A Model Performance to Information Security Management

Ioannis Koskosas[1], Konstantinos Kakoulidis[1], Christos Siomos[2]
[1]Technological Educational Institute of Western Macedonia,
Department of Finance
[2]SY.F.FA.S.DY.M (Pharmaceuticals of Western Macedonia)
KOZANI, 50100, Greece

Abstract

The investigation in this paper takes a social and organizational approach to information systems security management and proposes a framework which illustrates three important issues in the process of security management through goal setting, these are: trust, culture, and risk communication. Three case studies show evidence that there is a chain reaction among these issues with a subsequent effect on the level of security goal setting. Ultimately, the paper identifies the determinants of trust within the IT departments of three financial institutions in Greece and provides also a discussion regarding the research methods that were used to obtain the results.

Keywords: Trust, culture, risk communication, security management, goal setting.

1. Introduction

The research described in this paper is concerned with Information Systems (IS) security. A number of major studies on information security conducted in Europe, among these being the Ernst and Young 2006 survey, the Andersen 2006 survey, and the DTI report 2006, indicate a general upward trend in the number of security incidents in organizations. These studies further suggest that organizations expressed less confidence about future security issues, noting that security incidents are increasing both in terms of number and complexity. Over the years a number of security approaches have been developed that help in managing IS security and in limiting chances of an IS security breach. The various approaches fall into three broad categories: checklists (e.g., SAFE and AFIPS checklists), risk analysis (e.g., CRAMM, MARION, and RISKPAC), and evaluation methods (e.g., TCSEC, ITSEC, BS7799). Since annual security related incidents are on increase, current means for managing IS security have been unable to fulfill the promise. The application of risk management approaches, seems inadequate in managing IS security risks and overall, the IT groups' performance in managing risks, remains limited. As also Dhillon and Backhouse (2001) point out, most IS security approaches tend to offer narrow, technically oriented solutions, while ignore the social aspects of risks and the informal structures of organizations (see the arguments proposed by Baskerville, 1991; Willcocks and Margetts, 1994; Straub and Welke, 1998). To this end, managing IS security needs to adopt a socio-organizational point of view.

Following these trends the investigation in this paper adopts a social and organizational point of view to the management of information systems security and suggests a framework which is mainly based on the concept of goals. The aim of the framework is to improve the performance of an IT group in managing systems' security and to this end, it illustrates three important issues in the process of security goal setting, which are: trust, culture, and risk communication. Evidence from three case studies, show a positive chain reaction among these issues with a subsequent effect on the level of security goal setting. Specifically, it has been shown that trust among the members of an IT group and towards the upper levels of management, provides the conditions under which culture and risk communication are likely to occur through positive attitudes, higher levels of cooperation and coordination of activities and satisfaction towards senior management. The ultimately scope of this investigation is also to identify the determinants of trust as it would allow both theorists and practitioners to understand reasons of conflict to goal setting. In the following, section 2 discusses the research methods used to collect the data for analysis. Section 3, explains the rationale behind the framework and presents the findings of the case studies. Section 4 ends with some conclusions and suggestions for further research.

2. Research Approach

The objectives of this paper were to investigate:

- if IT managers set in particular, security goals in relation to the integrity, confidentiality and availability of information through electronic banking systems
- the relationship among trust, culture and risk communication at the level of information systems security goal setting

- the determinants of trust among individuals within an IT group in setting information systems security goals

At the level of macro goal setting, researchers' interest has been in strategic management and organizational theory whose focus is on the organization as a whole (Locke and Latham, 1990). Due to the difficulty of using controlled experimental designs, they have used correlational and observational methods and both quantitative and qualitative approaches have been employed. In this investigation, a qualitative research approach having philosophical foundations, mainly in interpretivism, was deemed the most appropriate. Miles and Huberman (1994) describe qualitative research as simply, research based upon words, rather than numbers. A more generalised, but appropriate definition is: "Qualitative research is multimethod in focus, involving an interpretive, naturalistic approach to its subject matter" (Denzin and Lincoln, 1998). This definition implies that qualitative researchers study things in their natural environment and understand events in terms of the meaning people assign to them and this is the strategy applied to this investigation. The term 'interpretivism' is defined as "Studies that assume that people create and associate their own subjective and intersubjective meanings (inductive process) as they interact (processual) with the world around them (contextual) (Orlikowski and Baroudi, 1991).

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 commitment, it was difficult for them to provide a response without having been involved with the rest of the group. Similar situations arose in the instance of trust, culture, and risk communication. The next issue under consideration was the research method to be used. Having considered the possible benefits of each available method e.g. action research, case studies, field studies, application descriptions, it was decided that the advantages offered by case studies were deemed more appropriate to this research. Cavaye (1996) and Yin (1984) cite a benefit of a case study as 'an investigation of a phenomenon within its real life context'. However the question was whether to employ single case studies or multiple case studies. Theorists support the view that a single case study should be employed, particularly when exploring a previously unresearched subject (Yin, 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).

In the opposite, multiple case studies enable the researcher to relate differences in context to constants in process and outcome (Cavaye, 1996). According to Miles and Huberman (1994) multiple case studies can enhance generalisability, deeper understanding and explanation. Herriot and Firestone (1983) point out that the evidence from multiple case studies is often considered more convincing, with the overall study being considered more robust. This investigation further asserts that although studying multiple cases may not provide the same rich descriptions as do studies of single cases, multiple cases enable the analysis of data across cases. To this end, a case study approach has been followed within the IT departments of three financial institutions in Greece due to the investigators' availability of access. The institutions ranged from small (Alpha-Bank)[1] to medium (Delta-Bank) to large (Omega-Bank) financial institutions accordingly, based on their financial assets. The reason for choosing these institutions (banks) according to their assets is to investigate if the suggested framework applies to different IT group structures. For example, the IT department of Alpha-Bank consisted of approximately 40 employees, while in Delta-Bank 150 employees, and in Omega-Bank 410 employees, respectively.

The research focuses in the area of banking because the banking industry is among the first to use innovative technologies and as information is highly leveraged, risk manipulation and dissemination is one of the main concerns of IT managers (Jacoby, 1995). However another issue to be resolved with the research approach used here concerns data collection. The design of this investigation employed multiple data collection methods as it is important in case research studies (Benbasat et al., 1987). In all cases data was collected through a variety of methods including interviews, documents, and observation and visits to the banks lasted for approximately three months. The total number of interviews within each of the three case studies, numbered to fifteen. The interviewees ranged from senior managers, IT managers, deputy managers, and IT staff people. The interviews were face-to-face and when necessary telephone interviews followed up to confirm something about the data that was unclear. In most cases, the conversations were tape-recorded. Tape recordings were used as they offer benefits that are not available with such other forms as the note taking of data collection.

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

Further, the use of multiple data collection methods makes triangulation possible and this provides stronger substantiation of theory (Eisenhardt, 1989). Triangulation is not a tool or strategy, but rather an alternative to validation (Denzin, 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 triangulation and Interdisciplinary. The present research used data triangulation, theory, methodological, and interdisciplinary. Having discussed the research methods, the next section presents the rationale behind the framework as well as the research findings.

3. The Framework

3.1 Goal Setting

Goal is a generic concept that encompasses the essential meaning of terms such as intention, task, deadline, purpose, aim, end, and objective (Locke and Latham, 1990). It is widely acknowledged that goals play a significant role in regulating human action at both the micro and macro levels. At the micro level, goals affect action by directing attention and effort, prolonging effort over time, and motivating people to develop relevant task strategies (Locke and Latham, 1990). Goals serve also as a benchmark against which performance feedback can be evaluated (Locke and Latham, 1984). These functions have also a parallel effect at the macro level. It has been asserted that goals serve a unifying function by mobilising and directing organization members' efforts toward a common task (Bradford and Cohen, 1984; Locke and Latham, 1990). It is also claimed that an organization's goals direct its planning process, influencing both its mission and its strategy (Pearce and David, 1987) and that such goals serve as a standard by which to measure success (Locke and Latham, 1990).

Evidence from the case studies shows, that goal setting is a significant process at the stage of risk planning in the risk management process. A goal in all cases was taken into consideration in terms of an IS project. All banks were following goal setting procedures based on manuals and it was believed that goals define the nature and purpose not only of an IT group but of the whole organization (Parsons, 1960). The goals in the three banking institutions were always business goals, which then were subdivided into each banking division in order to implement. It has been found that goals in IT departments are business-oriented and have an impact on security planning and implementation. As the IT manager at Alpha-Bank said:

"It is quite often that IT people do not understand that we work for the benefit of the bank which is translated in profits and only profits. Behind any project undertaken by IT groups within banking units, the main goal is reduction of costs, process automation, service improvement. So, there is not question of getting the best software but rather the most economical one".

It has been argued that goal setting should not be regarded as an 'add-on' to risk management, but as a central and integral part of the risk management process: whereas the goal of achieving acceptable risk exposure is also part of overall process aims. However goal setting within the IT departments of the three banks is equally divided into three phases, each containing several steps. These phases are shown in Table 1, below.

1st Phase: ***Project initiation phase***

Step 1: Selection of members for the project team
Step 2: Explanation of the method to the members of the team and planning of the 'security risk activities'.
Step 3: Physical security (external)
Step 4: Control of users' activities into networks
Step 5: Systems security (internal)

2nd Phase: ***Execution phase***

Step 1: Identification of risks
Step 2: Pre-selection of identified risks
Step 3: Final risk identification and selection via a joint security project management group meeting
Step 4: Control and Security
Step 5: Risk monitoring

3rd Phase: ***Evaluation phase***

Last Step: Compiling a security management evaluation report

Table 1 The Goal Setting Process

Broadly speaking, these goal setting steps apply to all of the three banking institutions with a few differences though in the evaluation and implementation process.

For example, Omega-Bank which is the largest institution among the three, established the department of disaster recovery planning (and post-evaluation) for possible future security incidents while Alpha- and Delta-Bank were still in process. Similarly, software applications for Omega-Bank were mainly developed in-house (through a subsidiary company), Delta-Bank was semi-outsourcing and Alpha-Bank outsourcing. Further, it has been found that different stakeholder interests have a significant impact at the level of goal setting and sometimes to a great extent. As the IT manager at Omega-Bank said: *"There are some times that we choose software solutions from companies whose product specifications are not satisfied but we do so on the basis of long-term bank's customer relationships"*. The above quote means goal setting within the IT group at Omega-Bank was affected to a certain degree by customer relationships, something that was also familiar with Alpha- and Delta-Bank. In addition, the different stakeholder interests had an impact on group commitment too.However, in Figure 1 below, the theoretical framework shows that at the level of security goal setting the issues of trust, culture, and risk communication play a significant role.

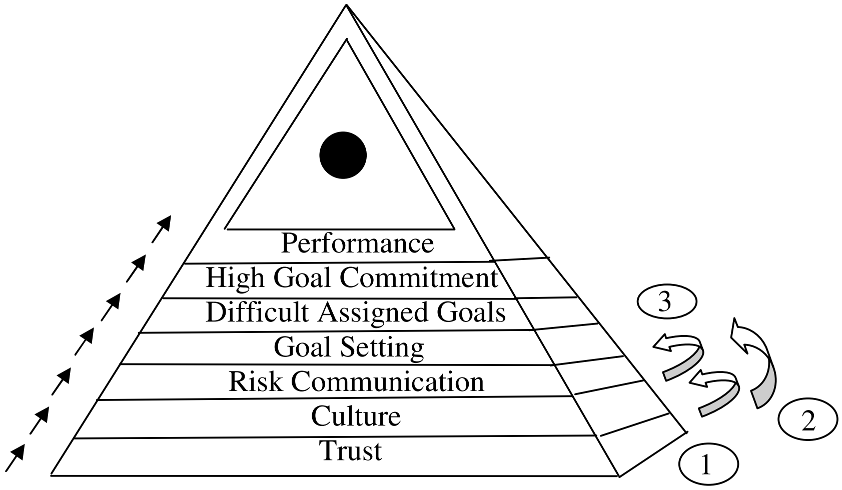

Figure 1 *Performance Pyramid Framework*

3.2 Trust

At the bottom of the pyramid lies the level of trust. Many studies argue that trust determines the performance of a society's institutions and it is a propensity of people in a society to co-operate to produce socially efficient outcomes (Coleman, 1990; Gambetta, 1998). Similarly, Rousseau et al., (1998) observed that several theorists focused on interpersonal trust in work relationships have positioned trust as a moderator. Dirks (1999) for example, found that trust did moderate the relationship between group members' motivation and group processes and outcomes. Specifically, groups with high levels of motivation tended to direct their effort toward group goals in the high trust condition, although they directed their effort toward individual goals, in the low trust condition. This investigation supports that trust has a dual effect: first, that trust among the members of an IT group will provide the conditions under which a strong culture and an effective communication of risks are likely to occur; and second, that trust plays an important role when IT groups set security goals.As trust may consist of different dimensions, asking directly about trust seemed most appropriate because it was felt that the respondents would not provide the required answers, and the question could be misinterpreted. This is also because issues connected to individual or organizational behaviour, are highly emotional, and any incorrect type of questioning could be misinterpreted.

In all cases, trust was found to be of vital importance among the members of an IT group at the process of security goal setting. However from the case studies, it is shown that issues of trust at Delta- and Omega-Bank accordingly, are of minority importance at the level of security goal setting. This is because the procedures according to which IT employees co-operate and co-ordinate their activities, are based on bureaucratic criteria which do not allow individual intellect. Evidence also shows that not all IT employees participate in decision making with regards to security issues and in effect, there was a distrust of motives, attitudes and beliefs of few employees towards top-management. However the main reason for employees' non-participation was that top-management within Delta- and Omega-Bank believed that the less people involved in security issues the more secure were the security procedures.However the case at Alpha-Bank was different as the IT group was more family-oriented, in the sense that employees were working together for years, had social relationships outside the work environment and the majority of them were participating in decision making. Trust though was recognized as an important issue within IT groups, in all cases under study, and particularly at the phase of execution, depicted in Table 1. For example, it was argued that risk monitoring requires loyal and committed people.

However evidence shows that trust is part of an IT group's culture and provides the conditions under which a strong culture is likely to occur through:

- Positive attitudes among co-members
- Higher levels of co-operation
- Satisfaction of IT members through high levels of trust to the IT manager

3.2 Culture

Culture is at the next level of the performance pyramid. In this investigation, the definition of culture is based on Reilly and Chatman's (1996) definition as *'a system of shared values (which define what is important) and norms that define appropriate attitudes and behaviours for organizational members'*. Much of behavioural theories focus on the hypothesis that strong cultures enhance organization performance (Deal and Kennedy, 1982; Kotter and Heskett, 1992). This hypothesis is based on the idea that organizations benefit from having highly motivated employees dedicated to common goals. It is also believed that the performance benefits of a strong corporate culture are thought to derive from three consequences of having widely shared and strongly held norms and values: enhanced coordination and control within the organization, improved goal alignment between the organization and its members, and increased employee effort (Sorensen, 2002). A culture can be considered strong if those norms and values are widely shared and intensely held throughout the organization (Kotter and Heskett, 1992; O'Really and Chatman, 1996).

Similarly, when employees understand their culture they actually understand the organization's goals and co-ordination becomes easier, as they are likely to take actions towards common goals among them and with other parts of the organization (Cremer, 1993). This investigation subscribes to this notion by supporting that culture plays a significant role at the level of security goal setting and further asserts that culture will provide the conditions under which an effective communication of risks is likely to occur.Each banking institution had its own sub-culture that sets values, attitudes and beliefs shared by a group of people that guide and influence their behaviours and reactions to various stimuli. The culture at Delta- and Omega-Bank respectively, was generally defined by many members within the IT departments as:

"A process driven and controls oriented culture with delivering superior customer processors rather than delivering substantial growth".

The findings also showed that the banks' culture did not allow much room for individual contributions. Policies and procedures should run the banks, not necessarily the people. This, however, was limiting people's creativity as they felt their ideas were limited by bureaucratic procedures with an effect to abandon their efforts. For example, some IT employees were asked the question: *Do you think sometimes your creativity pushes you to work over-time?* The answer was: *if I am paid*. However the case at Alpha-Bank was different as IT employees were strongly believing and sharing the company's norms and values. Members of the IT group were constantly attending educational seminars and had more freedom of individual intellect. Culture at Alpha-Bank seemed more family-oriented and IT employees felt they were contributing to the institution as a whole. Findings show that a strong culture at Alpha-Bank is likely to occur through high levels of trust among the members of the IT group as the levels of cooperation and coordination of activities become higher while at Delta- and Omega-Bank due to the bureaucratic criteria, trust had a less significant role and thus, the culture was less consistent with the overall goals and objectives of the institutions.

3.4 Risk Communication

At the third level is the communication of security risks among the members of an IT group. Although there are numerous definitions for the term 'communication', this investigation adopts DeVito's (1988) definition that covers the essentials of the communication as the act:

'communication refers to the act, by one or more persons, of sending and receiving messages that are distorted by noise, occur within a context, have some effect, and provide some opportunity for feedback'.

However effective communication of risks is a difficult task. What makes risk communication difficult is not only the exchange of information amongst the involved parties, but also amongst the wider institutional and cultural contexts within which risk messages are formulated, transmuted and embedded (Krimsky and Plough, 1988). Based on interviews it has been shown that one of the most important barriers to communication of risks is mistrust between the IT manager and the IT group members. Distrust of the motives, attitudes and beliefs of the 'other side' makes it difficult to listen to, let alone to accept and respond respectfully to, what one's opposite party is trying to communicate. That was quite often the case at Delta- and Omega-Bank. The communication problem was also based on the fact that different departments were in a different geographical location with each other and in effect, the communication was mainly taking place either through telephone or e-mails. This way of communication proved to be ineffective quite often as one IT employee from Omega-Bank stated:

"Sometimes more e-mails are generated than necessary. In addition, there is a mix between e-mail, telephone, tele-conferencing and face-to-face communication; coming up with the right mix is very difficult. If you have the wrong mix, you can waste a lot of time, not get the job done. I don't know what is the right mix". Further, organizational cultures codify the organization's understanding of itself and its environment and thus, clarify the organization's beliefs and goals for members (Schein, 1992). Evidence shows that at Alpha-Bank the strong culture within the IT group makes people to understand what the group is trying to achieve and therefore, the co-ordination of activities becomes more efficient. Consequently, the communication of risk messages among the members of the IT group is likely to occur more efficiently. However evidence also shows that strong culture or effective communication of risks do not only occur as a consequence of establishing trust but rather that trust through better co-ordination of activities, positive attitudes and trust to the IT manager, provides the conditions under which culture and/or risk communication are more likely to occur.

3.5 The Determinants of Trust

One of the first determinants of trust mentioned in the interviews, is time. As stated, trust develops over time (Lewicki and Bunker, 1995) through transparent relationships between the members of either an organization or group, although trust is easy to loose. All the interviewees commonly agreed that trust depends on past performance of a group or individual and it builds upon time. They also stated that the manager of the IT group in particular, is responsible for exhibiting 'healthy' patterns of trust in terms that the decisions he makes do not cancel each other out, continuously. For example, in Alpha-Bank it was mentioned that if the IT manager categorises the group's activities to specific individuals and then, he changes his mind and rearranges the individuals' responsibilities in the group, those individuals not only will be confused but also they will lose trust to the manager, in terms of being capable to make decisions. Participation in decision making and in group activities is also another determinant of trust, since the IT employees feel that they can contribute to the group and that their input is being appreciated. Job satisfaction is also important, which means that if the employee likes the nature of his job and job related responsibilities he will be more likely to trust his manager and willing to co-operate in order to produce efficient work outcomes.

Similarly, all of the interviewees within the three case studies stated that moral and money rewards are also important determinants of trust. In the context of moral rewards, the manager plays a significant role in establishing trust among his employees since he is responsible for many duties such as performance evaluations, promotions, guidance on job responsibilities, and training (Rich, 1997). Money rewards is perhaps the most important determinant of trust, particularly in organizations where trust is viewed in terms of professionalism, such as Delta- and Omega-Bank, respectively. The respondents in Delta and Omega-Bank said that having money incentives creates a feeling of trust towards the top-management, as the employees' contribution is rewarded. During the interviews within the case of Alpha-Bank, the people also stated that group solidarity is another determinant of trust, in terms that different members within the group have to equally share the responsibilities assigned by the manager. In addition, they mentioned that each member has to understand his role within the group, something of which responsible is also the group's manager. Downsizing is also an important determinant of trust because during organizational downsizing survivors sense of empowerment can decrease and survivors do not believe that top-management communication is credible or that information is being withheld (Mishra and Spreitzer, 1998). All these determinants are exhibited in Table 2 below.

Determinants of Trust at a Macro-level
Time
Clarity and stability in decision making
Participation in decision making and group activities
Job satisfaction
Moral rewards (promotions, performance evaluations, guidance on job responsibilities, training)
Money rewards
Group solidarity
Role guidance
Downsizing

Table 2 The Determinants of Trust at Group level

4. Conclusions

The case study research conducted within the present research raised many social and organizational issues that had not been previously investigated in relation to the goal setting theory within an information systems risk management process. Therefore, the human and organizational aspects, such as trust, culture, and risk communication have been recognized but not investigated further into the context of information systems risk management process.

The research described in this paper was concerned with Information Systems security risks. The last decade it is believed that the approaches and techniques used for the management of security risks tend to ignore the social aspect of risks and the informal structure of organizations (as suggested by Baskerville, 1991; Straub and Welke, 1998; Dhillon and Backhouse, 2001). Thus, in this paper a social and organizational approach was being adopted to the management of information systems security with the particular aim to improve the performance of an IT group in managing security. The first issue was to identify issues that play a significant role in the process of goal setting and these were: trust, culture, and risk communication. The results have shown that there is a chain reaction among these issues with a subsequent effect on the level of security goal setting. It was found that trust results into higher levels of cooperation and positive attitudes, something that provides with a better understanding of group culture. Since trust is a value of a group's culture, establishing trust helps to strengthen an IT group's culture. In strong cultures people understand the group goals and coordination becomes easier, as they are more likely to take actions towards common goals with other parts of the organization.

Similarly, it has been shown that high levels of trust and strong culture improve the communication of risks among the members of an IT group. However, results show that the issues of trust, culture and risk communication have less significant role to large IT structures because large organizations have rigid cultural environments which do not allow individual intellect. Further the framework shows that in complex task environments if people are assigned specific, challenging goals (given goal acceptance), people's commitment to the goals will increase (Locke et al., 1981). In the same line of reasoning, goal level, commitment and performance have a complex relationship including both direct and moderator effects (Latham and Locke, 1991). That is, when the goal level is held constant it appears that there are direct effects of commitment on performance. However much of goal setting research is at the individual level, the relationship of goal level, commitment and performance may not necessarily hold at the group level. For example, 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. Thus, the relationship among goal level, commitment and performance within the context of information systems security could be an issue for future research.

The ultimate scope of this paper was also to investigate the determinants of trust at the process of goal setting. The findings from the three case studies are being depicted in Table 2. Understanding the determinants of trust at group level is very important since failure to recognize and improve such social issue may lead to an inefficient goal setting process, whereas security risks with regard to the integrity, confidentiality and availability of data may arise. The suggested framework could further be set in practice by finding also the determinants of culture and risk communication, something that the author of this paper intends to investigate in the future. Finally, the research approach based on the interpretivist paradigm seems the most appropriate to address the research questions of this investigation, as a positive approach would not have allowed the investigation of the social and organizational aspects of risks in their real life context. In addition, undertaking a project of such scale without the assistance of case studies and the use of qualitative research, which has a research philosophy of interpretivism, is difficult.

References

Andersen, I.T. (2006) Security Barometer survey: The Psychology of Security, Quocirca.

Baskerville, R. (1991) "Risk analysis: an interpretive feasibility tool in justifying information systems security", European Journal of Information Systems, 1(2), pp. 121-130.

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

Bradford, D.L. and Cohen, A.R. (1984) "Managing for excellence: The Guide to Developing High Performance in Contemporary Organizations", John Wiley.

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

Coleman, J. (1990) *Foundations of Social Theory*, Cambridge, Harvard University Press.

Cremer, J. (1993) "Corporate culture and shared knowledge". *Industrial and Corporate Change* 2, pp. 351-386.

Deal, T.E., and Kennedy, A.A. (1982) *Corporate Cultures*, Reading, MA: Addison-Wesley.

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

Denzin, N.K. and Lincoln, Y.S. (1998) *Collecting and Interpreting Qualitative Materials*, Sage Publications, Thousand Oaks, California, USA.

DeVito, J.A. (1988) *Human Communication*, 4^{TH} ed., New York: Harper & Row, Inc., pp. 14-15.

Dhillon, G. & Backhouse, J. (2001) "Current directions in IS security research: towards socio-organisational perspectives", *Information Systems Journal*, 11, pp 127-153.

Dirks, K.T. (1999) “The effects of interpersonal trust on work group performance”, Journal of Applied Psychology, 84, pp.445-455.

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

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

Ernst and Young (2006), *Global Information Security Survey*, Ernst & Young, London.

Flick, U. (1992) “Triangulation revisited: Strategy of validation or alternative? *Journal for the Theory of Social Behaviour*, 22, pp.175-198.

Gambetta, D. (1998) *Trust: Making and Breaking Cooperative Relations*, Cambridge, UK, Basil Blackwell.

Herriott, RE. & Firestone, XV.A. (1983) “Multisite qualitative policy research: Optimizing description and generalizability”, *Educational Researcher,* 12, pp. 14-19.

Jacoby, W.E. (1995) “Strategic Information Systems Planning and Implementation in the U.S. Financial Services Industry”. PhD Dissertation, University of London

Janesick, V. (2000) “The choreography of qualitative research design”. In Handbook of qualitative research, N.Y.K. Denzin and Y.S. Lincoln, (eds.), Sage Publications, Thousand Oaks, CA, pp.379-399.

Keil, M. (1994) “Pulling the Plug: Software project management and the problem of project escalation”, CIS Working Paper, Georgia State University CIS-93-13, Atlanta, GA.

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

Krimsky, S. and O. Plough (1988) *Environmental Hazards: communicating risks as a social process*, Auburn House.

Locke, E.A. and Latham, G.P. (1984) *Goal Setting: A Motivational Tool That Works!*, Englewood Cliffs, NJ: Prentice-Hall.

Locke, E.A. and Latham, G.P. (1990) *A theory of goal setting and task performance*, Englewood Cliffs, NJ: Prentice-Hall.

Markus, M.L. (1989) “Case Selection in a Disconfirmatory Case Study, in: The information systems research challenge: qualitative research methods, edited by Cash, J.I. and Lawrence, P.R., Harvard Business School, Cambridge, Massachusetts, USA.

Miles, M.B. and Huberman, A.M. (1994) *Qualitative Data Analysis*, Second Edition, Sage Publications, Inc, Thousand Oaks, California, USA.

Orlikowski, W.J. and Baroudi, J.J. (1991) “Studying information technology in organizations: Research approaches and assumptions, *Information Systems Research*, 2, pp.1-28.

O’ Reilly, C.A. and Chatman, J.A. (1996) “Culture as Social Control: Corporations, Culture and Commitment”. In Staw, B.M. and Cummings, L.L. (eds.), Research in Organizational, 18, pp. 157-200. Greenwich, CT: JAI Press.

Parsons, T. (1960) *Structure and Process in Modern Societies*. New York: Free Press.

Pearce, J.A. and David, F. (1987) “Corporate mission statements: the bottom line”, *Academy of Management Executive*, 1 (2), pp.109-116.

Ross, J. and Staw, B.M. (1993) “Organizational Escalation and Exit: Lessons from the Shoreham Nuclear Plant”, Academy of Management Journal, (36:4), pp.701-732.

Rousseau, D., Sitkin, S., Burt, R., Camerer, C. (1998) “Not so different after all: A cross-discipline view of trust”, Academy of Management Review, 23, pp.387-392.

Seijts, G.H., & Latham, G.P. (2000). The construct of goal commitment: Measurement and relationships with task performance. In: R. Goffin and E. Helmes (Eds.), *Problems and solutions in human assessment: Honoring Douglas N. Jackson at seventy* (pp. 315-332). Dordrecht, the Netherlands: Kluwer Academic Publishers.

Schein, E.H. (1992) *Organizational Culture and Leadership*, 2nd edition, San Francisco: Jossey-Bass.

Sorensen, B. (2002) “The strength of corporate culture and the reliability of firm performance”, *Administrative Science Quarterly*, 47 (1), pp.70-96.

Straub, D.W. and Welke, R.J. (1998) “Coping with systems risks: Security Planning Models for Management Decision Making”, *MIS Quarterly*, 22(4), pp.441-469.

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

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

Von Solms, R. (1998) “Information security management (1): why information security is so important”, *Information Management and Computer Security*, 8(1), pp.224-225.

Yin, R.K. (1984) *Case study research: Design and Methods*, SAGE publications, Inc., Beverly Hills, California, USA.

Yin, R. (1994). *Case Study Research: Design and Methods* (2nd ed.). Thousand Oaks, CA: Sage Publishing.

Willcocks, L. and H. Margetts (1994) “Risk assessment and information systems”, *European Journal of Information Systems*, 3(2), pp.127-138.