 ISSN:2229-6247

# Management of Information Systems Security Based on a Goal Setting Strategy

Ioannis Koskosas, Konstantinos Pavlitsas, Konstantinos Kakoulidis
Technological Educational Institute of Western Macedonia, KOZANI, 50100, Greece

***ABSTRACT***
*A large part of information systems security approaches is technical in nature with less consideration on people and organizational issues. To this end, there is a need to investigate other means of managing information systems security since most information systems security approaches although valuable they focus on technical oriented solutions, e.g. checklists, risk analysis, evaluation methods, and ignore the social aspects of risks and the informal structures of organizations. This research adopts a psychological-organizational point of view to information systems security by investigating the role and application of goals to informal structured organizations in the banking industry. The ultimate scope of this research is to investigate the importance of having an efficient goal setting structure in the context of information systems security in banking. The research contributes to interpretive information systems with the study of goal setting in a security management context.*

***Keywords****: Information Systems Security, Goal Setting, Organizational Behaviour*

## 1. INTRODUCTION

This research is concerned with information systems (IS) security from a psychological-organizational point of view in the context of 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. Although new technologies, systems and networks provide opportunities for businesses to increase their customer base, reduce transaction costs, and sell their products globally, security implications impede the business (Forcht and Wex, 1996).

While a number of significant, valuable approaches help to minimize and control security risks, most of them ignore the human factor and the informal structure of organizations (Siponen, 2001; Trompeter and Eloff, 2001; Dhillon and Torkzadeh, 2006). To this end, approaching different psychological and organizational issues that may have an effect on information systems security is the theme of this research. Hence, this research is based on the rationale that, since goals are an integral part of management theory, *security risks may arise due to a failure to obtain some or all of the goals that are relevant to the management of data through an organization's information systems*.

To this end, this research adopts a psychological- organizational approach to information systems security in banking by exploring and describing the process of goals setting in the context of IS security management. Following a brief introduction, the next section describes the research methodology adopted in this research. The third section, presents the IS security background research and the theory of goal setting is then introduced. The fourth section, presents the empirical findings and then discusses the research contribution, issues for further research and practice. The last section presents some concluding remarks.

## 2. RESEARCH METHODOLOGY

The first objective of this paper was to investigate if (do) information security managers and groups set goals to manage highly confidential data through the organizations' information systems? Based on this main research question it was further imperative for the research to identify the procedures based on which information security managers and groups set security goals.

To this end, a qualitative research methodology having philosophical foundations, mainly in interpretivism, was deemed more appropriate, than the quantitative or scientific approach, for this research. Miles and Huberman (1994) 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 (Denzin & Lincoln, 1998). This definition implies that qualitative researchers study things in their physical environment and understand events in terms of the meaning people assign to them; this is the strategy applied to this research. 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; Orlikowski & 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 goals, it was difficult for them to provide a response without having been 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 (Yin, 1994; Cavaye, 1996).

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 (Yin, 1994) or for theory testing by confirming or refuting theory (Markus, 1989). When a single case study is used, a phenomenon is investigated in depth, and a rich description and understanding are acquired (Walsham, 1995).

Conversely, multiple case studies enable the researcher to relate differences in context to constants in process and outcome (Cavaye, 1996). According to Miles and Huberman (1994) multiple case studies can enhance generalisability, deeper understanding, and explanation. This research further asserts that although studying multiple cases may not provide the same rich descriptions as do studies of single cases, multiple cases enable the analysis of data across cases.

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 and goals and 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 information security/IT managers in the three case studies. Moreover, the method of selection could bias the results due to (a) the specific market sector, that is, 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 (employees) 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 (Benbasat et al., 1987). 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.

The use of multiple data collection methods makes triangulation possible and this provides for stronger substantiation of theory (Eisenhardt, 1989). Triangulation is not a tool or strategy, but rather an alternative to validation (Denzin, 1989; Flick, 1992). Thus, any finding or conclusion made from the cases is likely to be more convincing and accurate if it is based on several different sources of information (Yin, 1994). Five types of triangulation have been identified in the literature (Janesick, 2000): data, investigator, theory, methodological, and interdisciplinary. The present study used data, theory, methodological, and interdisciplinary triangulation.

## 3. THEORETICAL BACKGROUND

### 3.1 Information Security Background

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

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

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

A number of studies investigated inter-organizational trust in a technical context. Some of them have studied the impacts of trust in an e-commerce context (Gefen et al., 2003; Gefen and Straub, 2004; McKnight et al., 2002) and others in virtual teams (Ridings et al., 2002; Sarker et al., 2003). Workman (2007) studied trust as a factor in social engineering threat success and found that people who were trusting were more likely to fall victims to social engineering than those who were distrusting.

Albrechtsen (2006) found that users considered a user-involving approach to be much more effective for influencing user awareness and behaviour in information security. Similarly, Leach (2003) studied influences that affect a user's security behaviour and suggested that by strengthening security culture organizations may have significant security gains. Debar and Viinikka (2006) investigated security information management as an outsourced service and suggested augmenting security procedures as a solution, while von Solms and von Solms (2004) suggested a model based on the Direct-Control Cycle for improving the quality of policies in information security governance. Jones and Rastogi (2004) discussed the importance of gaining improvements from software developers during the software developing phase in order to avoid security implications.

Moreover, Siponen et al. (2007) advanced a new model that explains employees' adherence to IS policies and found that threat appraisal, self-efficacy and response efficacy have an important effect on intention to comply with information security policies. Siponen and Willison (2007, p. 1551) also reviewed 1043 papers of the IS security literature for the period 1990-2004 and found that almost 1000 of the papers were categorized as 'subjective-argumentative' in terms of methodology with field experiments, surveys, case studies and action research accounting for less than 10% of all the papers. That said, this research adopts a case study approach to study goal setting in information systems security since no prior research has studied these specific contexts and their interrelationship in the banking industry.

### 3.2 The Goal Setting Theory

The theory of goal setting falls within the broad domain of cognitive psychology and its literature is an essential element of social learning theory (Bandura, 1997), which has become increasingly influential (Mitchell et al., 2000). A 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 (2002), 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 (Locke & Latham, 1990, 2002). Miner (2003) 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 (1990) reported that 90% of the studies show an increase on performance. Rodgers and Hunter (1991, 1994), using MBO programs, and Pritchard (1995), with his PROMES system, confirmed that specific goals have a positive impact on performance. Similarly, O' Leary-Kelly et al. (1994) found strong effects of assigned group goals on group performance and Crown and Rosse (1995) reported that when individual and group goals were congruent, group members were committed to increasing group performance. Shalley and Johnson (1996) found that when individual and group goals were incongruent, individuals gave priority to a specific goal over a more ambiguous goal. Koskosas et al. (2008) found an important relationship of organizational group culture and goal setting in information security management, while Koskosas (2008) found evidence that, high levels of trust among IT security group members, in terms that one member is capable of delivering, led

to clarity to goal achievement. Furthermore, Latham et al. (1994) reported evidence that participation in goal setting directly influences self-efficacy, whereas 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 (Bandura and Locke, 2003), which means they might also be likely to accept more challenging goals as part of a group task.

Although, early studies of 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 (e.g., Harackiewicz et al., 2002; Elliot, 2005). Finnegan et al. (1999) found that group goal commitment was not related to group performance, Seijts and Latham (2000) found different impacts of goal setting on performance based on group size, and Wegge (2000) found moderating effects from participation in goal setting, group cohesion and group conflict. Elliot (2005) 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 the importance of learning goals when people need to find strategies for new complex tasks (Seijts & Latham, 2001), the relation of goals and goal orientation (Vande-Walle et al., 2001), or the relation of goals and risks (Knight et al., 2001). Most of the research reported however showed that there is a positive link between goals and performance. Similarly, Dhillon and Torkzadeh (2006) 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 research follows a macro-goal level approach and supports the rationale that an efficient goal setting procedure may well improve the management process of information security. Consequently, the main research question becomes, “Do information managers and groups who follow goal setting procedures set goals relevant to the management of data through an organization’s information systems?

## 4. RESEARCH FINDINGS

### 4.1 Goal Setting

It was imperative for this research that any organizations used as a case study should have followed goal setting procedures, particularly in the banks’ security/IT departments. 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. 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.

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.

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 whereas Delta-Bank and Omega-Bank did not. At Alpha-Bank this stage is considered as reactive because 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, but at Alpha-Bank the IT group members argued that although feedback is achieved at the evaluation phase, some of the goal activities planned may be ‘jeopardised’ before that phase. Thus, the control of goal setting activities planned is a ‘premature’ stage, which provides though more valuable information at the time needed.

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

| ***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 |

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.

However evidence from the three case studies showed the existence of political agendas that ultimately affected the goal setting process. In the case of Omega-Bank the establishment of the Disaster Recovery Planning (DRP) centre, established problems due to different stakeholders' interests that 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. During the interviews with the organizations, there was an argument that goal setting was not always efficient due to such political agendas because different banking units were competing with each other for the greater share of funds and often in disregard of the IT units. As one IT employee said: *Goal setting should be a group effort rather than a process run by different stakeholders' interests*.

At Delta-Bank, there were similar patterns of political agendas that drove backwards the goal setting activities plan of the IT group. An example was the investment of approximately €1 million for security risk surveillance purposes e.g., a new firewall software architecture, new intrusion detection systems and other investments in hardware including physical security, where even though the funding was agreed the decision was interrupted several times before. An IT employee said: *"Banks try to invest in new ways where the investment is directly returned while with security the return is most of the time indirect. This makes it for IT units more difficult to convince top management for project funding"*. From the interviews, though, it was argued that effective goal setting is not just about making stakeholders understand but rather improving the quality of debate and understanding of security issues among all stakeholders. To this end, the process of setting security goals will also improve.

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 including IT security projects. The procedures according to which the IT groups within the three organizations respectively set goals, in the context of security risk management, exhibit similar patterns, albeit with a few minor differences in the implementation process, in terms of stage prioritisation.

## 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 banking security as part of the goal setting process. If an information systems 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 management 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 security goals, strategies and processes. In the practical application of goal setting, the understanding leads to a clear definition of the appropriate level of security measure with regard to 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 management to be successful and so the goal setting procedure with regard to security risks.

However, an effective and successful goal setting is not just about giving out information or about making stakeholders understand. Nowadays, successful goal setting 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 information security, will also improve.

### 5.1 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 information security management. Although an effective goal setting seems to positively influence security management, we cannot be sure as to how an effective goals setting procedure could always lead to security implementation success. Future research on information 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 information security, e.g., whether the type of feedback (outcome or process feedback) provided affects the communication goals 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 research an attempt was made to address this issue by developing a theoretical framework of social and organizational factors which may improve the management of information security. Although, qualitative research does not offer the pretence of replication since controlling the research will destroy the interaction of variables, this research was conducted in a structured methodology guided by the specific 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, this research used a collection of various perspectives and an interpretation of how the interviewees react to the opinion expressed by other members.

## 6. CONCLUDING REMARKS

The research described in this paper was concerned with information security from a social, organizational point of view. 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 management of data through an organization's information systems*.

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 communication among the groups that would, in turn, lead to an effective goal setting procedure with regard to information security. The findings of this research also suggested that data management were positioned within the broader business activities plan in the three case studies. At least, this is what is evidenced from this research. Interviews with respondents suggested that information security management 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 information security in the context of goal setting.

Past research showed that information security can be more efficiently managed if there is more investigation beyond the technical means of protecting information resources. The research described in this paper was concerned with information system security from a social, organizational perspective. Thus, the findings of this research may be used to some extent to explore security organizational practices in real life.

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

## REFERENCES

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

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

Backhouse, J. and Dhillon, G. (1996) Structures of Responsibility and Security of Information Systems, *European Journal of Information Systems*, 5(1), pp.2-9.

Bandura, A. (1997) *Self-efficacy: The Exercise of Control*, New York, W.H. Freeman Publishing.

Bandura, A. and Locke, E.A. (2003) Negative Self-Efficacy and Goals Revisited, Journal of Applied Psychology, 88(1), pp. 87-99.

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

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

Crown, D.F. and Rosse, J.G. (1995) Yours, Mine and Ours: Facilitating Group Productivity Through the Integration of Individual and Group Goals,
Organizational Behaviour and Human Decision Processes, 6(4), pp. 138-150. Debar, H. and Viinikka, J. (2006) Security Information Management as an Outsourced Service, *Computer Security*, 14(5), pp. 416-434.

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

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

Dhillon, G. and Torkzadeh, G. (2006) Value-focused assessment of information System Security in Organizations, *Information Systems Journal*, 16(3), pp. 293-
314.

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

Elliot, A.J., (2005) A Conceptual History of the Achievement Goal Construct. In Elliot, A. and Dweck, C. (Eds.) *Handbook of Competence and Motivation*. New
York: Guilford Press.

Ernst and Young (2006), Achieving Success in a Globalized World: Is your Way Secure? *Global Information Security Survey*, Ernst & Young, London.

Finnegan, P., Murphy, C., O' Riordan, J. (1999) Challenging the Hierarchical Perspective on Information Systems: Implications from External Information Analysis, *Journal of Information Technology*, 14(1), pp.23-37.

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

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

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

Harackiewicz, J., Barron, K., Pintrich, P.R., Elliot, A.J. and Thrash, T.M. (2002) Revision of Achievement Goal Theory, Journal Educational Psychology, 94(5), pp. 638-645.

Herriot, R. E., and Firestone, W. A. (1983). Multisite Qualitative Policy Research: Optimizing Description and Generalizability, *Educational Researcher*, 12(3), pp14-19.

Hirschheim, R., Klein, H.K. and Lyytinen, K. (1995) *Information Systems Development and Data Modelling: Conceptual and Philosophical Foundations* Cambridge University Press, UK.

James, H. (1996) Managing Information Systems Security: A Soft Approach, *Proceedings of the Information Systems Conference in New Zealand*, Editor Phillip Sallis, October 30-31, Palmerston North, New Zealand.

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

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

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

Knight, D., Durham, C.C. and Locke, E.A. (2001) The Relationship of Team Goals Incentives, and Efficacy to Strategic Risk, Tactical Implementation and Performance, *Academy of Management Review*, 44(2), pp. 326-338.

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

Koskosas, I.V., Charitoudi, G. and Louta, M. (2008) The Role of Culture to Information Systems Security Management: A Goal Setting Perspective, *Journal of Leadership Studies*, **2**(1), pp. 7-36.

Latham, G.P., Winters, D.C., and Locke, E.A. (1994) Cognitive and Motivational Effects of Participation: A Mediator Study, *Journal of Organizational Behaviour*, 15(2), pp. 49-63.

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

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

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

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

Miles, M.B. and Huberman, A.M. (1994) *Qualitative Data Analysis: An Expanded Sourcebook*, Sage publications, Newbury Park, CA.

Miner, J.B. (2003) The Rated Importance, Scientific Validity, and Practical Usefulness of Organizational Behaviour Theories: A Quantitative Review, AOM Learning and Education, 2(3), pp. 250-268.

Mitchell, T.R., Kenneth, R.T. and George-Falvy, J. (2000) Goal Setting: Theory and Practice, In: *Industrial and Organizational Psychology: linking theory with practice*, Editors: C.L. Cooper and E.A. Locke, Blackwell Publishers Ltd, First Published 2000.

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

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

O' Leary-Kelly, A.M., Martocchio, J.J., and Frink, D.D. (1994) A Review of the Influence of Group Goals on Group Performance, *Academy of Management Journal*, 3(7), pp. 1285-1301.

Pritchard, R.D. (1995) *Productivity measurement and improvement: Organizational case studies*, New York: Praeger.Ridings, C., Gefen, D. and Arinze, B. (2002) Some Antecedents and Effects of Trust in Virtual Communities, *Journal of Strategic Information Systems*, 11(3/4), pp. 271-295.

Rodgers, R. and Hunter, J.E. (1991) Impact on Management by Objectives on Organizational Productivity (monograph), *Journal of Applied Psychology*, 76(2), pp.322-336.

Rodgers, R. and Hunter, J.E. (1994) The Discard of Study Evidence by Literature Reviewers, *Journal of Applied Behavioural Science*, 30(2), pp. 329-345.

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

Seijts, G.H. and Latham, G.P. (2000) The Construct of Goal Commitment: Measurement and Relationships with Task Performance, In: *Problems and Solutions in Human Assessment: Honoring Douglas N. Jackson at seventy,* R. Goffin and E. Helmes (eds.), (pp. 315-332), Dordrecht, The Netherlands: Kluwer Academic Publishers.

Shalley, C.E., and Johnson, P.R. (1996) *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.Simpson, B. and Wilson, M. (1999) Shared Cognition: Mapping Commonality and Individuality, *Advances in Qualitative Organizational Research*, 2(1), pp. 73-96.

Siponen, M.T. (2001) An Analysis of the Recent IS Security Development Approaches: Descriptive and Prescriptive Implications, In: *Information Security Management: Global Challenges in the New Millenium*, Dhillon, G. (eds.), Idea Group Publishing, Hershey.

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

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

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

Tushman, M.L., and O' Reilly, C.A. III (1997) *Winning through Innovation*, Boston: Harvard School Press.

VandeWalle, D.M Cron, W.L., and Slocum, J.W.Jr. (2001) The Role of Goal Orientation Following Performance Feedback, *Journal of Applied Psychology*, 86(2), pp. 629-640.

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

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

Wegge, J. (2000) Participation in Group Goal Setting: Some Novel Findings and a Comprehensive Model as a New Ending Ton at Old Story, *Applied Psychology: in International Review*, 49(3), pp. 498-516.

Weingart, L.R. (1992) Impact of Group Goals, Task Component Complexity, Effort and Planning on Group Performance, *Journal of Applied Psychology*, **77**(5), pp 682-693.

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

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