

Article

TRUST AND RISK COMMUNICATION IN SETTING INTERNET BANKING SECURITY GOALS

Ioannis V. Koskosas

University of Western Macedonia, Kozani, Greece

Correspondence: Ioannis V. Koskosas, Department of Information and Communication Technologies Engineering, University of Western Macedonia, Agios Dimitrios Park, Kozani 50100, Greece.
E-mail: ikoskosas@uowm.gr

Abstract

The aim of this research is to investigate information systems security in the context of Internet banking. In doing so, it adopts a socio-organizational approach to the subject matter by investigating the interrelationship between trust and risk communication within information technology groups and their possible effect on the level of security goal setting. The research explores and describes different socio-organizational issues and seeks to demonstrate the importance of trust and risk communication in setting efficiently Internet banking goals within the broader context of information systems security management. To this end, it gives also an overview of different goal setting procedures within the IT departments of three financial institutions.

Keywords

trust; risk communication; security management; Internet banking

Risk Management (2008) 10, 56–75.

doi:10.1057/palgrave.rm.8250035

Introduction

The research described in this paper is concerned with information systems security in the context 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). 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). The research reported in this paper makes the consideration that although IT managers and groups have a variety of security risk management methods, tools and techniques available, they may not make an efficient use of them in the context of risk management activities. 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, the research in this paper adopts a socio-organizational approach to investigate information systems security within the scope of Internet banking by exploring and describing the concept of trust and risk communication within the use of goal setting theory. In the following sections, the issue of Internet banking is being briefly discussed. Then, the research approach used for the purposes of this investigation is being discussed and the concepts of trust, risk communication and goal setting are introduced. Thereafter, the paper presents the empirical research findings and ends with some conclusions.

Research approach

The objectives of this research were to investigate:

- 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;
- if there is an interrelationship between trust and risk communication at the level of security goal setting;
- if there is an effect of trust and risk communication at the level of security goal setting.

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). Owing 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 generalized, but appropriate definition is: "Qualitative research is multimethod in focus, involving an interpretive, naturalistic approach to its subject matter" (Denzin and Lincoln, 1998). This definition implies that qualitative researchers study things in their natural environment and understand events in terms of the meaning people assign to them and this is the strategy applied to this investigation. The term "interpretivism" is defined as "Studies that assume that people create and associate their own subjective and intersubjective meanings (inductive process) as they interact (processual) with the world around them (contextual)" (Orlikowski and Baroudi, 1991).

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

The next issue under consideration was the research method to be used. Having considered the possible benefits of each available method for example 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 generalizability, 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 interrelationship of different socio-organizational perspectives to different IT group structures. For example, the IT department of Alpha-Bank consisted of approximately 40 employees, while in Delta-Bank 150 employees, and in Omega-Bank 410 employees, respectively.

However, another issue to be resolved with the research approach used here concerns data collection. The design of this investigation employed multiple data collection methods as it is important in case research studies (Benbasat *et al.*, 1987). In all cases data were collected through a variety of methods including interviews, documents, and observation and visits to the banks lasted for approximately 3 months. The total number of interviews within the three case studies, numbered to 15. 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 (Flick, 1992; Denzin, 1989). 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.

Having discussed the research approach, the paper then will introduce the concepts of goal setting, trust, and risk communication in order to provide a deeper understanding of the issues under investigation.

The issue of Internet banking

The Internet has rapidly gained popularity as a potential medium for electronic commerce (US Department of Commerce, 1999). The reasons 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 (Tan and Teo, 2000). 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.

The concept of goal setting

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

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

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

In the first proposition, research shows that when individuals accept an assigned difficult goal, task performance tends to increase. In particular, 90% of the studies support this proposition with an effect size on performance being

approximately 10–15% 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% of those studies support the second proposition with an effect size on performance being approximately 8–16% 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 a group level will improve the process of information systems management in the context of Internet banking security. Consequently, the main research question becomes: Do organizations set goals relevant to the management of the integrity, confidentiality and availability of information through the Internet banking channel?

The concept of trust

Trust is a social phenomenon. In their research Porta *et al.* (1996) review several studies (Coleman, 1990; Putnam, 1983; Gambetta, 1998) on trust. These studies argue that trust determines the performance of a society's institutions so that according to them trust is a propensity of people in a society to cooperate to produce socially efficient outcomes (Coleman, 1990). Putnam (1983), for example, defines trust as a habit formed over centuries long history of "horizontal networks of association" between people covering both commercial and social activities. Rousseau *et al.* (1998, p 395) defined trust as: a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another. In this paper we treat trust as a unidimensional psychological state, although we recognize that trust is a complex psychological state that may consist of different dimensions.

A handful of studies suggest that trust is beneficial to organizations through two main effects. Either when trust results in direct effects on a variety of outcomes or when moderates the effects of other determinants on attitudinal, perceptual, behavioural and performance outcomes via two distinct perceptual processes. Hence, instead of proposing that trust directly results in desirable outcomes, this paper suggests that trust moderates the effects by providing the

conditions under which a certain outcome, such as risk communication is likely to occur. Trust though is defined as confidence and positive expectations of one party within an IT group that another party is willing to cooperate to set goals efficiently, in the context of Internet banking security.

According to Mayer *et al.* (1995), individuals' beliefs about another's ability, benevolence and integrity, lead to a willingness to risk, which in turn leads to risk-taking in a relationship, as manifested in a variety of behaviours. Thus, a higher level of trust in a work partner increases the likelihood that one will take a risk with a partner (e.g., cooperate, share information) and/or increases in the amount of risk that is assumed. Consequently, risk-taking behaviour is expected to lead to positive outcomes for example individual performance, and in social units such as work groups, cooperation, information sharing are expected to lead to higher unit or group performance (Klimoski and Karol, 1976; Larson and LaFasto, 1989; Davis *et al.*, 2000).

However, other studies examining the main effect of trust on workplace behaviours and outcomes found only partial support or no support. That is, some studies report a significant main effect, others do not. For instance, while Boss (1980) found that trust within group has a positive effect on openness in communication, De Dreu *et al.* (1998) found that trust between negotiators mediates the effects of social motives and punitive capability on information exchange. Hwang and Burgers (1997) proposed that trust is necessary, but not sufficient, condition for cooperation. This terminology suggests that trust may act as a moderator, although the mathematical model does not specifically consider how trust might operate in this manner.

Given all these characteristics of trust this investigation further supports that trust may also have an effect on the communication of messages between the employees of an IT group as well as on the level of goal setting with regard to Internet banking security. To this end, this investigation supports the rationale that trust at group level:

- provides the conditions under which an efficient communication of risks is likely to occur
- plays a significant role at the macro-goal level of security management.

The concept of risk communication

Communication, in simple terms, could be thought as an interactive process of sending and receiving messages among individuals, groups and organizations including some form of feedback. Although there are numerous definitions for the term "communication", this investigation adopts DeVito's (1988, p 14) definition that covers the essentials of the communication as the act: "communication refers to the act, by one or more persons, of sending and receiving

messages that are distorted by noise, occur within a context, have some effect, and provide some opportunity for feedback”.

Risk communication, however, is believed to be part of the risk management process as it allows the selection of risk control options and supplies the information on which third parties such as the government, industry or individual decision makers base their choices (National Research Council, 1989). Thus, the US National Research Council (NRC) defines risk communication as:

Risk communication is an interactive process of exchange of information and opinion among individuals, groups, and institutions. It involves multiple messages about the nature of risk and other messages, not strictly about risk, that express concerns, opinions, or reactions to risk messages or to legal and institutional arrangements for risk management. (NRC, p 21)

However, risk communication is more complicated and difficult as it might appear. In particular, what makes risk communication difficult is not only the exchange of information among the parties involved, but also among the wider institutional and cultural contexts within which risk messages are formulated, transmuted and embedded (Krimsky and Plough, 1988).

The National Research Council distinguishes between two types of major problems in risk communication: those deriving from institutional and political systems and those between risk communicators and receivers. In the first case, various kinds of legal considerations such as liability and informed consent, affect the content of risk messages by influencing the available options for risk managers. Similarly, the problems between risk communicators and receivers arrive in case of difficulty to establish and recognize credibility, being alert in case of emergency, make messages understandable, capture and focus public's attention, and receive information (NRC, 1989).

Moreover, the success of risk communication is limited due to the insufficient attention it pays to social contexts within which individuals live and communicate (Otway and Wynne, 1989). In addition, it should be considered that the parties sending the messages may not always be honest, reliable as well as responsible (Otway and Wynne, 1989).

Risk communication though emerged from risk perception as the general public concerns about hazards were different to those of the experts, that is, the scientific and policy-making communities (NRC, 1989; Slovic, 1990). The difference, in particular, was that experts tended to focus on measurable, quantified attributes of risks while the public tended to focus on the qualitative value-laden attributes of risks such as fairness and controllability (Groth, 1991).

Sandman (1987) uses the term “outrage” to incorporate many of the qualitative dimensions of risks while “hazard” is the quantitative, measurable

aspect of risk. According to him, although the public seems concerned with “outrage” at the expense of “hazard”, the experts often tend to ignore “outrage” at their own danger. He also points out that if the public’s legitimate concerns are not being addressed by the risk management process, the outrage level will be greater than when the public concerns are taken into consideration.

Thus, risk communication was developed as a way to communicate effectively the experts’ assessments of risks to the public so that the public would understand the real nature of risks and at the same time, to diminish the tension among parties with different perceptions of risks (Herriot and Firestone, 1983). This investigation supports that an efficient communication of risks has an effect on the level of security goal setting. Specifically, risk communication *plays a significant role at the macro-goal level of security management.*

Research findings

Goal setting

It was imperative for this investigation that any organization used for the research should have followed goal setting procedures and particularly the organizations’ 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 all of the three organizations, come in the form of projects which either originate from the top-management to the different banking units or from those units to the top-management in the form of project proposals. Goal setting activities, in the context of security risk management, are distinguished into three main phases, as shown in Figure 1: the *goal setting initiation phase*, the *goal execution phase* and the *evaluation phase*.

However, it is not in the scope of this 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

<i>1st Phase: Goal Setting Initiation Phase</i>	
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)
<i>2nd Phase: Goal Execution Phase</i>	
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
<i>3rd Phase: Evaluation Phase</i>	
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 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.

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

The interrelationship of trust and risk communication

The communication between the employees in Delta-Bank took place through various means including e-mails, telephone and face-to-face meetings. Although the communication within Delta-Bank was efficient, mainly due to the strictly followed procedures, there were a few communication problems which were explained as a result of mistrust between some of the employees to the management. With regard to the security risk event of fault tolerance, different political agendas had influenced the communication of security risk messages between the involved project teams to a certain degree. The postponement of the vulnerability assessment scheme due to different stakeholders' interests caused also a breach in the communication of risks between different banking units. Thus, mistrust of the motives, attitudes and beliefs of one party towards another had a negative impact on the way communication was processed within Delta-Bank.

Another problem in communication was that the number of employees in the IT group was large, which did not allow flexibility in decision making, as compared to the case of Alpha-Bank. In addition, the non-participation of some IT employees in decision making created feelings of mistrust and dissatisfaction, with an ultimate effect on the communication of messages within the

group, as the employees felt less motivated to participate in group activities. Although the issue of trust had a weak effect on the overall communication of security risk messages within the IT group, it was argued that trust provides the conditions under which an efficient communication of risks occurs through the *employees' satisfaction to the management, increased efforts and cooperation in group activities*.

In the case of Omega-Bank, the restriction of e-mail usage by a large number of employees created a "climate" of dissatisfaction among the employees, as they argued that the information flow within the bank was less accurate. Similarly, the different stakeholders' interests and the different political agendas had also an effect on the level of risk communication within Omega-Bank. From the interviews, it was argued that the communication of messages within Omega-Bank was quite often difficult due to the large size of the organization. That means there was a circulation of messages among different parties within different units of the bank and the involvement of such parties on decisions was, in some cases, unnecessary.

On the contrary, the communication of security risks within the Alpha-Bank IT group was characterized as efficient due to the high levels of trust between co-members and the shared values and beliefs consistent with the overall Alpha-Bank's culture. Evidence shows that there were not any particular problems in communication since the banking units were consistent of a small number of employees which allowed flexibility in managing projects. However, the efficient communication of security risk messages with regard to Internet banking was also attributed to the knowledgeable perception of risks between the IT employees which was based on good educational skills on the subject matter and of the clarity in goal achievement.

Therefore, evidence shows that there is indeed an interrelationship between trust and risk communication although the cases of Delta and Omega-Bank have shown different socio-organizational behaviour patterns. The main reason was the fact that people within Delta- and Omega-Bank valued most professionalism in terms of how capable is an individual or group to "deliver". When the IT deputy manager within Omega-Bank was asked to comment on that he replied: *policies and procedures should run the bank, not necessarily individual initiative*. For example, the top-management within Delta- and Omega-Bank did not allow all of the IT group members to participate in security goal activities due to the high confidentiality of the issue. To this end, some of the employees within the IT group and between different banking units, developed feelings of mistrust with an overall effect on the level of risk communication. Likewise, the IT groups within Delta- and Omega-Bank consisted of a large number of people which did not allow flexibility in decision making, like in the case of Alpha-Bank. In effect, there were a few problems in communication between different banking units and within the IT groups on issues of high concern such as the security of Internet banking.

The effect of trust and risk communication on goal setting

As previously described, goal setting within Delta- and Omega-Bank was an integral part of the organizations' overall business activities plan. From the interviews within Delta-Bank, the issue of trust was believed to have an effect on the level of goal setting to the degree that one party or group was capable of delivering. The differences of the business scope within different banking units had an effect on the IT groups' activities because the business units did not seek always to "deliver". Thus, some of the IT projects found difficulties at the project initiation phase, as the IT groups had to postpone decisions on security issues. Such an example includes the upgrade of the system fault tolerance level and the issue of vulnerability assessment.

The restriction imposed to some IT employees to participate in the process of goal setting with regards to the security of Internet banking, established a level of mistrust between these employees to the management, as they felt incapable of delivering. To this end, considering that trust in this investigation has been defined as willingness to cooperate in order to produce efficient work outcomes, trust had an effect on the level of security goal setting, although weak, as the non-participation of some IT employees to goal setting did not allow them to cooperate efficiently and even transfer their knowledge to other members within the group.

Similar patterns were exhibited in the case of Omega-Bank with the establishment of the Disaster Recovery Planning (DRP) centre, whereas different stakeholders' interests were diverged from those in the IT group. In effect, the DRP's input to goal setting was controlled since the DRP activities contribute to the risk monitoring and evaluation phase, as they also focus on post-evaluation implementation on security related projects.

The perception of Internet banking security risks within the Delta- and Omega-Bank IT groups was based on the same, knowledgeable criteria mainly due to educational and training courses the IT members had to attend. When the interviewees were being asked questions in the context of Internet banking 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 communication between members within the group. The confident, knowledgeable perception of security risks within the Delta and Omega-Bank IT departments was reflected on the overall success in Internet banking projects and in the effective project cooperation with third-party companies.

During the interviews though within both organizations, there was an argument that the communication of security risk messages was not always efficient due to different political agendas and competition between the banking units. Thus, the difficulties identified in the communication process had an ultimate effect at the level of goal setting particularly on specialized issues such

as Internet banking. Evidence shows that communication was a vital aspect of security goal setting since the activities defined in the context of risk management had to be coordinated with the overall organizations' activities, particularly when conflicts arise.

Conclusions

The cases of Delta- and Omega-Bank exhibited slightly different patterns of socio-organizational behaviour although the process of goal setting in the context of risk management was based on the same principles among the three case studies. Specifically, the undertaking of the three empirical studies revealed that IT managers and groups do set security goals with regard to the management of the integrity, confidentiality and availability of information through the Internet banking channel. Moreover, evidence has shown that there is indeed an interrelationship between trust and risk communication and that these issues have an ultimate effect on the level of security goal setting. However, this interrelationship and effect is stronger in organizations with small structures because such organizations exhibit "family-oriented" business patterns whereas the values and beliefs are strongly held and widely shared among the organizational members. Although the interrelationship and effect of such socio-organizational issues apply to organizations with large structures, their impact is rather minimal because such organizations depend strictly on manuals and procedures, which focus on professional criteria rather than individual initiative and intellect.

Evidence also has shown that trust provides the conditions under which an efficient risk communication occurs through employees' satisfaction to top-management, positive attitudes, increased efforts and higher levels of cooperation between members through participation in group activities. Likewise, the existence of different political agendas was found to have a greater impact to large organizations as compared to small ones. The conflict type identified within the three case studies was mainly due to differences in business scope between different banking units rather than due to insufficient knowledge on subject matters. The case of Alpha-Bank, the small structure organization, has exhibited greater flexibility in decision making and consistency within the IT group activities as compared to the other cases with large structures.

A major conclusion with regard to security is that socio-organizational issues such as trust and risk communication play an important role in the process of goal setting. To this end, failure to recognize and improve such socio-organizational issues may lead to inefficient processes of goal setting, whereas security risks with regard to the integrity, confidentiality and availability of information through the Internet banking channel, may arise.

Acknowledgements

The author would like to thank the reviewers of this paper for their useful comments before submission.

Note

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

References

- Andersen, K.V. (1998). *EDI and Data Networking in the Public Sector: Governmental Action, Diffusion, and Impacts*. Boston: Kluwer Academic Publishers.
- Backhouse, J. and Dhillon, G. (1996). Structures of Responsibility and Security of Information Systems. *European Journal of Information Systems*. Vol. 5, No. 1, pp 2–9.
- Bandura, A. (1997). *Self-Efficacy: The Exercise of Control*. New York: W.H. Freeman Publishing.
- Benbasat, I., Goldstein, D.K. and Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*. Vol. 11, No. 3, pp 369–386.
- Boss, R.W. (1980). Trust and Managerial Problem Solving Revisited. *Group and Organization Studies*. Vol. 3, pp 331–342.
- Burnham, B. (1996). *The Internet's Impact on Retail Banking*, Booz-Allen Hamilton Third Quarter (<http://www.strategy-business.com/briefs/96301>).
- Cavaye, A.L. (1996). Case Study Research: A Multi-Faceted Research Approach for IS. *Information Systems Journal*. Vol. 6, No. 3, pp 227–242.
- Coleman, J. (1990). *Foundations of Social Theory*. Cambridge: Harvard University Press.
- Davis, J., Schorman, F.D., Mayer, R. and Tan, H. (2000). Trusted Unit Manager and Business Unit Performance: Empirical Evidence of a Competitive Advantage. *Strategic Management Journal*. Vol. 21, pp 563–576.
- De Dreu, C., Giebels, E. and Van de Vliert, E. (1998). Social Motives and Trust in Integrative Negotiation: The Disruptive Effects of Punitive Capability. *Journal of Applied Psychology*. Vol. 83, pp 408–423.
- Denzin, N.K. (1989). *The Research Act*, 3rd edn. Englewood Cliffs, NJ: Prentice-Hall.
- Denzin, N. and Lincoln, Y. (1998). Major Paradigms and Perspectives. In Denzin, N.Y.K. and Lincoln, Y.S. (eds) *Strategies of Qualitative Inquiry*. Thousand Oaks: Sage Publication.
- DeVito, J.A. (1988). *Human Communication*, 4th edn. New York: Harper & Row, Inc.
- Eisenhardt, K.M. (1989). Building Theories from Case Study Research. *Academy of Management Review*. Vol. 14, No. 4, pp 532–550.
- Forcht, K. and Wex, R. (1996). Doing Business on the Internet: Marketing and Security Aspects. *Information Management and Computer Security*. Vol. 4, No. 4, pp 3–9.
- Flick, U. (1992). Triangulation Revisited: Strategy of Validation or Alternative? *Journal for the Theory of Social Behaviour*. Vol. 22, pp 175–198.
- Gambetta, D. (1998). *Trust: Making and Breaking Cooperative Relations*. Cambridge: UK, Basil Blackwell.
- Gore, A. (1999). Putting People First in the Information Age. In Lee, A. (ed) *Masters of the Wired World*. London: Financial Times Pitman Publishing, pp 31–36.

- Groth, E. (1991). Communicating with Consumers About Food Safety and Risk Issues. *Food Technology*. Vol. 45, No. 5, pp 248–253.
- Herriot, R.E. and Firestone, W.A. (1983). Multisite Qualitative Policy Research: Optimizing Description and Generalizability. *Educational Researcher*. Vol. 12, No. 3, pp 14–19.
- Hwang, P. and Burgers, W. (1997). Properties of Trust: An Analytical View. *Organizational Behaviour and Human Decision Processes*. Vol. 69, pp 67–73.
- 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.
- Klimoski, R.J. and Karol, B. (1976). The Impact of Trust on Creative Problem Solving Groups. *Journal of Psychology*. Vol. 61, pp 630–633.
- Kosir, D. (1997). *Understanding Electronic Commerce*. Redmond, WA: Microsoft Press.
- Krimsky, S. and Plough, A. (1988). *Environmental Hazards: Communicating Risks as a Social Process*. Dover, MA: Auburn House Publishing.
- Lagoutte, V. (1996). *The Direct Banking Challenge*, Unpublished Honours Thesis, Middlesex University.
- Larson, C. and LaFasto, F. (1989). *Teamwork*. Newbury Park, CA: Sage.
- Locke, E.A. and Latham, G.P. (1990). *A Theory of Goal Setting and Task Performance*. Englewood Cliffs, NJ: Prentice-Hall.
- Markus, M.L. (1989). Case Selection in a Disconfirmatory Case Study. In Cash, J.I. and Lawrence, P.R. (eds) *The Information Systems Research Challenge: Qualitative Research Methods*, Harvard Business School Research Colloquium, Cambridge, MA: Harvard Business School, pp 20–26.
- Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review*. Vol. 20, pp 709–734.
- Miles, M.B. and Huberman, A.M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. Newbury Park, CA: Sage Publications.
- Mitchell, T.R., Kenneth, R.T. and George-Falvy, J. (2000). Goal Setting: Theory and Practice. In Cooper, C.L. and Locke, E.A. (eds) *Industrial and Organizational Psychology: Linking Theory with Practice*. Oxford: Blackwell Publishers Ltd. (First Published 2000).
- National Research Council (1989). *Improving Risk Communication*, Report of the Committee on Risk Perception and Communication, Commission on Behavioural and Social Sciences and Education, National Research Council. Washington, DC: National Academy Press.
- Orlikowski, W. and Baroudi, J.J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*. Vol. 2, No. 1, pp 1–28.
- Otway, H. and Wynne, B. (1989). Risk Communication: Paradigm and Paradox. *Risk Analysis*. Vol. 9, No. 2, pp 141–145.
- Porta, R. Lopez-de-Silanes, F., Shleifer, A. and Vishny, R. (1996). *Trust in Large Organizations*, NBER Working Paper.
- Putnam, L.L. (1983). The Interpretive Perspective: An Alternative to Functionalism. In Putnam, L.L. and Pacanowsky, M.E. (eds) *Communication and Organization*. Beverly Hills, CA: Sage, pp 31–54.
- Rousseau, D., Sitkin, S., Burt, R. and Camerer, C. (1998). Not So Different After All: A Cross-Discipline View of Trust. *Academy of Management Review*. Vol. 23, pp 387–392.
- Sandman, P. (1987). Risk Communication: Facing Public Outrage. *EPA Journal*. Vol. 13, No. 9, pp 21–22.
- Seijts, G.H. and Latham, G.P. (2000). The Construct of Goal Commitment: Measurement and Relationships with Task Performance. In Goffin, R. and Helmes, E. (eds)

- Problems and Solutions in Human Assessment: Honoring Douglas N. Jackson at Seventy.* Dordrecht, The Netherlands: Kluwer Academic Publishers, pp 315–332.
- Siponen, M.T. (2000). A Conceptual Foundation for Organizational Information Security Awareness. *Information Management and Computer Security*. Vol. 8, No. 1, pp 31–41.
- Slovic, P. (1990). The Legitimacy of Public Perceptions of Risk. *Journal of Pesticide Reform*. Vol. 10, No. 1, pp 13–15.
- Straub, D.W. and Welke, R.J. (1998). Coping with Systems Risks: Security Planning Models for Management Decision Making. *MIS Quarterly*. Vol. 22, No. 4, pp 441–469.
- Tan, M. and Teo, T.S.H. (2000). Factors Influencing the Adoption of Internet Banking. *Journal of the Association for Information Systems*. Vol. 1, No. 5, pp 217–245.
- Ternullo, G. (1997). *Banking on the Internet: New Technologies, New Opportunities and New Risks*, Boston Regional Outlook, Second Quarter (<http://www.fdic.gov/index.html>).
- U.S. Department of Commerce (1999). *The Emerging Digital Economy II* (<http://www.ecommerce.gov/ede/>).
- Walsham, G. (1995). Interpretive Case Studies in IS Research: Nature and Method. *European Journal of Information Systems*. Vol. 4, No. 2, pp 74–81.
- Wegge, J. (2000). Participation in Group Goal Setting: Some Novel Findings and a Comprehensive Model as a New Ending Ton at Old Story. *Applied Psychology: in International Review*. Vol. 49, No. 3, pp 498–516.
- Yin, R.K. (1984). *Case Study Research, Design and Methods*. Newbury Park, CA: Sage Publications.

Appendix 1

Internet Banking Security Checklist (Alpa-Bank)

Cluster 1: Internet Banking Policy

- *Internet banking risks and controls*
- *Transaction risks*
- *Control and security*
 - Security controls
 - Network and data access controls
 - User authentication
 - Firewalls
 - Encryption
 - Transaction verification
 - Virus protection
- *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

- *Risk management and risk management controls*
 - Security risks
 - Costs *vs* security breaches
- *Controlling client PCs*
 - Desktop computer controls
- *Password management*
 - Password management alternatives
 - Retrieving lost passwords
- *Watching the employees*
 - Surveillance in and around the office
- *Controlling networks and servers*
 - Managing network administration
 - EFT switches and network services
 - Electronic imaging systems
 - Operational and administrative security
 - Authentication security
 - Encryption security
- *Shutting down compromised systems*
 - Manageable security enforcement
 - Sample secure applications e-mail security
 - Internet access security
- *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

- *Website and Internet banking features checklists*
 - Website development and hosting
 - Internet banking package
 - Cash management package
 - Bill pay

- Security
- Options
- *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

- *Establishing the identity of an applicant*
 - Identification documents
 - Information collection
 - Verifying identification information
- *Assisting customers who are victims of identity theft*
 - What to tell to victims of identity theft
 - Using the FTCs affidavit
- *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

- *The computer network*
 - Security of internal networks
 - Security of public networks
- *Electronic capabilities*
 - Examination categories for electronic capabilities
 - (Level 1: information only systems)
 - (Level 2: electronic information transfer systems)
 - (Level 3: fully transactional information systems)
 - electronic payment systems
 - financial institution roles in electronic payment systems
- *Risks*
 - Specific risks to electronic systems
- *Risk management*
 - Strategic planning and feasibility analysis
 - Incidence response and preparedness
 - Internal routines and controls
 - Other considerations