ISSN : 2231-0711

E-Banking Security Adoption in the Organizational Context

Dr. Ioannis Koskosas
Dept. of Informatics and Telecommunications Engineering
University If Western Macedonia, Greece

Abstract-Although information security is critical for organizations to survive, a number of studies continue to report incidents of critical information loss. To this end, there is a continuous interest to study information security from a non-technical perspective. In doing so, this research focuses on organizational culture and commitment to e-banking security development and management. Even though considerable work has been done in banks in adopting e-banking security, continuous vigilance and management will be essential as the scope of e-banking increases. Two questions motivated this research. First, what is the possible relationship between organizational culture and commitment in e-banking adoption? Second, what is the effect of these organizational perspectives to the success in e-banking security adoption? A case study approach was used to investigate culture and commitment in e-banking security adoption at three banks in Greece. The results have shown that there is indeed a positive interrelation between organizational culture and commitment in e-banking security adoption and this interrelation affects positively e-banking security development through: e-banking project alignment, support from top management, information transparency, project flexibility, e-banking security knowledge and awareness, availability of resources and effective alignment of technology-organizational processes. The paper concludes that banks may need to re-consider their approach to e-banking adoption in favour of the long-term benefits it offers.

Keywords: e-banking security, culture, commitment, case study methodology

1. INTRODUCTION

The reliance by every organization upon information technology has increased dramatically as technology has developed and evolved. Over recent years, information has developed into a strategic asset, while the computerized information systems have become ultimate strategic tools for both government and organizations (McCumber, 2005; Sherwood et.al, 2005). Due to globalization and competitive economic environments, efficient information management is critical to business survival and effective decision making activities.

While e-banking can provide a number of benefits for customers and new business opportunities for banks, it exacerbates traditional banking risks i.e., operational risks, reputational risks, legal risks, security risks, to mention only few of them. In effect, the use of new distribution channels such as the internet increases the importance of e-banking security as it becomes sensitive to the environment and may leave organizations vulnerable to system attacks.

Although the area of e-banking has only appeared in Information Systems (IS) literature since the mid-1990s, there is a lack of research into e-banking security adoption and associated organizational issues, especially in the Greek context. There is also a lack of case studies reporting the actual experience of organizations in implementing e-banking security. Since e-banking is an IT product for development, this gap in the research poses some problems for banks, especially those who develop e-banking, because the limitations in relation to this area usually mean difficulties in planning and developing e-banking security.

This research aims to help address such gaps in the current literature by studying organizational culture and commitment in e-banking security adoption in terms of development and management. From one angle, human behaviour is complex and multi-faceted and this becomes more complicated in organizations whereas their culture defies the expectations for control and predictability that developers routinely assume for technology. From another angle, e-banking can provide enormous benefits to consumers in terms of ease and cost of transactions but it also poses new challenges for banks in supervising their financial systems and in designing and implementing necessary security measures and controls. Thus, understanding security through organizational culture and commitment in e-banking adoption is important for senior management since it would help them to improve e-banking security procedures.

Whilst there are many approaches to security (e.g., checklists, risk analysis, formal methods and soft approaches) whose value is evident, there is a belief that security can be more efficiently managed if the focus goes beyond technical oriented solutions (James, 1996; Siponen, 2001; Dhillon and Torkzadeh, 2006). This paper addresses this issue by reporting a case study approach in three Greek banks, namely, Omega-Bank, Vision-Bank and Front-Bank. In doing so, this research aims to investigate what is the possible relation between organizational culture and commitment in e-banking security adoption, what is the possible effect of such issues to the success in e-banking security development and what key lessons come out of their experience which could be generalised. The case is developed using qualitative research methods such as semi-structured interviews and observations.

In the following, a brief literature review is presented related to e-banking and security as well as the issues of organizational culture and commitment. The research methodology is described next. An analysis of the results and discussion section follow. At the end, lessons learnt from the case study, limitations and further research are presented.

2. SOFT-APPROACHES TO INFORMATION SECURITY

Similarly, in the context of information security, researchers' interest has also been on social and organizational factors, that may influence IS security development and management. Orlikowski and Gash (1994) have emphasized the importance of understanding the assumptions and values of different stakeholders to successful IS implementation. Such values have also been considered important in organizational change (Simpson and Wilson, 1999), in security planning (Straub and Welke, 1998) and in identifying the values of internet commerce to customers (Keeney, 1999). Dhillon and Torkzadeh (2006) have also used the value-focused thinking approach to identify fundamental and mean objectives, as opposed to goals, that would be a basis for developing IS security measures. These value-focused objectives were more of the organizational and contextual type.

A number of studies investigated inter-organizational trust in a technical context. Some of them have studied the impacts of trust in an e-commerce context (Gefen et al., 2003; Gefen and Straub, 2004; McKnight et al., 2002) and others in virtual teams (Ridings et al., 2002; Sarker et al., 2003). Workman (2007) studied trust as a factor in social engineering threat success and found that people who were trusting were more likely to fall victims to social engineering than those who were distrusting. Koskosas (2008) used a goal setting approach to identify weaknesses in security management procedures and found that goals are incongruent if employees misplace their trust to top management.

Siponen and Willison (2007, p. 1551) also reviewed 1043 papers of the IS security literature for the period 1990-2004 and found that almost 1000 of the papers were categorized as ‘subjective-argumentative’ in terms of methodology with field experiments, surveys, case studies and action research accounting for less than 10% of all the papers. That said, although less than 10% of all papers use a case study methodology this research due to the nature of the research questions follows a case study approach as it seems more appropriate to investigate a phenomenon within its real life context, as will be discussed in more detail further below.

2.1 Information Security Behaviour in the Context of Culture

Culture is the perception of organizational norms and values and so it exists within the organizations, not in the individual. To this end, individuals with different backgrounds or at different levels in the organization may tend to describe the organization in similar way.

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. One 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.

Albrechtsen (2006) found that users considered a user-involving approach to be much more effective for influencing user awareness and behaviour in information security. Leach (2003) studied influences that affect a user’s security behaviour and suggested that by strengthening security culture organizations may have significant security gains. Debar and Viinikka (2006) investigated security information management as an outsourced service and suggested augmenting security procedures as a solution, while von Solms and von Solms (2004) suggested a model based on the Direct-Control Cycle for improving the quality of policies in information security governance. Jones and Rastogi (2004) discussed the importance of gaining improvements from software developers during the software developing phase in order to avoid security implications. Siponen et al. (2007) advanced a new model that explains employees’ adherence to IS policies and found that threat appraisal, self-efficacy and response efficacy have an important effect on intention to comply with information security policies.

In terms of information security, organizational culture is a system of learned behaviour which is reflected on the level of end-user awareness and can have an effect on the success or failure of the information security process. Similarly, information security behaviour can be seen as part of the organizational culture and may define how employees understand information security risks. Since security and risk minimization are embedded into the organizational culture, all employees, managers and end-users, must be concerned with security issues in e-banking adoption. In order for e-banking adoption to ensure effective and proactive information security, all staff must be active participants rather than passive observers of e-banking security.

However most of the literature on organizational culture focuses on the hypothesis that strong cultures enhance organizational performance (Kotter & Heskett, 1992; Burt et al., 1994). This hypothesis is based on the notion that having widely shared and commonly held strong organizational norms and values lead to higher performance through at least three ways. First, a strong culture enhances coordination and control within the organization. Second, it improves goal alignment between the organization and its members. Third, a strong culture improves employee’s efforts. This paper supports the rationale that first, organizational culture may affect organizational commitment to e-banking security adoption through effective coordination and control. Second, organizational culture may have a positive effect to the success in e-banking security adoption.

2.2 Organizational Commitment

Locke et al. (1981) suggests that commitment is the determination to try for a goal and the persistence in pursuing it over time. In this paper, commitment is defined as a state of mind that holds people and organizations in line of behaviour (Staw, 1982) and encompasses psychological factors that force individuals to take action (Kiesler, 1971). Hence this paper supports the rationale that commitment may have an effect to the success in e-banking security adoption.

The successful development of an information system has long been believed to depend on the commitment to the project (Lucas, 1981; Kwon and Zmud, 1987). It also affects an organization’s effectiveness in converting information technology investments into useful outputs (Weill and Olson, 1989). On the contrary, lack of commitment could lead to indifference or deliberate resistance (Grover, et al., 1988) and may even cause project development to be abandoned (Ewusi-Mensah and Przasnyski, 1991).

Organizational commitment is clearly important to the success of information system (IS) development projects, but managers may sometimes become too committed to certain IS projects (Neumann, 1994). Sometimes decision makers are too committed to an information system project, even though, they are faced with indications that the project may be failing. In some cases, information systems development projects may take too much time, or even fail, if commitment is erratic, as in situations where the champion for the project departs in the middle of the project (Reich and Benbasat, 1990).

Considering that there is feedback on goal achievement, goal commitment, and task knowledge and given requisite ability and task familiarity, the more difficult and specific the goal, the higher the performance (Locke & Latham, 1990, 2002). Also, Crown and Rosse (1995) reported that when individual and group goals were congruent, group members were committed to increasing group performance.

There was a belief that information technology and security were difficult issues to be understood by non-IT staff. Nowadays, it is believed that people make the difference to information technology and e-banking security and that, training on the ethical, legal and security aspects of information technology usage should be ongoing at all levels within organizations (Nolan, 2005). A major need for effective information security arises from the poor state of security caused by low awareness levels within organizations. To this end, there is a need for increased security awareness in all employees and users at all levels within organizations, in terms of task knowledge and familiarity to e-banking security.

Thus, the main implication for information security is to focus on changing attitudes and human behaviour, which are part of the organizational culture, in order to enhance employees' commitment to e-banking security related tasks. In doing so, organizational commitment may have a positive effect to the success in e-banking security adoption.

3. Research Approach

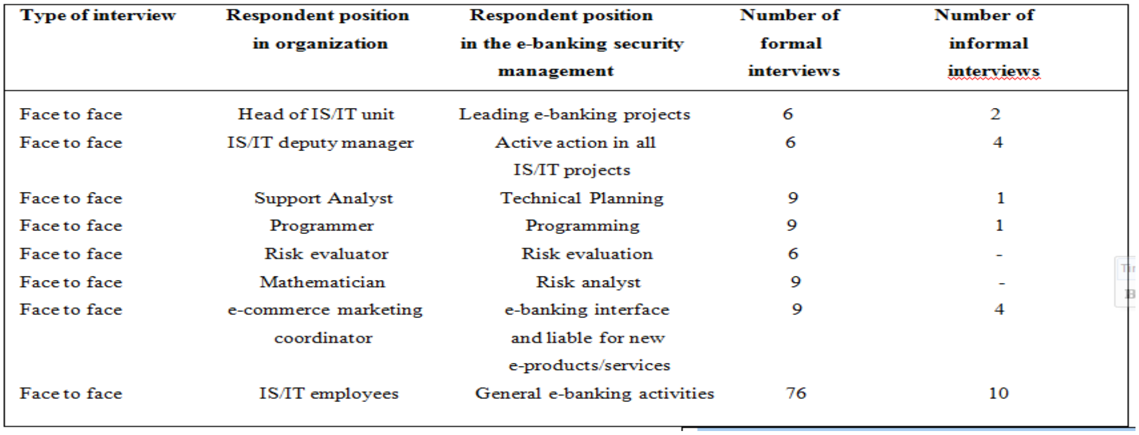
In order to identify appropriate research methods for this research, a taxonomy of IS research methods proposed by Galliers (1992) was used. The ontology of this research with regard to e-banking security is that security should not only be treated as something tangible and concrete, but also as an organizational issue. To this end, a qualitative research approach having philosophical foundations mainly in interpretivism was deemed appropriate for this study. Data were collected over a period of six months. Access to the banks was gained through insisting efforts in part of the researcher due to research purposes while the results were promised to be delivered to the banks in return. Vision Bank consisted of more than 5500 employees globally with approximately 400 employees in the IT unit. Omega Bank consisted of approximately 3000 employees with 100 of them positioned in the IT unit and Front Bank consisted of 2500 employees with approximately 60 employees in the IT unit. Details about the banks' annual return and financial figures are given in the section of the banks' background.

For the purpose of this research, multiple case studies was the approach to be chosen. 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) pointed out that the evidence from multiple case studies is often considered more convincing, with the overall study being considered more robust. This research further asserts that although studying multiple cases may not provide the same rich descriptions as do studies of single cases, multiple cases enable the analysis of data across cases. However, the method of selection could bias the results due to (a) the specific market sector studied, i.e., bank and (b) the investigation followed through within different cultures which may not apply to other cultures as well.

Data for this case study were collected using a number of data gathering tools such as interviews, archival records, documents (data triangulation) and observations. These tools and their applications in this research are described in the following.

3.1 Interviews

Rubin and Rubin (1995) defined interviews as, any verbal confirmation or dis-confirmation of observation or any formal, informal or casual answers to questions. Interviews took place as a primary tool for data collection, as they provide in-depth information about a particular research issue or question. The total number of people interviewed within the three banks was approximately 130. Each interviewee was conducted approximately 3 to 6 times during the 6-month period. The interviewees ranged from IT managers, deputy managers, auditors, and general IT staff. The interviews were conducted face-to-face, and when necessary, follow-up telephone interviews were scheduled to discuss unclear data. Table 1 presents the type of interviews and other related details. When the interviews were of the formal type, they were focused only upon the research and recorded. Informal interviews were conducted in informal settings such as lounge room, corridors, outside the building and were not tape recorded.



Type of interview	Respondent position in organization	Respondent position in the e-banking security management	Number of formal interviews	Number of informal interviews
Face to face	Head of IS/IT unit	Leading e-banking projects	6	2
Face to face	IS/IT deputy manager	Active action in all IS/IT projects	6	4
Face to face	Support Analyst	Technical Planning	9	1
Face to face	Programmer	Programming	9	1
Face to face	Risk evaluator	Risk evaluation	6	-
Face to face	Mathematician	Risk analyst	9	-
Face to face	e-commerce marketing coordinator	e-banking interface and liable for new e-products/services	9	4
Face to face	IS/IT employees	General e-banking activities	76	10

Table 1 Type of total interviews conducted within banks

3.2 Observations

An observation is the act of being part of a phenomenon, often with instruments and trying to recorded it for scientific reasons or otherwise. Data gathered also from observations are used for the purpose of description of settings, activities, people and the meanings of what is observed from the perspective of the participants (Patton, 1990). Observation was also useful during this research period as it provided useful insights into the banks' culture and overall commitment to e-banking security.

3.3 Examination of organizational documents

Another issue to be resolved with the research approach used here concerns data collection. This study employed multiple data-collection methods, as this is important in case research studies (Benbasat et al., 1987). In all cases, data were collected through a variety of methods and secondary data, including documents, reports, white papers, organizational records, and physical artefacts as shown in Table 2. The use of multiple data collection methods makes triangulation possible, and this provides for 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 case is likely to be more convincing and accurate if it 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, and interdisciplinary. The present study used data, theory, methodological and interdisciplinary triangulation.

- Organizational annual reports
- Banks' organizational chart
- Archival records
- Leaflets informing customers about e-banking products and services
- Investment reports
- E-banking security development reports on previous projects
- White papers
- Organizational records
- Financial investments on previous technologies relative to e-banking security
- Observation of physical artefacts

Table 2 Sources of secondary data used in this research

3.4 Data analysis

The analysis begins with the identification of themes emerging from the raw data and was focused over issues found to be critical. This technique provided a reflection in the understanding of organizational culture and commitment from different perspectives. The result findings were presented in the form of a report which was sent to all participants in the research. Thereafter, having discussed the findings with the research participants at Vision Bank, Omega Bank and Front Bank and after few corrections on the results interpretation it was commonly agreed that the data analysis was within focus.

4. Institutions' Background

Vision Bank (*the banks' names are not real due to confidentiality reasons*) is one of Greece leading providers of personal financial services and products with more than 5500 employees and assets of €35 billion in year 2009-2010. Vision Bank has more than 900 branches around the world, including Greece, and is a very innovative organization with large investments on new technologies that put Vision Bank at the forefront of providing financial services through its electronic channels in the country.

Similarly, Omega Bank consists of approximately 3000 employees and assets of €15 billion in year 2009-2010. Omega Bank has 600 branches in Greece and in 3 branches in the Balkans area (Bulgary, Yiogoslavia and Romania). The Bank invests steadily in new technology schemes such as e-banking. Finally, Front Bank has 230 branches in Greece and assets of €9 billion in year 2009-2010. Front Bank is a relatively new bank in the Greek financial market sector and focuses in the provision of financial products and services on-line.

4.1 The Banks' organizational culture

The organizational culture of Vision bank was held rather strong due to the determination of employees to cope with the organization's norms and values. In the context of e-banking, the culture of Vision Bank allowed for continuous planning in e-banking activities in order to meet future challenging security requirements.

In terms of e-banking security adoption, its organizational culture was reflected on the level of employees' security awareness which had an ultimate effect to the success in e-banking adoption. From the interviews, it was clear that its consistent organizational culture provided better coordination and control of e-banking security activities with a continuous effect upon employees' commitment to such activities. The IT deputy manager with regard to e-banking adoption stated: "*if you know your goals then you have to focus on achieving them with all available resources within reasonable time frames and at the lower cost. This is necessary if you like to act as a professional*". From this statement, it can be concluded that IT employees at Vision Bank were considering e-banking activities with full caution and awareness.

Similarly, the norms and values of the organizational culture at Omega Bank supported the participation of all staff in e-banking security activities since the main notion was that all should be active participants rather than passive observers. Since security and risk minimization are embedded into the organizational culture, all employees, managers and end-users must be concerned with e-banking security adoption.

To provide flexible and secure access, Front Bank continuously invested heavily in technology and went through many organizational changes. Having an IT security program consistent with the overall business goals ensures that problems can be managed for effectively during the support of e-banking products and services to the customers. That said, the security activities with regard to e-banking development and management, implies that part of them should consider the overall business goals of the bank strategic scheme; such business goals mainly include cost reduction, service quality and systems efficiency through channels integration. Front Bank used a middleware layer for the integration of different systems and channels. This middleware layer with a common interface to all existing systems enabled the IT unit of the bank to add new systems quickly and to implement a component-based architecture. By doing so, checking accounts, e-payments and so forth, were available as business objects in the middleware and could be used by all channels. Figure 1 shows the middleware layer at Front Bank which allowed for the coordination of business-technology goals and especially in e-banking adoption.

The security of e-banking channels, for Front Bank, was a key enabler for minimizing consumers' fears about such type of transactions, since security is one of the main obstacles for e-commerce growth (Turban et al., 2000). In doing so, Front Bank used the highest levels of encryption standards to secure e-banking services. The Front Bank IT deputy manager claimed "*we use the finest encryption techniques in all areas of our front end and back end systems. In particular, we use secure layer technology which encrypts all information, from a customer logging in or filling in an application form to storage and feedback to the customer*".

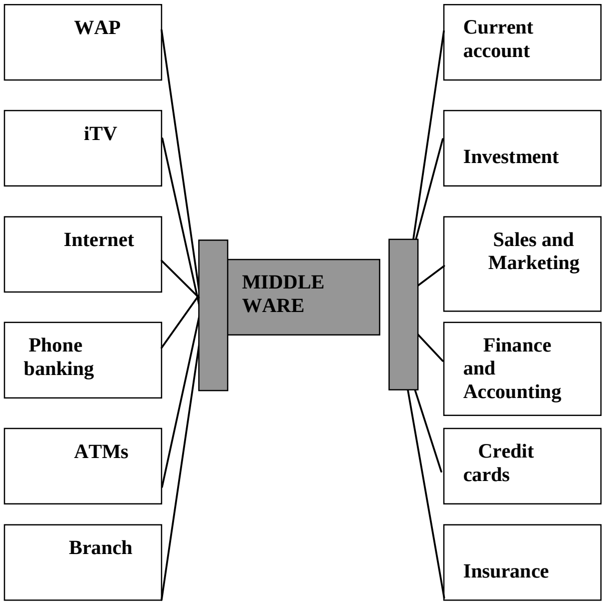


Figure 1 Integration of channels and services through middleware at Front Bank

The experience of the three banks in e-banking security activities was positively related to new technology schemes since the real-time perception of e-banking security risks was reflected on the overall success of e-banking security without any serious loses in the past, in terms, of operational failure, legal failure or successful attacks to systems.

4.2 Commitment within Banks

The commitment to e-banking security activities within Vision Bank was rather high and had an ultimate positive effect to the success of e-banking adoption. The bank through the organizational changes it experienced, adopted a very persistent approach to new security technology requirements in order to ensure that no problems will affect the trust of their customers in using e-banking services. The staff was affected by these changes with a result to insist in implementing security projects with accuracy and on time. However the employees' commitment was very consistent due to the consistency of the bank's organizational culture which in turn, provided better coordination and control of project activities in security tasks.

In Omega Bank, the employees' perception and knowledge of e-banking security risks was reflected on the overall success of e-banking security adoption since employees were motivated to act in high standards and be as more competitive they can against drawbacks. That said, there were few minor problems, occasionally, with regard to project funding since different political agendas from different organizational units within Omega Bank pulled the string far enough. That was due to competition in getting a larger share of funds in order to take advantage of larger investment projects within each competing unit. However the norms and values of Omega Bank did not allow much space for intrigue and conflict among these units since, ultimately, everyone understood the important role and requirements of the IT unit in investing continuously on new technology projects and particularly to e-banking security. As an IT employee said: "*we believed from the beginning that e-banking adoption will improve our products and services offered to our customers and to gain a larger share of the market by also reducing our operational costs especially those transaction costs*". Thus, any initial conflict between different banking units was minimized as a result of the strong organizational culture within Omega Bank which had an ultimate positive effect on commitment through better coordination and control of e-banking security activities.

Similarly, the commitment to e-banking security projects within the Front Bank was depicted to the overall success of e-banking projects that were finished on time and had no any side effects for the reputation of the bank. That said, the bank gave importance to e-banking security development projects with the main focus to ensure customers credibility and easy of access to financial products and services with the minimum cost while offering a secure environment. As it comes out from the interviews with IT member staff, the culture of Front Bank opened continuous channels of communication among employees in terms of e-banking applications. Specifically, its organizational culture allowed for the circulation of new ideas, and applications in the e-banking context and provided with more ease the communication of them between the bank's different units. As a consequence, all employees within Front Bank understood the importance of the capabilities e-banking can offer and the security needs that go along its development. In the following, the means through which organizational culture and commitment have an effect to the success of e-banking security adoption are presented.

4.3 Alignment of technology-organizational processes

Vision Bank was one of the first banks in Greece to offer e-banking products and services to its customers. In doing so, the bank went through many organizational changes in order adopt new technology investments to organizational needs. That means many processes had to be re-evaluated and re-designed from the beginning so that the staff could cope easily and without stress. A wide range of educational seminars for the organizational staff took place with an effective outcome on the followed through organizational activities. The main purpose was to align effectively 'tailor' new technology schemes into existing organizational processes that would allow the management of the daily work flow to continue more effectively. The culture of the bank and the commitment of employees to such changes made this alignment of technology-organizational processes as smooth as possible.

Similar technology-organizational processes were also adopted by Omega Bank which focused on expanding its communication technology network to its representative branches in Balkan countries. The bank invested large amounts to technology innovations such as its e-banking channel and to security projects that are tailored to e-banking solutions.

Front Bank did not have to go through many organizational changes since the bank is new in its market sector and from the beginning of its operations tailored its products and services to its dynamic presence on the web. That said, the strategy of the bank was mainly developed through alternative channels such as the Internet. In doing so, a large number of its customers are young people from the age of 20 to 40 years old.

4.4 Organizational flexibility

To provide flexible access, Vision Bank invested in new technology applications and went through some organizational changes such as the establishment of the e-banking unit as a separate banking unit with all the relevant resources dedicated for its purpose. In going on-line, the bank changed some of its business processes and departmental structures. The head of the IT unit, in which e-banking stated: "*we firstly introduced e-banking and then followed the re-engineering of business processes. In effect, there were many processes that were totally integrated and automated such as deposit books at the customer's request, delivering cheques or transfer of money*".

Thus, the culture the bank's culture allowed the organization to be flexible enough to radical changes and provided more efficient coordination and control of project activities with a positive effect on employees' commitment to relative projects.

In the context of e-banking security, Omega Bank invested on the latest encryption techniques for the exchange of information through its e-delivery channels. The bank hired knowledgeable people on security issues from software companies in order to develop its e-banking applications based on a secure environment that will build trust and credibility for its customers.

Front Bank due to its smaller structure and therefore its flexibility, was more easily adjusted to changes in technology solutions in the context of e-banking considering also that the bank since its initial operations had also a strong presence on-line. That said, the average age of the bank employees ranged from 24 to 45 years and were people that just either obtained their degree to information technology studies or had experience on technology solutions due to their experience in the software market.

4.5 Availability of resources

Availability of financial and human resources is critical in all types of development and maybe even more to security and that was equally understandable from the three banks. However, new technology development projects such as e-banking, shortage of readily financial or human resources may represent a main problem. Vision Bank, with regard to its human resources, got around this problem by implementing an intensive and time frequent training programme for new staff hired; with regard to financial resources, large amounts were invested on developing new software solutions (in-sourcing). Although there were some political agendas due to different executives' interests, the culture of Vision Bank did not allow any conflict to undermine any e-banking security investments and activities and so the IT staff was committed to its schedule.

Omega and Front Banks were also considering that availability of their human and financial resources in a similar context as Vision Bank. Both of them, invested on employees education on new technology solutions and applications through education seminars and practical training.

4.6 E-banking security knowledge and awareness

In all of the three banks, most of the interview participants exhibited full knowledge and awareness of e-banking security risks. That was a result of the training seminars which employees had to attend on a regular basis and of the exchange of information in doing so. The banks invested time and financial resources on employees to continuously upgrade their knowledge on e-banking security issues which is also depicted on their culture and commitment to e-banking security project development activities.

4.7 Support from top management

Support and understanding either ethical or financial from top management is a basic requirement for successful completion of e-banking projects (Turban et al., 2000). The culture within the three banks played a determined role in the effective communication between top management and the lower levels of the hierarchy which allowed the continuous planning and setting of e-banking security activities without any interruption. That was especially the case for Front Bank where its relatively small structure allowed for ease of communication between top management and employees. In doing so, the top management executives from the strategic hierarchy levels proposed a bonus motivation scheme on projects that met time deadlines. That enabled better coordination among the IT employees with a positive effect on the management of e-banking security projects. The support analyst stated: "*with the introduction of the bonus scheme the overall production and commitment was increased*". Thus, support from top management, in the form of the bonus scheme, had a positive effect to project deadlines and ultimately, to the success of e-banking security projects.

4.8 E-banking project alignment

Although security is a sensitive and confidential issue, the employees within Vision, Omega and Front Banks were participating to e-banking planning and development which allowed space for better coordination of project activities and clarity of project goals. In doing so, commitment to security activities led to better project alignment. The IT deputy manager of Vision Bank said: "*if you do not have efficient coordination on security planning and development, communication will break down and e-banking security activities will follow a dead end*". From the research results that was obvious the case for Omega and Front Banks as well.

4.9 Information transparency

In Vision Bank, a continuous effort was given to avoid different political agendas among the banking units and that there will be a continuous flow of information from higher levels of the hierarchy to lower and vice versa, without any obstacles in the communication process. That was achieved to a certain degree through the intervention of top management in dead-end times and where confusion was starting to take place among different banking units. The culture of the three banks enabled their employees to exchange information among each other and to compete as a team rather than individually. That was especially the case in Front Bank where its culture was more flexible to new information input and its structure was more flexible to market changes.

5. DISCUSSION

Two questions motivated this research. First, what is the possible relation between organizational culture and commitment in e-banking security adoption? Second, what is the effect of these organizational perspectives to the success in e-banking security adoption? The results have shown that there is indeed a positive interrelation between organizational culture and commitment in e-banking security adoption mainly through the organizational norms and values of Vision bank that enable a more effective coordination and control of security planning and management activities. Further this interrelation affects e-banking security through a variety of organizational issues such as: e-banking project alignment, support from top management, information transparency, project flexibility, e-banking security knowledge and awareness, availability of resources and effective alignment of technology-organizational processes.

Although there were some different political agendas between organizational units for project funding the culture of Vision bank controlled any possible conflicts that would be against its business objectives, through e-banking adoption, which included cost reduction, service quality and systems efficiency through channel integration. In the context of e-banking security, if a security task requires significant effort and interferes with the business tasks, business units need to understand the reason for this and be motivated to comply. Since business-unit people are users of security, failure to understand security needs will result to ineffective e-banking development and management through misunderstanding in communication at the expense of security.

At an organizational level, a success key to the success of e-banking adoption may be the consideration of organization’s needs and values at the centre of security design. Effective e-banking security adoption through development and management has to take into account different stakeholders needs, acknowledge that their needs may sometimes conflict and find a solution that is acceptable by all stakeholders. That said, understanding different stakeholder needs can form the basis for security commitment with respect to developing e-banking security goals, strategies and processes. In the practical application of security commitment, knowledge and understanding leads to a clear definition of the appropriate level of security measures with regard to e-banking security. The challenges of innumeracy, heuristic and other biases add to difficulty of commitment about security. Nevertheless, these perspectives need to be recognized in order for culture to be strengthened and so organizational commitment with regard to e-banking security risks.

However, an effective and successful e-banking security is not just about giving out information or about making stakeholders understand. Nowadays, successful e-banking security development is part of the organizational culture and commitment and can result when the quality of debate and understanding of security issues among all stakeholders is improved. In doing so, the process of information security with regard to e-banking will also improve.

5.1 Limitations and Further Research

There are opportunities to undertake further intensive research to identify more social and organizational factors that affect communication standards and procedures in e-banking security adoption. Although communication seems to positively influence e-banking security, we cannot be sure as to how communication can always do that. Future research should focus on the perception and development of communication strategies and how they could be applied to different organizational structures as well as security measures and policies according to organizational structure size that improve employees awareness on e-banking security issues. That said, different structured organizations may have different business objectives and therefore, security needs. Likewise, another issue interesting to investigate would be the role and type of feedback in communication in the context of e-banking, e.g., whether the type of feedback (outcome or process feedback) provided affects the communication-information security relationship.

The relationship between theory and practice may be considered weak and unstructured, as qualitative approaches have been criticised for not infusing theoretical factors. To this end, in this investigation an attempt was made to address this issue by investigating the communication standards and procedures which are critical to the success of e-banking security. Although, qualitative research does not offer the pretence of replication since controlling the research will destroy the interaction of variables, this investigation was conducted in a structured methodology guided by the specific organizational factors based on the literature review.

Moreover, the research findings may be influenced by political games that different banking units wish to play. As the participation in a research study can help organizational members to voice their concerns and express their views they can use this opportunity to put forward those views that they wish to present to other members of the organization. To this end, in order to mitigate or record the effect of ‘suspicion’ for interpretive research as suggested by Klein and Myers, this investigation used a collection of various perspectives such as archival documents, reports, white papers, bank regulations and an interpretation of how the interviewees react to the opinion expressed by other members.

6. CONCLUSIONS

The more organizations will rely on e-banking systems to survive in competitive markets the more increasing will become the need to ensure that security processes are managed more effectively. However the technology advancement rate for the use and management of e-banking security is more radical than ever if it is considered that security threats remain high.

There was a belief that information technology and security were difficult issues to be understood by non-IT staff. Nowadays, it is believed that people make the difference to information technology and security and that training on the ethical, legal and security aspects of information technology usage should be ongoing at all levels within organizations (Nolan, 2005). Thus, the main implication for e-banking security is to focus on changing attitudes and human behaviour which are parts of the organizational culture and commitment to e-banking security in order to enhance awareness among the employees about risk security issues. In doing so, banks may also need to re-consider their approach to technology-business goals in favour of the long-term benefits that new technology investments may offer in the long-term.

The relationship between theory and practice may be considered weak and unstructured, as qualitative approaches have been criticised for not infusing theoretical factors. To this end, in this research an attempt was made to address this issue by investigating the relation between organizational culture and commitment and their effect to the success in e-banking security adoption. Although, qualitative research does not offer the pretence of replication since controlling the research will destroy the interaction of variables, this research was conducted in a structured methodology guided by the specific organizational factors based on the literature review.

This study contributed to existing knowledge in a number of ways:

- It showed that there is indeed a positive interrelation between organizational culture and commitment to the success in e-banking security adoption mainly through effective coordination and control of security development and management
- It succeeded in uniting existing literature in this area and underpinning it with its findings from real world experience
- It managed to identify critical issues of organizational culture and commitment which have an effect in the success in e-banking security adoption. Such issues include: e-banking project alignment, support from top management, information transparency, project flexibility, e-banking security knowledge and awareness, availability of resources and effective alignment of technology-organizational processes.
- It provided new perspectives of research in the areas of e-banking security adoption and organizational culture and commitment.

There are opportunities to undertake further intensive research to identify more critical factors to the success in e-banking security adoption. Although organizational culture seems to positively influence organizational commitment, we cannot be sure as to how culture can always do that. Future research should focus on the perception and development of security risk strategies and how they could be applied to different organizational structures as well as the security measures and controls existent within organizations with different cultures. That said, different structured organizations may have different business objectives and therefore, security needs. Likewise, another issue interesting to investigate should be the role and type of feedback in commitment in the context of e-banking security, e.g., whether the type of feedback (outcome or process feedback) provided affects the commitment-project security relation.

7. REFERENCES

Albrechtsen, E. 2007 A Qualitative Study of User's View on Information Security, Computer and Security, 26(4), pp. 276-289.

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

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

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

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

Debar, H. and Viinikka, J. 2006 Security Information Management as an Outsourced Service, Computer Security, 14(5), pp. 416-434.

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

Dhillon, G. and Torkzadeh, G. (2006) Values-focused assessment of information system security in organizations, Information Systems Journal, 16(3), pp. 293-314.

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

Ewusi-Mensah, K. and Przasnyski, Z.H. (1999) On Information Systems Project Abandonment: An Exploratory Study of Organizational Practices, MIS Quarterly 15(1), pp.67-88.

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

Galliers, R.D. (1992) Choosing information system research approaches. In R. Galliers (Ed.), Information systems research: Issues, methods and practical guidelines (pp. 144-146). Oxford: Blackwell Scientific Publications.

Gefen, D., Karahanna, E. and Straub, D. (2003) Trust and TAM in online Shopping: An Integrated Model, MIS Quarterly, 27(1), pp. 51-90.

Gefen, D. and Straub, W. (2004) Consumer Trust in B2C e-Commerce and the Importance of Social Presence: Experiments in e-Products and e-Services, Omega, 32(6), pp. 407-424.

Grover, V., Lederer, A.L., and Sabherwal, R. (1988) Recognizing the Politics of MIS, Information and Management, 14(3), pp.145-156.

James, H. (1996) Managing Information Systems Security: A Soft Approach, In: P. Sallis (Ed.) Proceedings of the Information Systems Conference of New Zealand (pp. 10-20), Washington, D.C.: IEEE.

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.

Jones, R.L. and Rastogi, A. 2004 Secure Coding: Building Security into the Software Development Life Cycle, Information Systems Security, 13(5), pp. 29-39.

Keeney, R.L. (1999) The Value of Internet Commerce to the Customer, Management Science, 45(3), pp. 533-542.

Kiesler, C.A. (1971) The Psychology of Commitment: Experiments linking behaviour to beliefs, New York: Academic Press.

Koskosas, I.V. (2008) Goal Setting and Trust in a Security Management Context, Information Security Journal: A Global Perspective, 17(3), pp. 151-161.

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

Kwon, T.H. and Zmud, R.W. (1987) Unifying the Fragmented Models of Information Systems Implementation, In: Critical Issues in Information Systems Research, R.J. Boland and R.A. Hirschheim (eds.) Wiley, New York.

Leach, J. 2003 Improving User Security Behaviour, Computers and Security, 22(8), pp. 685-692.

Locke, E. A., Shaw, K. N., Saari, L. M., & Latham, G. P. (1981) Goal setting and task performance: 1969-1980. Psychological Bulletin, 90, pp. 125-152.

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

Locke, E.A. and Latham, G.P. (2002) Building a Practically Useful Theory of Goal Setting and Task Motivation, American Psychologist, 57(9), pp. 705-717.

Lucas, H.C. Jr. (1981) Implementation: The Key to Successful Information Systems, Columbia University Press, New York.

McCumber, J. 2005 Assessing and managing security risk in IT systems: a structured methodology, USA: Addison- Wesley.

McKnight, D.H., Cummings, L.L. and Chervany, N.L. (2002) Developing and Validating Trust Measures for E-Commerce: An Integrative Typology, Information Systems Research, 13(3), pp. 334-359.

Neumann, S. (1994) Strategic Information Systems: Competition Through Information Technologies, MacMillan College Publishing Company, Inc. New York.

Nolan, J. (2005) Best practices for establishing an effective workplace policy for acceptable computer usage, Information Systems Control Journal, 6(2), pp. 32-35.

Orlikowski, W. and Gash, D. (1994) Technological Frames: Making Sense of Information Technology in Organizations, ACM Transactions on Information Systems, 12(3), pp. 174-207.

Patton, M. (1990) Qualitative evaluation and research methods (2nd ed.). London, UK: Sage Publications.

Reich, B.H. and Benbasat, I. (1990) "An Empirical Investigation of Factors Influencing the Success of Customer-Oriented Strategic Systems," Information Systems Research, Vol. 1, No. 3, pp. 325-347.

Ridings, C., Gefen, D. and Arinze, B. (2002) Some Antecedents and Effects of Trust in Virtual Communities, Journal of Strategic Information Systems, 11(3/4), pp. 271-295.

Rubin, H.J. and Rubin, I.S. (1995) Qualitative Interviewing, the Art of Hearing Data. CA, USA: Sage Publications.

Sarker, S., Valacich, S.J. and Sarker, S. (2003) Virtual Team Trust: Instrument Development and Validation in an IS Educational Environment, Information Resources Management Journal, 16(2), pp. 35-55.

Sherwood, J., Clark, A. and Lynas, D. 2005 Enterprise Security Architecture: A business- Driven Approach, San Francisco, CA, USA: CMP Books.

Siponen, M.T. (2001) An Analysis of the Recent IS Security Development Approaches: Descriptive and Prescriptive Implications. In G. Dhillon (Ed.), Information Security Management: Global Challenges in the New Millenium (pp. 101-124). Hershey, PA: Idea Group.

Siponen, M. and Willison, R. (2007) A Critical Assessment of IS Security Research Between 1990-2004, The 15th European Conference on Information Systems, Session chair: Erhard Petzel, pp. 1551-1559.

Siponen, M., Pahnila, S. and Mahmood, A. (2007) Employees' Adherence to Information Security Policies: An Empirical Study, In: IFIP International Federation for Information Processing, Vol. 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J. von Solms, R., (Boston: Springer), pp. 133-144.

Staw, B.M. (1982) Counterforces to change, In: P.S. Goodman and Associates (eds), Change in Organizations: New Perspectives on Theory, Research and Practice, pp. 87-121, San Francisco: Jossey-Bass.

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

Turban, E., Less, J., King, D., and Shung, H.M. (2000) Electronic Commerce: A Managerial Perspective. London, UK: Prentice-Hall.

Von Solms, R. and Von Solms, S.H. 2006 Information Security Governance: A model based on the Direct-Control Cycle, Computers and Security, 25(6), pp. 408-412.

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

Weill, P., & Olson, M. H. (1989). An Assessment of the Contingency Theory of Management Information Systems. Journal of Management Information Systems, 6(1), pp. 59-85.

Workman, M. (2007) Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security, 16(6), pp. 315-331.

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