culture to goal setting the majority of the interviewees within Delta-Bank argued that culture has an effect on the level of goal setting. Having an IT program consistent with the bank's overall activities was very important on the goal execution level and it was stated that a strong culture improves goal alignment between the employees and among different banking units. However, due to the structure size of Delta-Bank a number of stakeholders with different political agendas influenced the IT group activities. Considering that the stakeholders are part of the organization's culture, their different interests had an effect on the way the IT group co-ordinated and controlled its activities, quite often in the context of security issues.

In the case of Omega-Bank, the interview respondents said that the hierarchical system within the bank did not allow enough room for innovations, individual initiative, and freedom of individual intellect, which ultimately had an effect on the contribution of employees in goal setting. In addition, the non-participation of some IT employees in security goal setting was believed to affect the level of goal setting since the co-ordination and control of the IT group's activities could otherwise be improved. As one IT member said: "*goal setting is a group effort rather than a process run by a specific number of employees"*.

However, from the interviews within both Delta- and Omega-Bank, it was found that culture had a relatively weak effect on the overall goal setting activities, because the organizations, and particularly the IT groups, co-ordinate their activities based on manuals and procedures which provide the necessary control over the groups' activities.

The perception of risks with regard to security was characterised as ‘positive’ within the Delta- and Omega-Bank IT groups mainly due to educational and training courses the IT members had to attend. When the interviewees were being asked questions in the context of information systems security, they exhibited full knowledge and awareness of the issue under concern and they mentioned that having equally shared information on security issues has a positive effect on the level of goal setting. The ‘positive’ perception of security risks within all of the organizations was reflected on the overall success in information systems security projects. That was particularly the case in Alpha-Bank whereas the strongly held and widely shared norms, values and beliefs, had a positive outcome on the process of goal setting.

However, evidence from the cases of Delta- and Omega-Bank shows that the phenomenon of culture had also an effect on the communication of security risks between different banking units. For instance, some of the interviewees in Delta-Bank argued that the communication of risks was always efficient due to different political agendas and competition between different units for project funding. To this end, the effect of culture to communication had an ultimate effect on goal setting since the activities defined in the context of security risk management had to be co-ordinated with the overall organization’s activities, particularly when conflicts arise.

Nevertheless, the scope of this research was also to identify the determinants of strong culture as it will shed some light both to academics and practitioners into how to an organization’s culture strength can be improved. To this end, the research proceeded to the identification of the determinants of strong culture within the three organizations. The findings are based on the interviewees’ work related experience, social relationships between people within the IT groups, knowledge and personal value attributes.

The most important determinant mentioned from the majority of the interviewees within the three organizations was education and training seminars. It was argued that people with educational background understand better the responsibilities they are assigned within the group and thus, the co-ordination and control of group activities is likely to become more efficient. Educated employees on issues under group concern

are likely to co-operate with other members of the groups more efficiently and use their knowledge to participate in decision making as well as to transfer efficiently that knowledge to other group members.

Likewise, training seminars on issues of security was also an important factor in co-ordinating efficiently group activities, providing goal alignment within the group, which ultimately has an effect on culture strength. Participation in group activities was also another important determinant in strong culture since in strong cultures employees feel free to participate in group activities (O' Reilly and Chatman, 1996). That is, allowing the members of a group to participate in group activities, makes them feel important to the group and their efforts are increased.

Clarity on goal achievement was also found to affect culture strength. In particular, evidence shows that the IT manager and/or project leader is key aspect in providing clarity of goals to be achieved by the group. Clarity of goal achievement provides better co-ordination and control of group activities since the employees face less uncertainty about the proper course of action when faced with difficulties (Cremer, 1993).

Mergers, is also an important determinant of strong cultures. A merger may have negative consequences especially for the smaller organization whose identity may be absorbed by the larger organization. Finally, competitive/political rivalry between different banking units within an organization has an effect on a group's culture since the interests of a particular group may outweigh over the interests of another. These determinants are also included in Table 1 below.

Determinants of Strong Cultures
▪ Education/training seminars ▪ Group participation in group activities/decision making ▪ Clarity in goal achievement ▪ Competitive/political rivalry ▪ Mergers

Table 1 The Determinants of Strong Cultures

6."CONCLUSIONS"

The research described in this paper was concerned with information system security from a social organizational point of view. The research was based on the rationale that security risks may arise due to a failure to obtain some or all of the goals that are relevant to the integrity, confidentiality and authenticity of data through an organization's information systems. To this end, the main research question was if IS managers and groups follow goal setting procedures in the context of security risk management activities and what is the role of culture strength on the level of goal setting.

The cases of Delta- and Omega-Bank exhibited slightly different patterns of social organizational behaviour although the process of goal setting in the context of risk management was based on the same criteria among the three case studies. The research findings from the case of Alpha-Bank show that culture strength plays an important role on the level of security goal setting. The actual reason is that the small structure size of the organization exhibited patterns of a 'family-oriented' business environment whereas the values and beliefs were widely shared and strongly held among the members of the organization. In effect, the strong culture within Alpha-Bank allowed clarity in goal achievement, efficient co-ordination and control of group activities, goal alignment, and a certain course of action by organization employees.

However, the effect and role of culture strength were less important to large-structure organizations such as Delta-Bank and Omega-Banks since the values and beliefs of these organizations are based on professional criteria. In saying so, people within Delta- and Omega-Banks valued most professionalism between third parties and groups, and that policies and procedures should run the bank not necessarily individual initiative. In effect, non-participation of IT members to security group activities influenced the process of goal setting within the IT groups, the communication of security risk messages was quite often inefficient between

individuals and different banking units, whereas different political agendas had also an effect on the level of security goal setting.

However, the majority of the interviewees argued that the process of goal setting with regards to security management could become even more efficient if the organizational values and beliefs were even more strongly held and widely shared among individuals and different groups.

In other words, the process of goal setting in the context of information systems security management could become even more efficient if the issue of culture is considered and determined more carefully than just acknowledging its value. To this end, failure to recognize and improve social organizational values such as culture strength may lead to an inefficient process of goal setting, whereas security risks in relation to the integrity, confidentiality, and authenticity of data through an organization's information systems, may arise.

Ultimately, this paper has made an important contribution to interpretive research by exploring and making practical recommendations for the process of goal setting within an interpretive research methodology. In particular, this investigation concludes that a social organizational approach is not independent of epistemological assumptions. In the opposite, this investigation has reinforced the argument that culture and goal setting are interrelated and that these aspects may have an effect in the context of information systems security management. In this respect, the research has contributed to a more holistic consideration of social organizational issues of information systems security as it allowed to break away from the narrow-technically oriented solutions of most IS security approaches to a variety of social, organizational issues that are of concern to researchers and practitioners alike.

7.”REFERENCES”

Andersen, K.V. (1998) EDI and Data Networking in the Public Sector: Governmental Action, Diffusion, and Impacts, Kluwer Academic Publishers, Boston.

Backhouse, J. and Dhillon, G. (1996) Structures of Responsibility and Security of Information Systems, *European Journal of Information Systems*, **5**(1), pp.2-9.

Bandura, A. (1997) *Self-efficacy: The Exercise of Control*, New York, W.H. Freeman Publishing.

Benbasat, I., Goldstein, D.K., and Mead, M. (1987) The Case Research Strategy in Studies of Information Systems, *MIS Quarterly*, **11**(3), pp. 369-386.

Burt, R.S., Gabbay, S.M., Holt, G., Moran, P. (1994) Contingent Organization as a Network Theory: The Culture-Performance Contingency Function, *Acta Sociologica*, **37**(4), pp. 345-370.

Cavaye, A.L. (1996) Case Study Research: A Multi-Faceted Research Approach for IS, *Information Systems Journal*, **6**(3), pp.227-242.

Cremer, J. (1993) Corporate Culture and Shared Knowledge, *Industrial and Corporate Change*, **2**(3), pp. 351-386.

Crown, D.F. and Rosse, J.G. (1995) Yours, Mine and Ours: Facilitating Group Productivity Through the Integration of Individual and Group Goals, Organizational Behaviour and Human Decision Processes, **6**(4), pp. 138-150.

Deal, T.E. and Kennedy, A.A. (1982) *Corporate Cultures*, Reading, MA: Addison-Wesley.

Denison, D.R. (1990) *Corporate Culture and Organizational Effectiveness*, New York, Wiley.

Denzin, N.K. (1989) *The Research Act*, Third Edition, Prentice-Hall, Eaglewood Cliffs, New Jersey, USA.

Denzin, N. and Lincoln, Y. (1998) Major Paradigms and Perspectives, In*: Strategies of Qualitative Inquiry*, N.Y.K. Denzin and Y.S. Lincoln, (eds.) Sage Publication, Thousand Oaks.

Dhillon, G. (1995) *Interpreting the Managing of Information Systems Security*. Unpublished PhD Thesis, London School of Economics and Political Science, University of London.

D.T.I. (2002) Information Security Breaches Survey 2002, *Technical Report*,

Department of Trade and Industry, London, April.

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

Ernst and Young (2001) *Information Security Survey*, Ernst and Young, London.

Flick, U. (1992) Triangulation Revisited: Strategy of Validation or Alternative? *Journal for the Theory of Social Behaviour*, 22, pp. 175-198.

Forcht, K. and Wex, R. (1996) Doing Business on the Internet: Marketing and Security Aspects, *Information Management and Computer Security*, **4**(4), pp.3-9.

Herriot, R. E., and Firestone, W. A. (1983). Multisite Qualitative Policy Research: Optimizing Description and Generalizability, *Educational Researcher*, **12**(3), pp. 14-19.

Hirschheim, R., Klein, H.K. and Lyytinen, K. (1995) *Information Systems Development and Data Modelling: Conceptual and Philosophical Foundations*, Cambridge University Press, UK.

James, H. (1996) Managing Information Systems Security: A Soft Approach, *Proceedings of the Information Systems Conference in New Zealand*, Editor: Phillip Sallis, October 30-31, Palmerston North, New Zealand.

Janesick, V. (2000) The Choreography of Qualitative Research Design. In: Denzin, N.K. and Lincoln, Y.S. (eds.) Handbook of Qualitative Research. Thousand Oaks, CA: Sage.

Kotter, J.R. and Heskett, J.L. (1992) *Corporate Culture and Performance*, New York: Free Press

Krimsky, S. and Plough, A. (1988*) Environmental Hazards: Communicating Risks as a Social Process*, Dover, MA: Auburn House Publishing.

Locke, E.A. and Latham, G.P. (1990) *A Theory of Goal Setting and Task Performance*, Englewood Cliffs, NJ: Prentice-Hall.

March, J.G. (1991) Exploration and Exploitation in Organizational Learning, *Organization Science*, **2**(1), pp. 71-87.

Markus, M.L. (1989) Case Selection in a Disconfirmatory Case Study, In: *The Information Systems Research Challenge*, Harvard Business School Research Colloquium, Boston: Harvard Business School, pp. 20- 26.

Miles, M.B. and Huberman, A.M. (1994) *Qualitative Data Analysis: An Expanded Sourcebook*, Sage publications, Newbury Park, CA.

Mitchell, T.R., Kenneth, R.T. and George-Falvy, J. (2000) Goal Setting: Theory and Practice, In: *Industrial and Organizational Psychology: linking theory with*

practice, Editors: C.L. Cooper and E.A. Locke, Blackwell Publishers Ltd, First Published 2000.

Orlikowski, W. and Baroudi, J.J. (1991) Studying Information Technology in Organizations: Research Approaches and Assumptions, *Information Systems Research*, **2**(1), pp.1-28.

O' Leary-Kelly, A.M., Martocchio, J.J., and Frink, D.D. (1994) A Review of the Influence of Group Goals on Group Performance, *Academy of Management Journal*, **3**(7), pp. 1285-1301.

O' Reilly, C.A. and Chatman, J.A. (1996) Culture as a Social Control: Corporations, Culture and Commitment, In: *Research in Organizational Behaviour*, B.M. Staw and L.L. Cummings (eds.), **18**, pp. 157-200, Geenwich, CT: JAI Press.

Pritchard, R.D. (1995) *Productivity measurement and improvement: Organizational case studies*, New York: Praeger.

Rodgers, R. and Hunter, J.E. (1991) Impact on Management by Objectives on Organizational Productivity (monograph), *Journal of Applied Psychology*, **76**(2), pp.322-336.

Rodgers, R. and Hunter, J.E. (1994) The Discard of Study Evidence by Literature Reviewers, *Journal of Applied Behavioural Science*, **30**, pp. 329-345.

Schein, E.H. (1992) *Organizational Culture and Leadership*, 2nd Edition, San Francisco: Jossey-Bass.

Seijts, G.H. and Latham, G.P. (2000) The Construct of Goal Commitment: Measurement and Relationships with Task Performance, In: *Problems and Solutions in Human Assessment: Honoring Douglas N. Jackson at seventy*, R. Goffin and E. Helmes (eds.), (pp. 315-332), Dordrecht, The Netherlands: Kluwer Academic Publishers.

Shalley, C.E., and Johnson, P.R. (1996) *The Dilemma of Dual Goals II: An Investigation of Resource Allocation Between Competing Goals*, Presented at the Society for Industrial and Organizational Psychology, San Diego Meetings.

Siponen, M.T. (2001) An Analysis of the Recent IS Security Development Approaches: Descriptive and Prescriptive Implications, In: *Information Security Management: Global Challenges in the New Millenium*, Dhillon, G. (eds.), Idea Group Publishing, Hershey.

Sorensen, J.B. (2002) The Strength of Corporate Culture and Reliability of Firm Performance, *Administrative Science Quarterly*, **47**(1), pp.70-96.

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

Tushman, M.L., and O' Reilly, C.A. III (1997) *Winning through Innovation*, Boston:

Harvard School Press.

Walsham, G. (1995) Interpretive Case Studies in IS Research: Nature and Method, *European Journal of Information Systems*, **4**(2), pp.74-81.

Wegge, J. (2000) Participation in Group Goal Setting: Some Novel Findings and a Comprehensive Model as a New Ending Ton at Old Story, *Applied Psychology: in International Review*, **49**(3), pp. 498-516.

Weick, K.E. (1985) The Significance of Corporate Culture. In: *Organizational Cultures*, P.J. Frost, L.F. Moore, M.R. Louis, C.C. Lundberg, and J. Martin (eds.), pp. 381-389, Beverly Hills, CA: Sage.

Weingart, L.R. (1992) Impact of Group Goals, Task Component Complexity, Effort and Planning on Group Performance, *Journal of Applied Psychology*, **77**(5), pp. 682-693.

Yin, R.K. (1994) *Case Study Research, Design and Methods*, Sage Publications, Newbury Park, CA.