Communications of the IIMA

Volume 4 | Issue 2 Article 5

2004

The Interrelationship and Effect of Trust and Strong Cultures in Setting information Systems Security Goals

Ioannis V. Koskosas
Brunel University

Jyoti Choudrie
Brunel University

Ray J. Paul
Brunel University

The Interrelationship and Effect of Trust and Strong Cultures in Setting Information Systems Security Goals

Ioannis V. Koskosas

Department of Information Systems and Computing, Brunel University, London, Uxbridge, UB8 3PH, UK Phone: +44 (1895) 274000,
Fax: +44 (1895) 251686, ioannis.koskosas@brunel.ac.uk

Jyoti Choudrie

Department of Information Systems and Computing, Brunel University, London, Uxbridge, UB8 3PH, UK Phone: +44 (1895) 274000,
Fax: +44 (1895) 251686, Jyoti.houdrie@brunel.ac.uk

Ray J. Paul

Department of Information Systems and Computing, Brunel University, London, Uxbridge, UB8 3PH, UK Phone: +44 (1895) 203 374,
Fax: +44 (1895) 251686, ray.paul@brunel.ac.uk

ABSTRACT

This paper investigates the interrelationship and effect of trust and culture on the level of goal setting within the context of information systems security. In doing so, it explores and discusses the concepts of trust and strong culture and seeks to demonstrate their importance in setting efficiently information systems security goals. The paper contributes to interpretive information systems research with the study of goal setting in a security management context and its grounding within an interpretive epistemology.

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 paper 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 are presented in Figure 1, below.

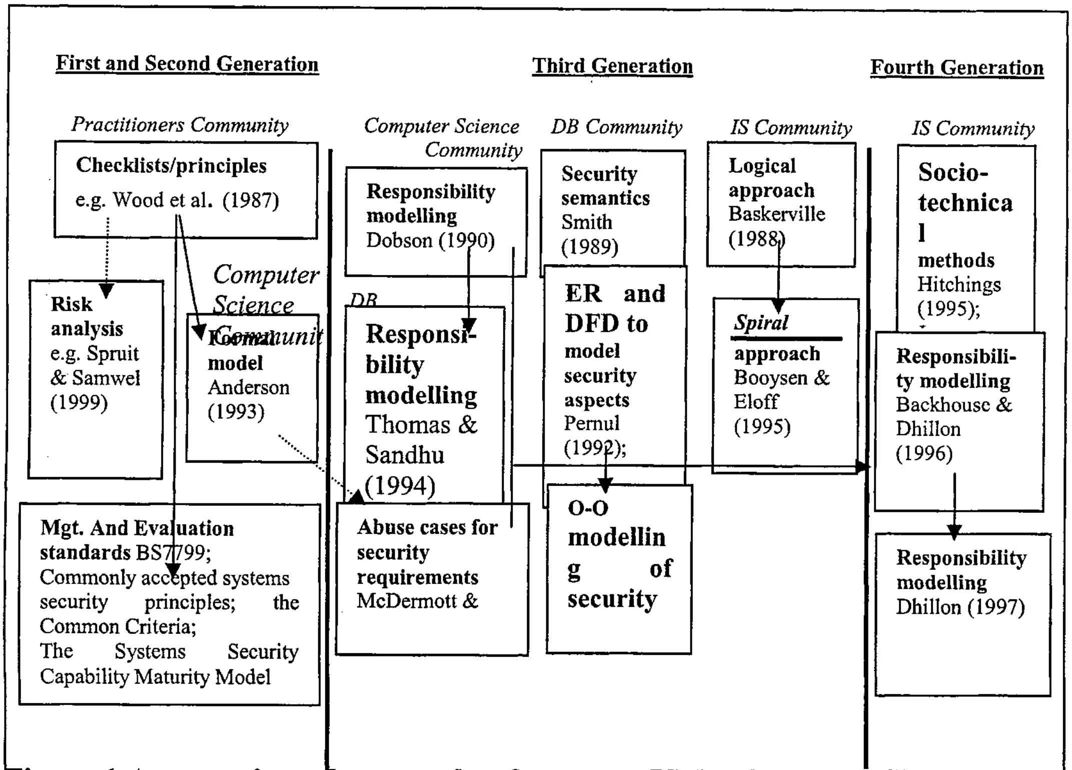

Figure 1 An overview of approaches for secure IS development (Siponen, 2001)

The thick separated lines represent the different generations originally presented by Baskerville (1988). The arrows show influences or inspirations while the broken arrows mean that the approach is influenced by the deficiencies of a certain approach. The tradition (*Computer Science, Data Modeling, Practitioners Community and IS Community*) from which the works sprung is described using italics. First and second generation methods aim at finding out what can be done and actually dominate the principles, checklists, and most standards for secure systems development. Third generation approaches include modelling and fourth generation emphasise socio-technical design. Siponen (2001) supports the view that there have been only a few isolated approaches to consider the socio-technical aspects of information systems security management. The majority of IS security methods entails checklists, risk analysis, and evaluation methods. Although these approaches help in managing security, 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 efficiently IS security risks and overall, the performance of an IS/IT manager and group in managing risks efficiently, remains limited.

Following these trends, this paper adopts a social organizational approach to information systems security and makes the consideration that although IS/IT managers and groups may have a variety of security risk management methods, tools, and techniques available, they may not make an efficient use of them in the context of risk management activities. Thus, this paper 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 availability of data through an organization's information systems. To this end, this paper intents to study the process of goal setting in the context of information systems security management by exploring and discussing the interrelationship and effect of trust and strong culture on the process. In the following sections, the research methodology is being discussed and the concepts of goal setting, trust and culture are introduced. Then, the paper presents the empirical research findings and ends with some conclusions.

RESEARCH METHODOLOGY

The objectives of this paper were to investigate:

- If IS/IT managers and groups set, in particular, security goals in relation to the integrity, confidentiality and availability of data in the context of information systems
- If there is an interrelationship between trust and culture on the level of goal setting
- If trust and culture have an effect on the level of security goal setting

In this investigation, a qualitative research approach having philosophical foundations, mainly in interpretivism, was deemed the most appropriate. 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 trust, it was difficult for them to provide a response without having been involved with the rest of the group. Similar situations arose in the instance of culture and goal setting.

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 investigation. 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).

In the opposite, 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 investigation 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)2 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 investigation 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

2 The Three Case Studies in this paper are described as Alpha-Bank, Delta-Bank, and Omega-Bank respectively, for confidentiality reasons

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 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, trust and culture in order to provide a deeper understanding of the issues under concern.

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:

- Increases in the difficulty of assigned goals (given goal acceptance) lead to increases in performance
- 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.

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 availability of data through an organization's information systems?

THE CONCEPT OF TRUST

Trust is a social phenomenon although with a multidisciplinary view. Thus, the issue of trust can be categorised based on how trust is viewed in different disciplines along different dimensions. Personality psychologists tend to view trust as an individual characteristic while social psychologists tend to view trust as the behavioural expectation of some parties involved in a transaction (Bhattacharya et al. 1998). Sociologists and economists tend to focus on how institutions are established and incentives are used to reduce uncertainty associated with transactions among relative parties (Bhattacharya et al., 1998).

Rousseau et al. (1998) argue that it is necessary to integrate the differing views of trust across disciplines and consider that trust may be a "meso" concept, which integrates both the individual and institutional level views of trust development. In this paper, the focus is on trust between the members of an IS/IT group is setting efficiently security goals relevant to the management of the integrity, confidentiality and availability of data through an organization's systems. The purpose at one level, is to integrate a particular viewpoint of trust with other social organizational concepts such as culture as this paper takes the standpoint that such "values" and their relationship with each other may have a significant role at the macro (group) goal setting level.

Trust, however, has different definitions according to the discipline in which it is used. Rousseau et al. (1998, p.395) based on a multiplex point of view suggest that trust is widely defined as: "*trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another*". Based on this definition, in this paper, trust is defined as confidence and positive expectations of one party within an IS/IT group that another party is willing to co-operate in setting goals efficiently with regards to security in the context of risk management.

The issue of trust has attracted particular attention through the years, due to the numerous benefits it offers to organizations (Kramer, 1999). Although, a significant amount of researchers have devoted attention to examining the potential benefits of trust, they have devoted less attention to examining the conditions under which trust provides these benefits (Dirks and Ferrin, 2001). Theorists of trust support the view that trust may work as an independent variable (cause), dependent variable (effect), or interaction variable (moderator) (Rousseau et al. 1998). For example, trust is used as a potential cause in choice scenarios framed around social dilemmas when economic outcomes are expected (Rousseau et al., 1998).

Further there are two fundamental perspectives that explain how the benefits of trust, emerge. The first perspective explains the effect of trust in a straightforward manner. That is, trust results in direct effects such as more positive attitudes, higher levels of cooperation, and higher levels of performance (Dirks and Ferrin, 2001). The second perspective explains the effects of trust in an indirect (moderate) manner. That is, trust provides the conditions under which certain outcomes such as cooperation, positive attitudes and perceptions and higher performance are likely to occur (Dirks and Ferrin, 2001). This paper supports the rationale that trust has a moderate effect and in so doing, trust:

1. Provides the conditions under which a strong group culture is likely to occur
2. Plays a significant role at the macro-goal level of security management.

THE CONCEPT OF CULTURE

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 paper. This hypothesis, however, is grounded 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. In the opposite, 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 paper, further, supports that a strong culture may also have an effect on the level of security goal setting. To this end, this paper supports the rationale that a strong culture at a group level:

3. Plays an important role at the macro-goal level of security management.

EMPIRICAL FINDINGS

Goal Setting

It was imperative for this investigation 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. Goal setting activities, in the context of security risk management, are distinguished into three main phases, as shown in Figure 1: the *goal setting initiation phase*, the *goal execution phase*, and the *evaluation phase*. 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 doing 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 interview respondents 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

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 interview replies, 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 INTERRELATIONSHIP OF TRUST AND CULTURE

In the case of Delta-Bank and Omega-Bank, trust was seen as an important issue in the relationship between employees although with a minor effect on their work behaviour. The issue of trust within the organizations and particularly within the IT groups was associated with delivery. That means the group members placed trust on each other in terms of their capability in successfully dealing with a problem. Based on the interviews evidence shows that trust within Delta-Bank and between different banking units was not equally shared mainly because the nature of business scope was different and therefore, the employees developed a certain level of trust only between people within their group.

Dirks and Ferrin (2001), argue that trust has significant effects on attitudes, perceptions and other cognitive constructs such as employees' satisfaction with decisions, supervisor, relationship and job. Likewise, in Omega-Bank there was a certain level of dissatisfaction between some of the IT employees towards the top-management because they did not participate in the process of goal setting with regard to security. Moreover, the different stakeholders' interests within the organization had negative consequences on the level of trust between the technology group and the different banking units as there was a belief that the greatest share of funds would be spend on technology projects. To this end, there were times upon which different banking units within the bank developed an intense competition between them in order to gain the greatest share of funds available for project spending. Dirks and Ferrin (2001) also confirm that under high levels of trust, individuals will be more likely to attend to co-operative motives, while under low levels of trust individuals will be more likely to attend to the competitive motives, which verifies the obtained results.

Conversely, evidence shows that trust within Alpha-Bank was an important issue and there was a widely held belief that the people can depend on each other and to the top-management for support in order to overcome any possible obstacle. All the IT interviewees within Alpha-Bank stated that top-management support plays a critical role in the establishment of trust within their group. Moreover, the majority of the IT members work together since the establishment of the bank and therefore, trust was based on a long-term relationship between bank employees. Likewise, the IT employees co-operated in a large number of projects that results into confidence among them which further makes them to believe they can depend on each other.

Similarly, the culture within Alpha-Bank was characterised as very strong and consistent with a set of values and beliefs and oriented towards the investment of human resources. In the case of Delta- and Omega-Banks, however, trust was believed to affect the organizations' culture due to the low salaries paid to the employees as compared to other financial institutions. Dirks and Ferrin (2001) argue that the extent to which individuals trust their manager, they are likely to devote their attention and effort, to role performance, norm conformance, and rule compliance because of their confidence that they will receive appropriate rewards. Although, that was indeed the case in Alpha-Bank, in Delta- and Omega-Bank as trust was seen in terms of professionalism, some of the IT employees were not satisfied with higher levels of the hierarchy, as they believed that they should have money rewards for excellence in performance. Instead, the low salaries paid to employees, as compared to other organizations, developed feelings of dissatisfaction with an effect, some highly IT skilful employees to leave the organization.

However, evidence from the three case studies shows that trust provides the conditions under which a strong culture occurs through *participation in group activities*, *positive attitudes*, *higher levels of co-operation* and *co-ordination of activities*, as well as *employees' satisfaction towards the top-management* that their efforts will be recognised. Trust though within the Delta- and Omega-Bank, was found to have a weak effect on culture because the organizations' large structure makes it difficult for the different banking units to become flexible while trust depends purely on professional criteria rather than willingness to co-operate. In these organizations the values and beliefs were less widely shared and less strongly shared among groups and individuals mainly because of different political agendas.

The Effect of Trust and Culture on Goal Setting

All the interview respondents within Delta-Bank, stated that trust has an ultimate effect on the level of goal setting to the degree that one party or group was capable of delivering. The difference in scope within different banking units had an effect on the IT groups' activities, as the business units did not always co-operate efficiently. In effect, some IT projects met difficulties at the project initiation phase, as the IT groups had to postpone decisions on security issues.

Likewise, the restriction imposed to some IT employees to participate in the process of goal setting with regard to security, developed a level of mistrust from these employees to the top-management, as they felt incapable of delivering. To this end, considering that trust in this paper has been defined as willingness to co-operate in order to produce efficient work outcomes, trust had an effect on the level of goal setting in the context of security since the non-participation of some IT employees to goal setting did not allow them to co-operate efficiently and even transfer their knowledge to other members within the group. However, the effect of trust on goal setting was weak because as the organizational members defined trust in terms of professionalism, the employees expected each other to deliver.

In the context of the effect of a strong culture to goal setting all the interviewees within Delta-Bank stated that culture had 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. As mentioned, 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, when the interview respondents has been asked on the effect of culture to goal setting, they replied 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 overall employees' contribution in decision making. 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*".

From the interviews, evidence also shows that the perception of risks with regard to security among the IT members of Omega-Bank, was based on certain, knowledgeable criteria due to the educational and training programs the employees had to attend. This was reflected in clarity of goal achievement and goal alignment between the members of the IT group, which was part of the organization's culture.

However, from the interviews within both Delta- and Omega-Bank, evidence shows that culture had a relatively weak effect on the overall goal activities planned, since the organizations and particularly the IT groups, co-ordinate their activities based on manuals and procedures which allow control over the groups' activities.

CONCLUSIONS

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 principles among the three case studies. The undertaking of the three empirical studies revealed that IS/IT managers and groups do set security goals with regard to the management of the integrity, confidentiality and availability of data through the organizations' information systems. In addition, research findings from the case of Alpha-Bank show that there is a strong interrelationship between trust and culture whereas, in turn, these aspects have an ultimate effect on the level of security goal setting. However, this interrelationship and effect is stronger in organizations with small structures because such organizations exhibit 'family-oriented' business patterns whereas the values and beliefs are strongly held and widely shared among the organizational members. Although, this interrelationship and effect apply to organizations with large structures, their impact is rather minimal because such organizations depend strictly on manuals and procedures, which focus on professional criteria rather than individual initiative and intellect.

Evidence also has shown that trust provides the conditions under which a strong group culture occurs through participation in group activities, positive attitudes across organizational members, higher levels of co-operation and co-ordination of activities, as well as employees' satisfaction to top-management that their efforts will be recognized. Likewise, the existence of different political agendas was found to have a greater impact to organizations with large structure as compared to small structure organizations. However, the conflict type identified within the three case studies was mainly due to differences in business scope between different banking units rather than due to inefficient knowledge on the subject matters. The case of Alpha-Bank, the small structure organization, has exhibited greater flexibility in decision making and consistency within the IT group activities as compared to the other cases with large structures.

A major conclusion with regard to security is that social and organizational perspectives such as trust and culture play an important role in the process of goal setting. To this end, failure to recognize and improve such social and organizational perspectives may lead to an inefficient process of goal setting, whereas security risks with regard to the management 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. Conversely, this investigation has reinforced the argument that trust and culture are interrelated and that these aspects may have different effect on security goal setting depending on the organization's structure. In this respect, the investigation makes an important contribution to social, organizational research in information systems security as well as to interpretive research.

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.

Baskerville, R. (1988) Designing Information Systems Security, John Wiley and Sons, New York, Information Systems Series.

Bhattacharya, R., Devinney, T., and Pillutla, M. (1998) A Formal Model of Trust Based on Outcomes, Academy of Management Review, **23**(3), pp. 459-472.

Burt, R.S., Gabbay, S.M., Holt, G., Moran, P. (1994) Contingent Organization as a 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.

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.

Dirks, K.T. and Ferrin, D.L. (2001) The Role of Trust in Organizational Settings, Organization Science, **12**(4), pp. 450-467.

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.

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

Kramer, R. (1999) Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions. Annual Review of Psychology, **50**(1), pp. 569-598

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.

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' 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.

Rousseau, D., Sitkin, S., Burt, R., Camerer, C. (1998) Not so Different All: A Cross-Discipline View of Trust, Academy of Management Review, **23**(3), pp. 393-405.

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.

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.

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