UDC 004.738.5:336.71, DOI: 10.2298/CSIS0901071K

Communicating Information Systems Goals: A Case in Internet Banking Security

Ioannis V. Koskosas

Department of Information and Communication Technologies Enginnering
University of Western Macedonia, KOZANI, GREECE, 50100
ikoskosas@uowm.gr

Abstract: A large part of information systems (IS) security approaches is technical in nature with less consideration on people and organizational issues. The research presented in this paper adopts a broader perspective and presents an understanding of IS security in terms of a social and organizational perspective. In doing so, it uses the communication of risk messages among the members of IT groups in setting Internet banking goals in order to identify any weaknesses in security management procedures. The novel approach of this investigation is that explores and presents the issues of risk communication and goal setting in Internet banking security through in-depth interviews within three case studies. That said, it promotes an interdisciplinary and inter-organizational theory which fosters a new dialog that transcends security industry specific contexts as opposed to other studies. Interview results suggest how an effective setting of Internet banking security goals can be achieved through specific considerations for improving the communication of security messages. The research contributes to interpretive information systems with the study of risk communication and goal setting in an Internet banking security context.

Keywords: Risk communication, goal setting, Internet banking security, intensive research.

1. Introduction

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 [1]. Today, customers demand new levels of convenience and flexibility on top of powerful and easy to use financial management tools, products and services, something that traditional retail banking could not offer.

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. A number of major studies recently conducted in Europe [e.g., 2, 3, 4 and 5] have indicated an increased concern for information systems (IS) security in organizations.

Various approaches have been developed over the years which ensure the minimization of security threats and these are distinguished into four broad categories: checklists, risk analysis, formal methods and soft approaches [6, 7, 8, 9]. Although the value of such approaches to IS security is evident, addressing IS security in terms of ethical and human considerations is also important [10]. Establishing a framework as to how various social and organizational factors may have an effect on IS security in the context of Internet banking is the theme of this paper. Although a range of social and organizational factors are embodied in the value of IS security [11, 12, 13, 14, 15] not previous research focused on Internet banking security in the contexts of risk communication and goal setting.

IS security is viewed as the minimization of risks arising from unauthorised access to and possession of information [16]. In the context of information systems, the asset under consideration are data and the main IS security foundations are the integrity, confidentiality and authenticity of such data [17]. That said, this investigation uses a goal setting approach to IS security and supports the rationale that "security risks may arise due to a failure to obtain some or all of the goals that are relevant to the integrity, confidentiality and authenticity of information through the Internet banking channel".

As Baskerville [18] also noted that the real benefit in IS security is to ensure a "communication link between the security and management professionals" (p. 128), this investigation further asserts that "an efficient communication of risk messages will have an effect on how Internet banking security goals are being set in IT groups". In doing so, a different point of view is being adopted for the analysis of IS security management by exploring and describing factors such as risk communication and goal setting in Internet banking security. The next section describes the research methodology adopted in this investigation. The third section presents a brief IS security background research and the theories of goal setting and risk communication are introduced. The fourth section describes the empirical findings. The fifth section discusses research contribution, and the sixth section includes further research and practice. The last section presents some concluding remarks.

2. An Intensive Research Methodology

A qualitative research methodology having philosophical foundations mainly in interpretivism was deemed more appropriate for this research. Miles and Huberman [19] described qualitative research as simply, research based upon words, rather than numbers. A more generalised, but appropriate definition is that qualitative research is multimethod in focus and involves an interpretive, physical approach to the subject under investigation [20]. This definition implies that qualitative researchers study things in their natural

environment and understand events in terms of the meaning people assign to them; this is the strategy applied to this study. The term *interpretivism* refers to 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; 21].

Interpretivism was particularly useful when the results were being obtained. The respondents were providing their views from their interactions with the rest of the group in which goal setting was in process. For instance, when the respondents were asked questions regarding goals, it was difficult for them to provide a response if they were not involved with the rest of the group.

The next issue under consideration was the research method to be used. Having considered the possible benefits of each available method (e.g., action research, case studies, field studies, application descriptions), it was decided that the advantage offered by a case study- investigating a phenomenon within its real-life context- made this method the most appropriate [22, 23].

However the question arose 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 [22] or for theory testing- when the goal is confirming or refuting theory [24]. When a single case study is used, a phenomenon is investigated in depth, and a rich description and understanding are acquired [25].

Conversely, multiple case studies enable the researcher to relate differences in context to constants in process and outcome [23]. According to Miles and Huberman [19] multiple case studies can enhance generalisability, deeper understanding and explanation. This study 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.

That said, a case study approach has been followed, using the IT departments of three financial institutions in Greece. Since no prior research has studied the relationship of information security goals and risk communication in Greece, the current study represents an innovative and original contribution to the field. It must be mentioned, though, that there were few biases and challenges in gaining access to the IT departments and groups of these institutions, mainly because security is a sensitive and confidential issue for banks' IT employees. However, we came to an agreement through a contract not to mention any data without the authorisation of the IS/IT managers in the three case studies. Moreover, the method of selection could bias the results due to (a) the specific market sector, i.e., financial institutions; (b) the investigation of the case studies in a single country's culture, which may not apply in another country's cultures; and (c) the evaluation of only IT departments.

In order to study and compare the goal setting procedures in different case studies, three financial institutions were chosen based on their IT group

(employee) structure: Alpha-Bank, Delta-Bank, and Omega-Bank[1]. The IT departments consisted of approximately 40 employees at Alpha-Bank, 150 employees at Delta-Bank, and 410 employees at Omega-Bank.

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 [77]. In all cases data was collected through a variety of methods, including interviews, archival records, documents, and observation and visits at the banks over approximately 3 months. The number of people interviewed in each of the three case studies was approximately 15. Each interviewee was conducted approximately 6 to 8 times during the 3-month period. The interviewees ranged from IT managers, deputy managers, and auditors to general IT staff. The interviews were conducted face-to-face, and when necessary, follow-up telephone interviews were scheduled to discuss unclear data.

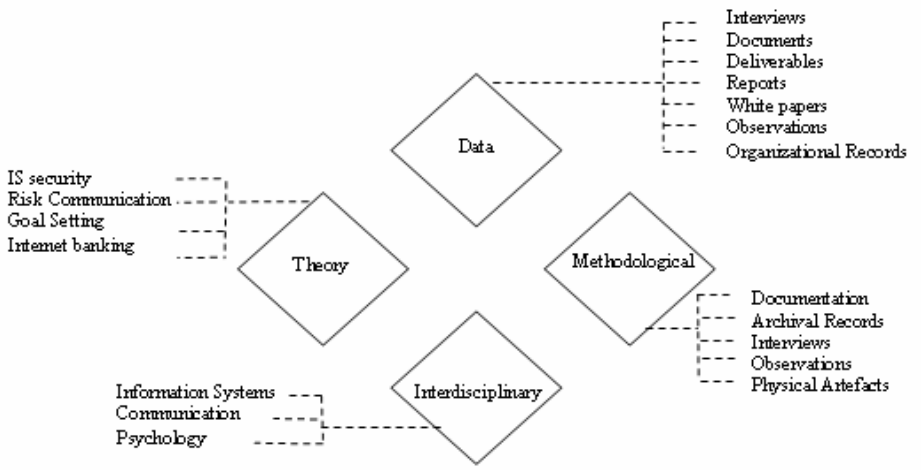

Fig. 1. Diagram 1- Types of triangulation used in the research

The use of multiple data collection methods makes triangulation possible and this provides for stronger substantiation of theory [26]. Triangulation is not a tool or strategy, but rather an alternative to validation [20, 27]. 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 [22]. Five types of triangulation have been identified in the literature [28]: data, investigator, theory, methodological, and interdisciplinary. The present study used data, theory, methodological, and interdisciplinary triangulation as shown in Figure 1.

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

3. Theoretical Background

3.1. IS Security Background on Recent Research Approaches

Although a number of IS security approaches have been developed over the years that reactively minimize security threats such as checklists, risk analysis and evaluation methods, there is a need to establish mechanisms to proactively manage IS security. That said, academics' and practitioners' interest has turned on social and organizational factors that may have an influence on IS security development and management. For example, Orlikowski and Gash [29] 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 [30], in security planning [31] and in identifying the values of internet commerce to customers [32]. Dhillon and Torkzadeh [14] 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 [33, 34, 35] and others in virtual teams [36, 37]. Workman [38] 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.

Albrechtsen [39] found that users considered a user-involving approach to be much more effective for influencing user awareness and behaviour in information security. Similarly, Leach [40] 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 [41] investigated security information management as an outsourced service and suggested augmenting security procedures as a solution, while von Solms and von Solms [42] suggested a model based on the Direct-Control Cycle for improving the quality of policies in information security governance. Jones and Rastogi [43] discussed the importance of gaining improvements from software developers during the software developing phase in order to avoid security implications.

Moreover, Siponen et al. [44] 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. Siponen and Willison [30, 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, the investigation in this paper adopts a case study approach to study Internet banking in the contexts of risk communication and goal setting as no prior research has studied these specific contexts and their interrelationship.

3.2. The Theory of Goal Setting

The theory of goal setting falls within the broad domain of cognitive psychology and is an essential element of social learning theory [45], which has become increasingly influential [46]. The word *goal* encompasses terms such as *intention*, *aim*, *task*, *deadline*, *purpose*, and *objective*, and it is part of the human condition, in the sense that almost all human activities are consciously or unconsciously directed by goals. According to Locke and Latham [47], goals motivate behaviour in at least four ways. First, goals boost behaviour by leading individuals to expend greater effort. Then, goals serve a directive function and maintain the individual focused on the goal. Third, goals lead to persistence in the face of difficulty, and finally, goals lead to exploration, arousal and the development of task-related strategies.

An assertion of goal setting theory is that, given requisite ability and task familiarity, the more difficult and specific the goal, the higher the performance, considering that there is feedback on goal achievement, goal commitment, and task knowledge [47, 48]. Miner [49] reported a peer review that ranked goal setting theory first in importance out of 73 management theories, as rated by organizational behaviour theorists.

Given goal difficulty and specificity, Locke and Latham [48] reported that 90% of the studies show an increase on performance. Rodgers and Hunter [50, 51], using MBO programs, and Pritchard [52], with his productivity, measurement and enhancement (ProMES) system, confirmed that specific goals have a positive impact on performance. Similarly, O' Leary-Kelly et al. [53] found strong effects of assigned group goals on group performance and Crown and Rosse [54] reported that when individual and group goals were congruent, group members were committed to increasing group performance. Shalley and Johnson [55] found that when individual and group goals were incongruent, individuals gave priority to a specific goal over a more ambiguous goal. Koskosas et al. [10] found that organizational group culture improved goal alignment in IS security management. Furthermore, Latham et al. [56] reported evidence that participation in goal setting directly influences self-efficacy, while self-efficacy, in turn, was found to influence performance. Hence, it seems that people with high self-efficacy are likely to seek out and set more challenging goals [57], which means they might also be likely to accept more challenging goals as part of a group task.

Although, early studies in the goal setting literature showed the existence of links between achievement goals and performance as clear and direct, recent work highlighted the need for a reanalysis of these outcomes [58, 59]. Finnegan et al. [60] found that group goal commitment was not related to

group performance, Seijts and Latham [61] found different impacts of goal setting on performance based on group size, and Wegge [62] found moderating effects from participation in goal setting, group cohesion and group conflict. Elliot [59] found that performance-avoidance goals undermined performance regardless of contingencies, whereas performance-approach goals had a positive influence on performance, but not without any contingencies.

Although the goal-performance relationship seems more complex than originally anticipated, additional research findings are added on the portrait which show (a) the importance of learning goals when people need to find strategies for new, complex tasks [61] (b) the relation of goals and goal orientation [63], or (c) the relation of goals and risks [64]. Most of the research reported, however, showed that there is a positive link between goals and performance. Similarly, Dhillon and Torkzadeh [14] 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.

Following these trends, this study follows a macrogoal- level approach and supports the rationale that an efficient goal setting procedure within IT groups may well improve the management of Internet banking security. Consequently, the main research question becomes, “Do IS managers and groups who follow goal-setting procedures set goals relevant to the management of the integrity, confidentiality and authenticity of data through the Internet banking channel?”

3.3. The Theory of Risk Communication

Despite its evolution from the science of risk assessment, risk communication could accurately be described as a subset of communications science. While communication has been described as the ‘management of messages for the purpose of creating meaning’ [65], risk communication then becomes the ‘management of messages about risk for the purpose of creating meaning’.

Although, there are numerous definitions for the term *communication*, this study adopts DeVito’s [66, p.131] definition that covers the essentials of the communication as the act: *communication refers to the act of sending and receiving messages that are distorted by noise, occur within a context, have some effect, and provide some opportunity for feedback*. That actually denotes that even when the goals of communication suggest the need for one-way transfer of information, it is critical to obtain feedback from the recipients in order to ensure that the message has indeed been understood.

Based on literature findings on current theory and practice in risk communication, an issue that appears repeatedly is that of trust and credibility [67, 68, 69, 70]. The relationship between the source of the communication and the recipient must be acknowledged as one important factor, if not the critical factor, in effective communication.

The evolution of practice in risk communication comes from an understanding that communication is more than just the transfer of knowledge. It can only be termed 'communication' if the message has been transferred and understood.

However risk communication is more complicated and difficult as it might appears. In particular, what makes risk communication difficult is not only the exchange of information amongst the parties involved but also amongst the wider institutional and cultural contexts within which risk messages are formulated, transmuted and embedded [71].

The US 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 [72].

Further the success of risk communication is limited due to the insufficient attention it pays to social contexts within which individuals live and communicate [73]. Also it should be considered that the parties sending the messages may not always be honest, reliable as well as responsible [73]. That said, the perception of risk communication to the general public was different to that of the experts. In particular, the difference 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 [74].

Sandman [75] used the term *outrage* to incorporate many of the qualitative dimensions of risks while *hazard* is the quantitative, measurable aspect of risk. He suggested that although the public seemed concerned with *outrage* at the expense of *hazard*, the experts often tend to ignore *outrage* at their own danger. In turn, 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 account.

Risk communication, therefore, 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. This study further supports the rationale that an "efficient communication of risk messages will have an effect on how Internet banking security goals are being set within IT groups".

4. Research Findings

4.1. 4.1 Goal Setting

It was imperative for this research that the IT departments of each organization used should have followed goal setting procedures. Before the interviews commenced, the contacted banks replied positively that goal setting was a consistent part of their overall business strategy. In fact, goal setting was a very important issue, and it was seen as an integral part of the overall risk management process. All the interviewees within Delta and Omega-Bank argued that goals are being set on a regular basis within each banking unit respectively, and that goals represent the identity of the banks' business activities plan. The goals within both organizations, like in the case of Alpha-Bank, are always business oriented and within the technology units the main goals are cost reduction, automation of processes, systems efficiency, and security. Likewise, goals within all of the three organizations come in the form of projects which either originate from top-management to the different banking units or from those units to top-management, in the form of project proposals.

Table 1. The Goal Setting Process in Alpha-Bank

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

The goal setting activities within the three organizations are shown in Tables 1, 2, and 3 respectively. However, it is not in the scope of this research 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.

Table 2. The Goal Setting Process in Delta-Bank

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

Table 3. The Goal Setting Process in Omega-Bank

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

That said, the IT group within Delta-Bank distinguishes the monitoring phase into an independent phase instead of being part of the execution phase, like in the cases of Alpha- and Omega-Banks. Similarly, the first four steps at the goal initiation phase within the organizations were identical although the IT group at Omega-Bank considers the level of security applications in Internet banking and alternative networks as separate levels of security goal activities. The interviewees within Omega-Bank argued that the

additional taxonomy of security levels gives a more clear insight into the different aspects of security especially in Internet banking.

In terms of Internet banking security, Omega-Bank was the only case study among the three to consider the security applications in relation to Internet banking as an additional step at the goal initiation phase. As one IT member said: "*Internet banking security applications consume much of our time and it should be established a co-department, in the future, which will focus only on that aspect of security*". However the three case studies make use of checklists which prioritize Internet banking security risks in terms of their likelihood ratio and impact. An example of such checklist was provided by Alpha-Bank and it is presented in Appendix 1. This checklist, in which new risk factors are identified and their impact to the organization evaluated, consists of five main clusters.

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

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

4.2. Risk Communication in the Context of Goal Setting

Goal setting in the three case studies was an integral part of the organizations' overall business activities plan. From the interviews in Delta Bank, the issue of risk communication was believed to have an effect on the level of goal setting to the degree that one IT member was capable of understanding the goal to be achieved. That is, the capability of each IT member to understand the IT group goals that had to be achieved in the context of Internet banking security, so that the communication of messages with other group members would take place effectively.

However, the differences of the business scope within different banking units had an ultimate effect upon the IT group's Internet banking security activities plan since the business units did not seek always to 'communicate'. One such reason was that since most interactions between users and security mechanisms take place in a socio-technical context with different stakeholders [76], these stakeholders have different goals and views, which sometimes conflict. In effect, some of the IT projects faced difficulties at the project initiation phase, since the IT group had to postpone decisions on

Internet banking security mechanisms to be applied. Such an example includes the upgrade of the system fault tolerance level and the issue of internet vulnerability assessment. The postponement of the internet vulnerability assessment scheme due to different stakeholders' interests caused a 'breach' in the communication of risks between the business units and the IT unit. One IT manager said: "*Most business-units, which are security users as well, are not knowledgeable about security, nor do they want to be. They take care only for themselves without realising that security takes care of them*".

Similar patterns were exhibited in the case of Omega-Bank with the establishment of the Disaster Recovery Planning (DRP) centre, where different stakeholder 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 and they also focus on post-evaluation implementation on security related projects. In effect, the communication of risks was 'broken-down'.

Another problem with communication at Omega-Bank was the employee size structure which did not allow flexibility in decision making, as compared to the case of Alpha-Bank with the small size structure. In addition, the non-participation of some IT employees in security decision making established a misunderstanding with an ultimate effect on the communication of goal messages since the employees felt less motivated to participate in other group activities. As one IT member said: *goal setting is a group effort rather than a process run by a specific number of employees*.

However, most IT members in the three case studies were regularly attending educational and training courses on security issues, especially on the internet evolution, which allowed a better understanding of the Internet banking security issues. In effect, the communication of goal messages with regard to Internet banking security was effective during the goal initiation phase. One IT manager at Alpha-Bank said: "*The link between risk-based decision-making and risk communication must be well understood in order for the security goal setting process to achieve its objectives and for the development of effective Internet banking policy*".

That said, the effective communication of security goals was necessary to maintain an effective level of goal setting with regard to Internet banking security.

5. Discussion

Based on the empirical findings from the three case studies, goal setting was indeed an integral part of their business activities plan. These goal setting procedures were presented in this paper. However different stakeholders had different goals and views, which sometimes conflicted at the expense of Internet banking security as part of the goal setting process. If an Internet banking security task requires significant extra 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 goal setting through misunderstanding in communication at the expense of Internet banking security.

At an organizational level, a success key to effective communication of security risk messages may be the consideration of users' needs and values at the centre of security design. Effective security goal setting has to take into account different stakeholders needs, acknowledge that their needs may sometime conflict and find a solution that is acceptable by all stakeholders. That said, understanding different stakeholders needs can form the basis for risk communication with respect to developing Internet banking security goals, strategies and processes. In the practical application of risk communication, the understanding leads to a clear definition of the appropriate level of security measure with regard to Internet banking security. The challenges of innumeracy, heuristic and other biases add to difficulty of communication about security. Nevertheless, these perspectives need to be recognized in order for communication to be successful and so the goal setting procedure with regard to Internet banking security risks.

However, an effective and successful risk communication and goal setting is not just about giving out information or about making stakeholders understand. Nowadays, successful risk communication can result when the quality of debate and understanding of security issues among all stakeholders is improved. In doing so, the process of goal setting with regard to Internet banking security will also improve.

6. Limitations and Further Research

There are opportunities to undertake further intensive research to identify more critical social and organizational factors and their relation in the context of IS security management. Although an effective risk communication seems to positively influence security goal setting, we cannot be sure as to how an effective communication of Internet banking risks could always lead to goal implementation success. Future research on IS security goal setting, especially research based on case studies, should therefore examine the role of other possible factors at the level of security goal setting in addition to social, organizational considerations. Likewise, another issue interesting to investigate would be the role and type of feedback in goal setting and communication in the context of IS security, e.g., whether the type of feedback (outcome or process feedback) provided affects the risk communication-goal setting 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 developing a theoretical framework of social and

organizational factors which may improve the management of Internet 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 social and 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 [78], this investigation used a collection of various perspectives and an interpretation of how the interviewees react to the opinion expressed by other members.

7. Concluding Remarks

The research described in this paper was concerned with Internet banking security from a social, organizational perspective. Based on a theoretical framework this research supported the rationale that "security risks may arise due to a failure to obtain some or all of the goals that are relevant to the integrity, confidentiality and authenticity of information through the Internet banking channel".

At a very practical level, enhancing cooperation among IT members through employee participation in group goal activities, positive attitudes, professionalism and employees' moral rewards could lead to an effective risk communication, which in turn, would lead to an effective goal setting procedure with regard to Internet banking security management. The findings of this investigation also suggested that integrity, confidentiality and authenticity of data were positioned within the broader business activities plan in the three case studies. At least this is what is evidenced in this investigation. Interviews with respondents suggested that IS security management with regard to Internet banking could be effectively improved if organizations consider more carefully the human factor, which could result to a better understanding in what the organization is trying to achieve on a security level. This is a significant contribution since previous research, while recognizing the importance of the human factor and behaviour, falls short of analysing Internet banking security in the contexts of risk communication and goal setting.

In conclusion, the triangulation methods used including interviews, documents, archival records, observation and physical artefacts, provided useful insights into IS security in the context of Internet banking and allowed the study of risk communication and goal setting within their *real life context*.

8. References

1. Burnham, B.: The Internet's Impact on Retail Banking, Booz-Allen Hamilton Third Quarter, Available: http://www.strategy-business.com/briefs/96301, (current November). (1996)
2. Ernst and Young: Achieving Success in a Globalized World: Is your Way Secure? Global Information Security Survey, Ernst & Young, London. (2006)
3. Quocirca: Security Barometer survey: The Psychology of Security, White paper, May. (2005)
4. DTI: Information Security Breaches Survey, managed by PricewaterhouseCoopers. (2006)
5. Computer Weekly: Security Special Report: The Internal Threat 2006, Technical Report, April, London. (2006)
6. Backhouse, J. and Dhillon, G.: Structures of Responsibility and Security of Information Systems, European Journal of Information Systems, Vol. 5, No., 2-9. (1996)
7. Siponen, M.T.: A Conceptual Foundation for Organizational Information Security Awareness, Information Management and Computer Security, Vol. 8, No. 1, 31-41. (2006)
8. Putnam, L.L.: The Interpretive Perspective: An Alternative to Functionalism. Communication and Organization. L.L. Putnam and M.E. Pacanowsky. Beverly Hills, CA, Sage: 31-54. (1993)
9. 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, 1551-1559. (2007)
10. Koskosas, I.V., Charitoudi, G. and Louta, M.: The Role of Organizational Cultures in Information Systems Security Management: A Goal Setting Perspective, Journal of Leadership Studies, Vol. 2, No. 1., 7-19. (2008)
11. Hirschheim, R., Klein, H.K. and Lyytinen, K.: Information Systems Development and Data Modelling: Conceptual and Philosophical Foundations, Cambridge University Press, UK. (1995)
12. James, H.: Managing Information Systems Security: A Soft Approach, Proceedings of the Information Systems Conference in New Zealand, Editor: Phillip Sallis, October 30-31, Palmerston North, New Zealand. (1996)
13. Andersen, I.T.: Security Barometer survey: The Psychology of Security, Quocirca. (2006)
14. Dhillon, G. and Torkzadeh, G.: Value-focused assessment of Information System Security in Organizations, Information Systems Journal, Vol. 16, No. 3, 293-314. (2006)
15. Koskosas, I.V.: Trust and Risk Communication in Setting Internet Banking Security Goals, Risk Management: An International Journal, Vol. 10, No. 2, 56-75. (2008)
16. Dhillon, G.: Interpreting the Managing of Information Systems Security. Unpublished PhD Thesis, London School of Economics and Political Science, University of London. (1995)
17. Forcht, K. and Wex, R.,: Doing Business on the Internet: Marketing and Security Aspects, Information Management and Computer Security, Vol. 4, No. 4, 3-9. (1996)
18. Baskerville, R.: Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, European Journal of Information Systems, Vol. 1, No. 2, 121-130. (1991)

19. Miles, M.B. and Huberman, A.M.: Qualitative Data Analysis: An Expanded Sourcebook, Sage publications, Newbury Park, CA. (1994)
20. Denzin, N.K.: The Research Act, Third Edition, Prentice-Hall, Eaglewood Cliffs, New Jersey, USA. (1989)
21. Orlikowski, W. and Baroudi, J.J.: Studying Information Technology in Organizations: Research Approaches and Assumptions, Information Systems Research, Vol. 2, No. 1, 1-28. (1991)
22. Yin, R.K.: Case Study Research, Design and Methods, Sage Publications, Newbury Park, CA. (1984)
23. Cavaye, A.L.: Case Study Research: A Multi-Faceted Research Approach for IS, Information Systems Journal, Vol. 6, No. 3, 227-242. (1996)
24. Markus, M.L.: Case Selection in a Disconfirmatory Case Study, In: The Information Systems Research Challenge, Harvard Business School Research Colloquium, Boston: Harvard Business School, pp. 20- 26. (1989)
25. Walsham, G.: Interpretive Case Studies in IS Research: Nature and Method, European Journal of Information Systems, Vol. 4, No. 2, pp.74-81. (1995)
26. Eisenhardt, K. M.: Building Theories from Case Study Research, Academy of Management Review, Vol. 14, No. 4, pp.532-550. (1989)
27. Flick, U.: Triangulation Revisited: Strategy of or Alternative to Validation of Qualitative Data, Journal for the Theory of Social Behaviour, Vol. 22, No. 4, pp. 175-197. (1992)
28. James, H.: Managing Information Systems Security: A Soft Approach, Proceedings of the Information Systems Conference in New Zealand, Editor: Phillip Sallis, October 30-31, Palmerston North, New Zealand. (1996)
29. Orlikowski, W. and Gash, D.: Technological Frames: Making Sense of Information Technology in Organizations, ACM Transactions on Information Systems, Vol. 12, No. 3, 174-207. (1994)
30. Siponen, M. and Willison, R.: A Critical Assessment of IS Security Research between 1990-2000, Proceedings of the 15th European Conference on Information Systems, June 7-9, St. Gallen, Switzerland, 1551-1559. (2007)
31. Straub, D. and Welke, R.: Coping with Systems Risks: Security Planning Models for Management Decision Making, MIS Quarterly, Vol. 22, No. 4, 441- 469. (1998)
32. Keeney, R.L.: The Value of Internet Commerce to the Customer, Management Science, Vol. 45, No. 3, 533-542. (1999)
33. Gefen, D., Karahanna, E. and Straub, D.: Trust and TAM in online Shopping: An Integrated Model, MIS Quarterly, Vol. 27, No. 1, 51-90. (2003)
34. Gefen, D. and Straub, W.: Consumer Trust in B2C e-Commerce and the Importance of Social Presence: Experiments in e-Products and e- Services, Omega, Vol. 32, No. 6, pp. 407-424. (2004)
35. McKnight, D.H., Cummings, L.L. and Chervany, N.L.: Developing and Validating Trust Measures for E-Commerce: An Integrative Typology, Information Systems Research, Vol. 13, No. 3, 334-359. (2002)
36. Ridings, C., Gefen, D. and Arinze, B.: Some Antecedents and Effects of Trust in Virtual Communities, Journal of Strategic Information Systems, Vol. 11, No. 3/4, 271-295. (2002)
37. Sarker, S., Valacich, S.J. and Sarker, S.: Virtual Team Trust: Instrument Development and Validation in an IS Educational Environment, Information Resources Management Journal, Vol. 16, No. 2, pp. 35-55. (2003)
38. Workman, M.: Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security, Vol. 16, No. 6, 315-331. (2007)
39. Albrechtsen, E.: A Qualitative Study of Users' View on Information Security, Computer and Security, 26(4), 276-289. (2007)

40. Leach, J.: Improving User Security Behaviour, Computers and Security, 22(8), 685-692. (2003)
41. Debar, H. and Viinikka, J.: Security Information Management as an Outsourced Service, Computer Security, Vol. 14, No. 5, 416-434. (2006)
42. Von Solms, R. and Von Solms, S.H.: Information Security Governance: A Model based on the Direct-Control Cycle, Computers and Security, Vol. 25, No. 6, 408-412. (2006)
43. Jones, R.L. and Rastogi, A.: Secure Coding: Building Security into the Software Development Life Cycle, Information Systems Security, Vol. 13, No. 5, 29-39. (2004)
44. Siponen, M., Pahnila, S. and Mahmood, A.: 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), 133-144. (2007)
45. Bandura, A.: Self-efficacy: The Exercise of Control, New York, W.H. Freeman Publishing. (1997)
46. Mitchell, T.R., Kenneth, R.T. and George-Falvy, J.: Goal Setting: Theory and Practice, In: Industrial and Organizational Psychology: linking theory with practice, Editors: C.L. Cooper and E.A. Locke, Blackwell Publishers Ltd, First Published 2000. (2000)
47. Locke, E.A. and Latham, G.P.: Building a Practically Useful Theory of Goal Setting and Task Motivation, American Psychologist, Vol. 57, No. 9, 705-717. (2002)
48. Locke, E.A. and Latham, G.P.: A Theory of Goal Setting and Task Performance, Englewood Cliffs, NJ: Prentice-Hall. (1990)
49. Miner, J.B.: The Rated Importance, Scientific Validity, and Practical Usefulness of Organizational Behaviour Theories: A Quantitative Review, AOM Learning and Education, Vol. 2, No. 3, 250-268. (2003)
50. Rodgers, R. and Hunter, J.E.: Impact of Management by Objectives on Organizational Productivity, Journal of Applied Psychology, Vol. 76, No. 22, 322-336. (1991)
51. Rodgers, R. and Hunter, J.E.: Influence of Top Management Commitment on Management Program Success, Journal of Applied Psychology, Vol. 78, No. 11, pp. 151-155. (1992)
52. Pritchard, R.D.: Effects of Group Feedback, Goal Setting and Incentives on Organizational Productivity, Journal of Applied Psychology, Vol. 73, No. 22, 337-358. (1988)
53. O' Leary-Kelly, A.M., Martocchio, J.J., and Frink, D.D.: A Review of the Influence of Group Goals on Group Performance, Academy of Management Journal, Vol. 3, No. 7, 1285-1301. (1994)
54. Crown, D.F. and Rosse, J.G.: Yours, Mine and Ours: Facilitating Group Productivity Through the Integration of Individual and Group Goals, Organizational Behaviour and Human Decision Processes, Vol. 6, No. 4, 138-150. (1995)
55. Shalley, C.E., and Johnson, P.R.: The Dilemma of Dual Goals II: An Investigation of Resource Allocation Between Competing Goals, Presented at the Society for Industrial and Organizational Psychology, San Diego Meetings. (1996)
56. Latham, G.P., Winters, D.C., and Locke, E.A.: Cognitive and Motivational Effects of Participation: A Mediator Study, Journal of Organizational Behaviour, Vol. 15, No. 2, 49-63. (1994)
57. Bandura, A. and Locke, E.A.: Negative Self-Efficacy and Goals Revisited, Journal of Applied Psychology, Vol. 88, No. 1, 87-99. (2003)

58. Harackiewicz, J., Barron, K., Pintrich, P.R., Elliot, A.J. and Thrash, T.M.: Revision of Achievement Goal Theory, Journal Educational Psychology, Vol. 94, No. 5, 638-645. (2002)
59. Elliot, A.J.: A Conceptual History of the Achievement Goal Construct. In Elliot, A. and Dweck, C. (Eds.) Handbook of Competence and Motivation. New York: Guilford Press. (2005)
60. Finnegan, P., Murphy, C., O' Riordan, J.: Challenging the Hierarchical Perspective on Information Systems: Implications from External Information Analysis, Journal of Information Technology, Vol. 14, No. 1, 23-37 (1999)
61. Seijts, G.H. and Latham, G.P.: The Effect of Distal Learning, Outcome, and Proximal Goals on a Moderately Complex Task, Journal of Organizational Behaviour, Vol. 22, No. 4, 291-307. (2001)
62. Wegge, J.: Participation in Group Goal Setting: Some Novel Findings and a Comprehensive Model as a New Ending Ton at Old Story, Applied Psychology: in International Review, Vol. 49, No. 3, 498-516. (2000)
63. VandeWalle, D.M Cron, W.L., and Slocum, J.W.Jr.: The Role of Goal Orientation Following Performance Feedback, Journal of Applied Psychology, Vol. 86, No. 2, 629-640. (2001)
64. Knight, G.: Goal Commitment and the Goal Setting Process: Conceptual Clarification and Empirical Synthesis, Journal of Applied Psychology, Vol. 84, No. 3, 885-896. (1999)
65. Griffin, E.M.: A First Look at Communication Theory, 3rd edition, McGraw Hill. (1997)
66. DeVito, J.A.: Human Communication, The Basic Course, 8th edition, Addison-Wesley Educational Publishers Inc. (2000)
67. Renn, O.: The Role of Risk Communication and Public Dialogue for Improving Risk Management, Risk, Decision and Policy, Vol. 3, No. 1, 5-30. (1998)
68. Metley, D.: Institutional Trust and Confidence: A jOUrney into a Conceptual Quagmire, In: Social Trust and the Management of Risk, G. Cvetkovich and R.E. Lefstedt (eds), London, Earthscan Publications, 100-116. (1999)
69. Johnson, B.B.: Ethical Issues in Risk Communication: Continuing the Discussion, Risk Analysis, Vol. 19, No. 3, 335-348. (1999)
70. Langford, I.H., Marris, C. and O' Riordan, T.: Public Reactions to Risk: Social Structures, Images of Science and the Role of Trust, In: Risk Communication and Public Health, P. Bennett and K. Calman (eds), New York, Oxford University Press, 3-50. (1999)
71. Krimsky, S. and Plough, A.: Environmental Hazards: Communicating Risks as a Social Process, Dover, MA: Auburn House Publishing. (1988)
72. National Research Council: Improving Risk Communication, Report of the Committee on Risk Perception and Communication, Commission on Behavioural and Social Sciences and Education, National Research Council. Washington, D.C.: National Academy Press. (1989)
73. Otway, H. and Wynne, B.: Risk communication: Paradigm and Paradox, Risk Analysis, Vol. 9, No. 2, 141-145. (1989)
74. Groth, E., 1991, Communicating with Consumers About Food Safety and Risk Issues, Food Technology, Vol. 45, No. 5, 248-253. (1991)
75. Sandman, P.: Risk Communication: Facing Public Outrage, EPA Journal, Vol. 13, No. 9, 21-22. (1987)
76. Checkland, P.: Soft Systems Methodology: A 30-year Retrospective, Chishester: John Wiley and Sons. (1999)
77. Benbasat, I., Goldstein, D.K., and Mead, M., 1987, The Case Research Strategy in Studies of Information Systems, MIS Quarterly, Vol. 11, No. 3, 369-386. (1987)

78. Klein, H.K. and Myers, M.D.: A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems, Management of Information Systems Quarterly, Vol. 37, No. 2, 205-236. (1999)

APPENDIX 1: Internet Banking Security Checklist (Alpha-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 versus 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 affidarit
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)
(Level3: 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

Dr. Ioannis Koskosas is a Lecturer in the Department of Information and Communication Technologies Enginnering at the University of Western Macedonia. He specializes in information systems security development and management as well as in digital economics.

Received: August 27, 2008; Accepted: November 10, 2008.