ISSN No. 0976-5697

Volume 2, No. 1, Jan-Feb 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A View in Internet Banking Through Organizational Culture

Ioannis V. Koskosas
Department of Informatics and Telecommunication Engineering
University of Western Macedonia,
Department of Business Administration
Technological Educational Institute of Western Macedonia
Agios Dimitrios Park, Kozani, 50100 Greece
ikoskosas@uowm.gr

Absract: The aim of this research is to investigate information systems security in the context of risk management. In doing so, it adopts a social and organizational approach by investigating the role and determinants of organizational culture in the process of security goal setting with regard to internet banking risks. The research seeks to demonstrate the important role of culture in the risk management context from a goal setting point of view through a case study approach within three financial institutions in Greece. The determinants of organizational culture are also explored and discussed as well as the different goal setting procedures within different information system groups. Ultimately, this research provides a discussion of an interpretive research approach with the study of culture and goal setting in the risk management context and its grounding within an interpretive epistemology.

Keywords: Culture, goal setting, security management, internet banking, interpretive epistemology

I. INTRODUCTION

The research described in this article is concerned with information systems security in the scope of internet banking. Banking is being a highly intensive activity that relies heavily on information technology (IT) to acquire process and deliver the information to all relevant users. To this end, IT provides a way for banks to differentiate their products and services delivered to their customers. Driven by the challenge to expand and capture a larger market share of the banking industry, some banks invest in bricks and mortar while others have considered a new approach to deliver their banking services via a new medium: the Internet.

While the internet provides opportunities for businesses to increase their customer base, reduce transactions costs, and sell their products globally, security implications impede the business Forcht and Wex (1996). As an example, a number of major studies recently conducted in Europe, among these being the Andersen 2006 survey, the Ernst and Young 2006 survey, and the DTI study 2006; 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

Although a number of significant, valuable approaches have been developed for the management of information systems security, they tend to offer narrow, technically oriented solutions and ignore the social aspects of risks and the informal structure of organizations (Backhouse and Dhillon, 1996; Straub and Welke, 1998; Siponen, 2000). 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).

Thus the main principle of this research is that even if information system managers and groups have available a variety of security risk management methods, tools and techniques, they may not make an efficient use of them in the process of risk management. In saying so, this research supports the view 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 availability of information through the internet banking channel.

To this end, this research adopts a social and organizational approach to investigate information systems security within the scope of internet banking by exploring and describing the role and determinants of organizational culture and goal setting procedures in risk management. In the following, the chosen research approach is being discussed as well as its appropriateness for the research objectives. Then, the issue of internet banking and the reasons for choosing such topic for investigation is being discussed and the theories of culture and goal setting are introduced. Ultimately, the research presents the empirical findings and concludes on the usefulness of an interpretive epistemology.

II. AN INTERPRETIVE RESEARCH APPROACH

At the level of macro goal setting, researchers' interest has been in strategic management and organizational theory whose focus is on the organization as a whole (Locke and Latham, 1990). Due to the difficulty of using controlled experimental designs, they have used correlational and observational methods and both quantitative and qualitative approaches have been employed.

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).

The objectives of this research were to investigate:

A. if IT managers and groups set, in particular, security goals in relation to the integrity, confidentiality and availability of information through the internet banking channel
B. the role and effect of organizational culture in the process of security goal setting
C. the determinants of culture in setting security goals efficiently

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 security goals, it was difficult for them to provide a response without having been involved in goal setting procedures.

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 (1984) 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, 1984) 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 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)[1] to medium (Delta-Bank) to large (Omega-Bank) financial institutions accordingly, based on their financial assets. The reason for choosing these organizations according to their assets was to investigate the role and effect of trust on different goal setting procedures within 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, 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 IT staff people. The interviews were face-to-face and when necessary telephone interviews followed up to confirm something about the data that was unclear. In most cases, the conversations were tape-recorded. Tape recordings were used as they offer benefits that are not available with such other forms as the note taking of data collection.

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 and Lincoln, 1998; 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, 1984). 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, as shown in Diagram 1. Having discussed the research approach, this investigation discusses the issue of internet banking and then introduces the theories of goal setting and culture.

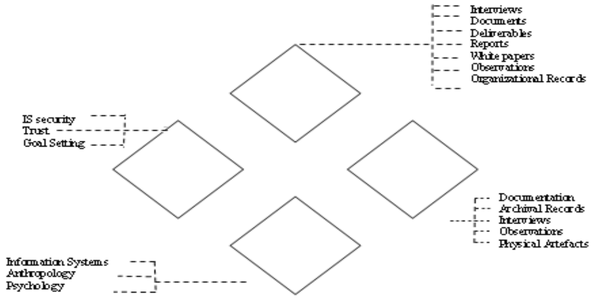


Diagram 1 Types of Triangulation Used in the Research

III. THE ISSUE OF INTERNET BANKING

The internet has rapidly gained popularity as a potential medium for electronic commerce (U.S. Department of Commerce, 1999). The reason of such popularity is the fact that individuals have the ability to communicate and exchange information with people all over the world (Gore, 1999). Firms have the potential to reach a large number of customers and fully automate their transactions in the values chain (Kosiur, 1997) while governments can provide more efficient services to citizens by automated procedures such as public procurement and local or national elections (Andersen, 1998). Today, the internet is believed to be on its way to become a full-fledged delivery and distribution channel while among the consumer-oriented applications riding at the forefront of this evolution are electronic financial products and services (Tan and Teo, 2000).

The emergence of internet banking has made banks re-think their IT strategies in order to remain competitive as internet banking services is believed to be crucial for the banks' long-term survival in the world of electronic commerce (Burnham, 1996). Today, customers demand new levels of convenience and flexibility (Lagoutte, 1996) on top of powerful and easy to use financial management tools, products and services, something that traditional retail banking could not offer (Krimsky and Plough, 1988). Thus, internet banking allows banks to provide these services by exploiting an extensive public network infrastructure (Ternullo, 1997).

The use of new distribution channels such as the internet, however, increases the importance of security in information systems as these systems become sensitive to the environment and may leave organizations more vulnerable to system attacks. Thus, the issue of security in the context of internet banking is an interesting candidate to investigate.

IV. THE THEORY 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:

A. Increases in the difficulty of assigned goals (given goal acceptance) lead to increases in performance
B. 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 difficult 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 though show that the relationship between goal level- performance may not necessarily hold at a macro (group) level. For instance, 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 though 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 investigation takes a macro-goal level point of view and supports that an efficient goal setting process, at group level, will improve the process of information systems risk management within the scope of internet banking security. Thus, the main research question becomes:

C. Do organizations set goals relevant to the management of the integrity, confidentiality and availability of information through the internet banking channel?

V. THE THEORY OF ORGANIZATIONAL 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 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 organizational cultures, this investigation further supports that a strong organizational culture may have an effect on the level of goal setting with regard to internet banking security. To this end, the investigation further supports that a strong culture at organizational level:

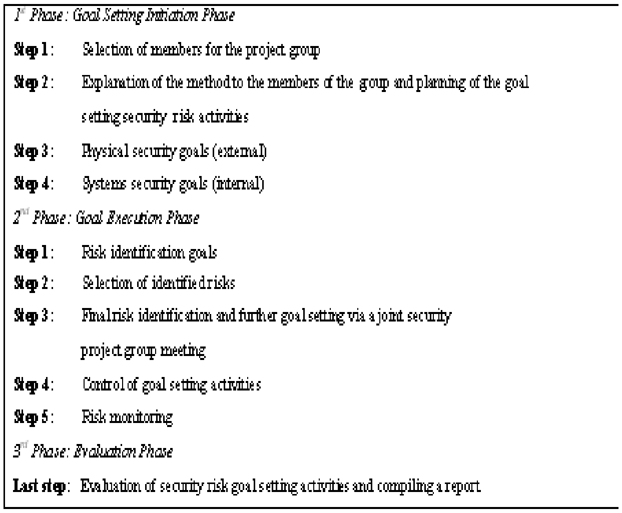
D. plays an important role and has an effect on the process of goal setting with regard to internet banking security goals

VI. RESEARCH FINDINGS

A. *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' IT groups. 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 stated 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 the three organizations, may 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 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 investigation 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. Goal Setting in the Context of Security Risk Management

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. In the context of internet banking security, all of the three case studies make use of a checklist which prioritises internet banking risks in terms of their likelihood ratio and possible impact. In doing so, the IT groups can take measures if necessary in order to maintain control of security related activities to internet banking.

Although, it was stated that the taxonomy of such risks and risk factors in internet banking change on a regular basis, the provision of such a checklist was not provided due to confidentiality reasons. However, in the case of Alpha-Bank, an example of such checklist was obtained for the purposes of this investigation. This checklist is included in Appendix 1, which consists of five main clusters of internet banking risk categories.

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, however, 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 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 set goals, in the context of risk management, exhibit similar patterns although with a few minor differences in the implementation process, in terms of stage prioritisation. In the context of internet banking security, all of the interview respondents within the organizations suggested that the use of the checklist proved to be beneficial as it provides clarity of the internet banking risks and of the security goal activities that have to be planned.

B. The Role and Effect of Organizational Culture on 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.

C. The Determinants of Organizational Culture

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.

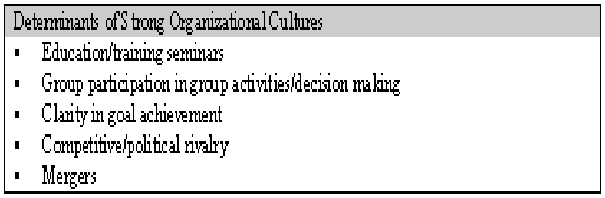
The most important determinant mentioned from the majority of the interviewees within the three organizations was education and training seminars. It was argued that people with educational background understand better the responsibilities they are assigned within the group and thus, the co-ordination 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.

Table 1 Determinants of Strong Organizational Cultures



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

VII. 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.

APPENDIX 1: Internet Banking Security Checklist (Alpa-Bank)

Cluster 1: Internet Banking Policy

[a] Internet banking risks and controls
[b] Transaction risks
[c] Control and security
Security controls
Network and data access controls
User authentication
Firewalls
Encryption
Transaction verification
Virus protection
[d] Monitoring
Security monitoring
Penetration testing
Intrusion detection
Performance monitoring
Audit/quality assurance
Contingency planning/business continuity
Internet expertise
Selection of internet banking providers
Internet banking functions available

Cluster 2: Internet Banking and Physical Security Risks

[a] Risk management and risk management controls
Security risks
Costs versus security breaches
[b] Controlling client PCs
Desktop computer controls
[c] Password management
Password management alternatives
Retrieving lost passwords
[d] Watching the employees
Surveillance in and around the office
[e] Controlling networks and servers
Managing network administration
EFT switches and network services
Electronic imaging systems
Operational and administrative security
Authentication security
Encryption security
[f] Shutting down compromised systems
Manageable security enforcement
Sample secure applications e-mail security
Internet access security
[g] Physical security
Security monitoring system overview
Major hazards
Fire flooding
Riot and sabotage
Freud or theft
Power failure
Equipment failure
Housekeeping rules

Cluster 3: Internet Banking Auditing

[a] Website and internet banking features checklists
Website development and hosting
Internet banking package
Cash management package
Bill pay
Security
Options
[b] Internet banking policy
Goals and objectives
Vendor management
Maintaining the institution's image
Insurance coverage
User access devices
File update responsibilities
Account reconciliation
Bill payment services
Bill pay controls
Bill pay processing
Bill pay customer support
Disaster recovery
Employee access
Security
Internet banking services request/fulfilment
Internet banking registration form
User logs and error reports
Privacy external links
Dial-in access (if applicable)
Audit
Geographic boundaries

Cluster 4: Identifying Customers in an Electronic Environment

[a] Establishing the identity of an applicant
Identification documents
Information collection
Verifying identification information
[b] Assisting customers who are victims of identity theft
What to tell to victims of identity theft
Using the FTCs affidarit
[c] Authentication in electronic banking environment
Risk assessment
Account origination and customer verification
Transaction initiation and authentication of established customers
Monitoring and reporting
Authentication methods: passwords and PINs
Digital certificates using public key infrastructures (PKI)
Tokens
Biometrics

Cluster 5: Electronic Commerce

[a] The computer network
Security of internal networks
Security of public networks
[b] Electronic capabilities
Examination categories for electronic capabilities
(Level 1: information only systems)

(Level 2: electronic information transfer systems)
(Level3: fully transactional information systems)
electronic payment systems
financial institution roles in electronic payment systems

[c] Risks

Specific risks to electronic systems

[d] Risk management

Strategic planning and feasibility analysis
Incidence response and preparedness
Internal routines and controls
Other considerations

VIII. REFERENCES

[1] Andersen, I.T. Security Barometer survey: The Psychology of Security, Quocirca, 2006.

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

[3] Backhouse, J. and Dhillon, G. Structures of Responsibility and Security of Information Systems, European Journal of Information Systems, 5(1), pp.2-9, 2006.

[4] Bandura, A. Self-efficacy: The Exercise of Control, New York, W.H. Freeman Publishing, 1997.

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

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

[7] Burham, B. The Internet’s Impact on Retail Banking, Booz-Allen Hamilton Third Quarter, (http://www.strategy-business.com/briefs/96301), 1996.

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

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

[10] Deal, T.E. and Kennedy, A.A. Corporate Cultures, Reading, MA: Addison- Wesley, 1982.

[11] Denison, D.R. Corporate Culture and Organizational Effectiveness, New York, Wiley, 1990.

[12] Dhillon, G. Interpreting the Managing of Information Systems Security. Unpublished PhD Thesis, London School of Economics and Political Science, University of London, 1995.

[13] Denzin, N.K. The Research Act, Third Edition, Prentice-Hall, Eaglewood Cliffs, New Jersey, USA, 1989.

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

[15] D.T.I. Security Special Report: The Internal Threat 2006, Technical Report, April, Department of Trade and Industry, London, 2006.

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

[17] ERNST and YOUNG. Global Information Security Survey, Ernst & Young, London, 2006.

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

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

[20] Gore, A. Putting People First in the Information Age, In: Masters of the Wired World, A. Lee, eds., Financial Times Pitman Publishing, London, pp.31-36, 1999.

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

[22] Jaeger, C.C., Renn, O., Rosa, E.A., and Webler, T. Risk, Uncertainty and Rational Action, First Published 2001, Earthscan Publications Ltd., London, 2001.

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

[24] Kotter, J.R. and Heskett, J.L. Corporate Culture and Performance, New York: Free Press, 1992.

[25] Kosiur, D. Understanding Electronic Commerce, Microsoft press, Redmond, Wash, 1997.

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

[27] Lagoutte, V. The Direct Banking Challenge, Unpublished Honours Thesis, Middlesex University, 1996.

[28] Locke, E.A. and Latham, G.P. A Theory of Goal Setting and Task Performance, Englewood Cliffs, NJ: Prentice-Hall, 1990.

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

[30] Markus, M.L. 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, 1989.

[31] Miles, M.B. and Huberman, A.M. Qualitative Data Analysis: An Expanded Sourcebook, Sage publications, Newbury Park, CA, 1994.

[32] Mitechell, T.R., Kenneth, R.T. and George-Falvy, J. 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.

[33] O’ Reilly, C.A. and Chatman, J.A. 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, 1996.

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

[35] Seijts, G.H. and Latham, G.P. 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, 2000.

[36] Schein, E.H. Organizational Culture and Leadership, 2nd Edition, San Francisco: Jossey-Bass, 1992.

[37] Siponen, M.T. A Conceptual Foundation for Organizational Information Security Awareness, Information Management and Computer Security, 8(1), pp.31-41, 2000.

[38] Straub, D.W., and Welke, R.J. Coping with Systems Risks: Security Planning Models for Management Decision Making, MIS Quarterly, 22(4), pp.441-469, 1998.

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

[40] Tan, M. and Teo, T.S.H. Factors Influencing the Adoption of Internet Banking, Journal of the Association for Informat ion Systems, 1(5), July 2000.

[41] Ternullo, G. Banking on the Internet: New Technologies, New Opportunities and New Risks, Boston Regional Outlook, Second Quarter, (http://www.fdic.gov/index.html), 1997.

[42] Trice, H.M. and Beyer, J.M. The Cultures of Work Organizations, Englewood Cliffs, NJ: Prentice Hall, 1993.

[43] Tushman, M.L., and O' Reilly, C.A. III Winning through Innovation, Boston: Harvard School Press, 1997.

[44] U.S. Department of Commerce The Emerging Digital Economy II, (http://www.ecommerce.gov/ede/), 1999.

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

[46] Wegge, J. 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, 2000.

[47] Weick, K.E. 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, 1985.

[48] Yin, R.K. Case Study Research, Design and Methods, Sage Publications, Newbury Park, CA, 1984.