A Socio-Organizational Approach to Information Systems Security Management in the Context of Internet Banking

Ioannis Vasileios Koskosas

A thesis submitted for the degree of Doctor of Philosophy

Department of Information Systems and Computing at St. John's

Brunel University

March 2004

ABSTRACT

This thesis takes a social and organizational point of view for studying information systems security in the context of internet banking. While the internet provides opportunities for businesses to extend their public network infrastructure, reduce transaction costs, and sell a wide range of products and services worldwide, security threats impede the business. Although, a number of valuable information systems security approaches have been developed through the years they tend to offer narrow, technically oriented solutions and they ignore the social aspects of risks and the informal structures of organizations. To this end, there is an emphasis in the literature to adopt a socio-organizational approach to information systems security (ISs) management. This thesis is based on the assumption that information systems security in the context of internet banking can be efficiently investigated and understood through a systematic and comprehensive study of various social organizational aspects in the goal setting context. To this end, the thesis presents a novel approach to the management of information systems security based on the use of the *performance pyramid model*. Using previous research in the social organizational literature this work examines the interrelationship of trust, culture, and risk communication and their possible effect on the level of goal setting within the context of information systems security management with a focus on internet banking. It explores and discusses the process of goal setting in the context of risk management. Based on the proposed performance pyramid model this research identifies the determinants of trust, culture, and risk communication as well as the determinants of goal commitment at macro level. The thesis contributes to interpretive information systems research with the in-depth analysis and study of the social organizational concepts in a security management context and its grounding within an interpretive epistemology. It emphasises the importance and interrelationship between different socio-organizational aspects of goal setting theory and demonstrates the values of each aspect in the information systems security domain thus contributing to a rich insight in the particular empirical research context.

DEDICATION

.....To my family

ACKNOWLEDGEMENTS

I would like to express my gratitude to my supervisor Professor Ray Paul for his commitment, advice and support but most of all, for the intellectual guidance he provided during my research years. I am also grateful to Dr. David Lee whose comments on my thesis reports are appreciated. I would like to thank Dr. Nancy Pouloudi for being an initial source of inspiration and support. Her thoughts and remarks were valuable. Many thanks to Dr. George Magoulas for expressing his views on the first 'drafts' of my thesis.

I would like also to thank all the members of the Information Systems and Computing department at Brunel University for their academic rigour and their unique angle in viewing and studying information systems. Similarly, I would like to thank all the participants in the case studies who spent their time, shared their views and experience with me. In particular, I am grateful to Mr. and Mrs. Karatoulioty for introducing me to the IT manager at one of the case studies as well as the IT managers of the remaining studies for accepting me and arranging the interviews with the participants. I hope the research findings will be a useful reference to them and to their organizations.

Last but not least, I would like to thank my family for their patience, moral and financial support throughout this research effort. Without them this research would not have materialised.

DECLARATION

Some of the material contained in this dissertation has been presented in the following publications:

Journal Papers

Koskosas, I.V. and Paul, R.J. (2004) Information Security Management in the Context of Goal Setting, *Risk Management: An International Journal*, Vol. 6, No. 1, pp. 19-29.

Koskosas, I.V. and Paul, R.J. (2003c) A Socio-Organizational Approach to Information Systems Security, *International Journal of Risk Assessment and Management*, Vol. 4, No. 2/3, pp. 232-244.

Papers in Refereed Conference Proceedings

Koskosas, I.V. (2004) The Interrelationship and Effect of Culture and Risk Communication in Setting Internet Banking Security Goals, *6th International Conference on Electronic Commerce*, Delft, The Netherlands, October 2004, (forthcoming).

Koskosas, I.V. (2004) The Interrelationship and Effect of Trust and Strong Cultures in Setting Information Systems Security Goals, *15th Annual Conference International Information Management Association*, Chicago, USA, October 7-9, (forthcoming).

Koskosas, I.V. and Paul, R.J. (2003a) The Performance of Risk Management in the Context of Goal Setting: The Case of Internet Banking, *Proceedings of the 8th Collaborative Electronic Commerce Technology and Research Conference*, Editors: Thomas Acton, June 24th, pp. 242-249.

Koskosas, I.V. and Paul, R.J. (2003b) A Socio-Organizational Approach to Information Systems Security, *Proceedings of the 2nd European Conference on Information Warfare and Security*, Editors: Bill Hutchinson, 30th June, pp. 175-185. (republished)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1: INTRODUCTION

1.1 Introduction

This chapter discusses the background of the research problem under investigation and some important concepts in this dissertation. It sets the context and explains the rationale, thus providing a basis upon which the work is subsequently described and the results interpreted.

The research described in this dissertation is concerned with information systems (IS) security in the context of internet banking. Banking, among others, is being a highly intensive activity that relies heavily on information technology (IT) to acquire, process and deliver the information to all relevant users. To this end, IT provides a way for banks to differentiate their products and services delivered to their customers. Driven by the challenge to expand and capture a larger share of the banking industry, some banks invest in bricks and mortar while others have considered a new approach to deliver their banking services via a new medium: the Internet.

While the internet provides opportunities for businesses to increase their customer base, reduce transactions costs, and sell their products globally, security implications impede the business (Forcht and Wex, 1996). Although a number of significant, valuable approaches have been developed for the management of information systems security, they tend to offer narrow, technically oriented solutions and they ignore the social aspects of risks and the informal structures of organizations (Backhouse and Dhillon, 1996; Straub and Welke, 1998; Siponen, 2000).

To this end, the research in this dissertation adopts a socio-organizational approach to investigate information systems security in the context of trust, culture, risk communication, and goal setting. This chapter gives an introduction to the problem under investigation and discusses the necessity to adopt a socio-organizational approach to IS security management and in so doing, it outlines *the performance pyramid model*

suggested in this dissertation. What then follows is the research motivation and objectives, an introduction to the emergent research methodology, the expected contributions of the research and ultimately, the chapter ends by describing the overall structure of the thesis.

1.2 The Issue of Internet Banking

The internet has been rapidly gaining popularity as a potential medium for electronic commerce (Crede, 1995; U.S. Department of Commerce, 1999). The reason for such popularity is the fact that individuals have the ability to communicate and exchange information with people all over the world (Gore, 1999). Firms have the potential to reach a large number of customers and fully automate their transactions in the value chain (Kosiur, 1997) while governments can provide more efficient services to citizens by automated procedures such as public procurement and local or national elections (Andersen, 1998). Today, the internet is believed to be on its way to becoming a full-fledged delivery and distribution channel while among the consumer-oriented applications riding at the forefront of this evolution are electronic financial products and services (Tan and Teo, 2000).

The emergence of internet banking has made banks re-think their IT strategies in order to remain competitive as internet banking services is believed to be crucial for the banks' long-term survival in the world of electronic commerce (Burnham, 1996). Today, customers demand new levels of convenience and flexibility (Lagoutte, 1996; Birch and Young, 1997) on top of powerful and easy to use financial management tools, products and services, something that traditional retail banking could not offer (Tan and Teo, 2000). Thus, internet banking allows banks to provide these services by exploiting an extensive public network infrastructure (Ternullo, 1997).

The use of new distribution channels such as the internet, however, increases the importance of security in information systems as these systems become sensitive to the environment and may leave organizations more vulnerable to systems' attacks. Thus,

the issue of security in the context of internet banking makes it an interesting candidate to investigate.

1.3 Background to the Research Problem

The rise of electronic commerce has highlighted awareness amongst organizations of the security threats to which they are likely to be exposed. Indeed, it has been reported that security threats and fear of security breaches, constitute the greatest inhibitors to an expansion in the uptake of electronic commerce (Ernst and Young survey, 2001).

Similarly, a number of major studies on information systems security recently conducted in Europe, among these being the Andersen 2001 survey, the Ernst and Young 2001 survey, and the DTI study 2002, indicate a general upward trend in the number of security incidents in organizations. These studies further suggest that organizations expressed uncertainty about future security issues, noting that security incidents are increasing both in terms of number and complexity. In this dissertation IS security is viewed as the minimisation of the risks arising from unauthorised access to and possession of information (Dhillon, 1995). In the context of information systems, the asset under consideration is data and the main IS security foundations are the integrity, confidentiality and authenticity of such data (Forcht and Wex, 1996).

Over the years, a number of security approaches have been developed that help in managing IS security and in limiting the chances of an IS security breach. The majority of these approaches are presented in Table 1 below. The thick separated lines represent the different generations originally presented by Baskerville (1988). The arrows show influences or inspirations while the broken arrows mean that the approach is influenced by the deficiencies of a certain approach. The tradition (*Computer Science, Data Modeling, Practitioners Community and IS Community*) from which the works sprung is described using *italics*. For example, responsibility modelling is developed in the Computer Science Community.

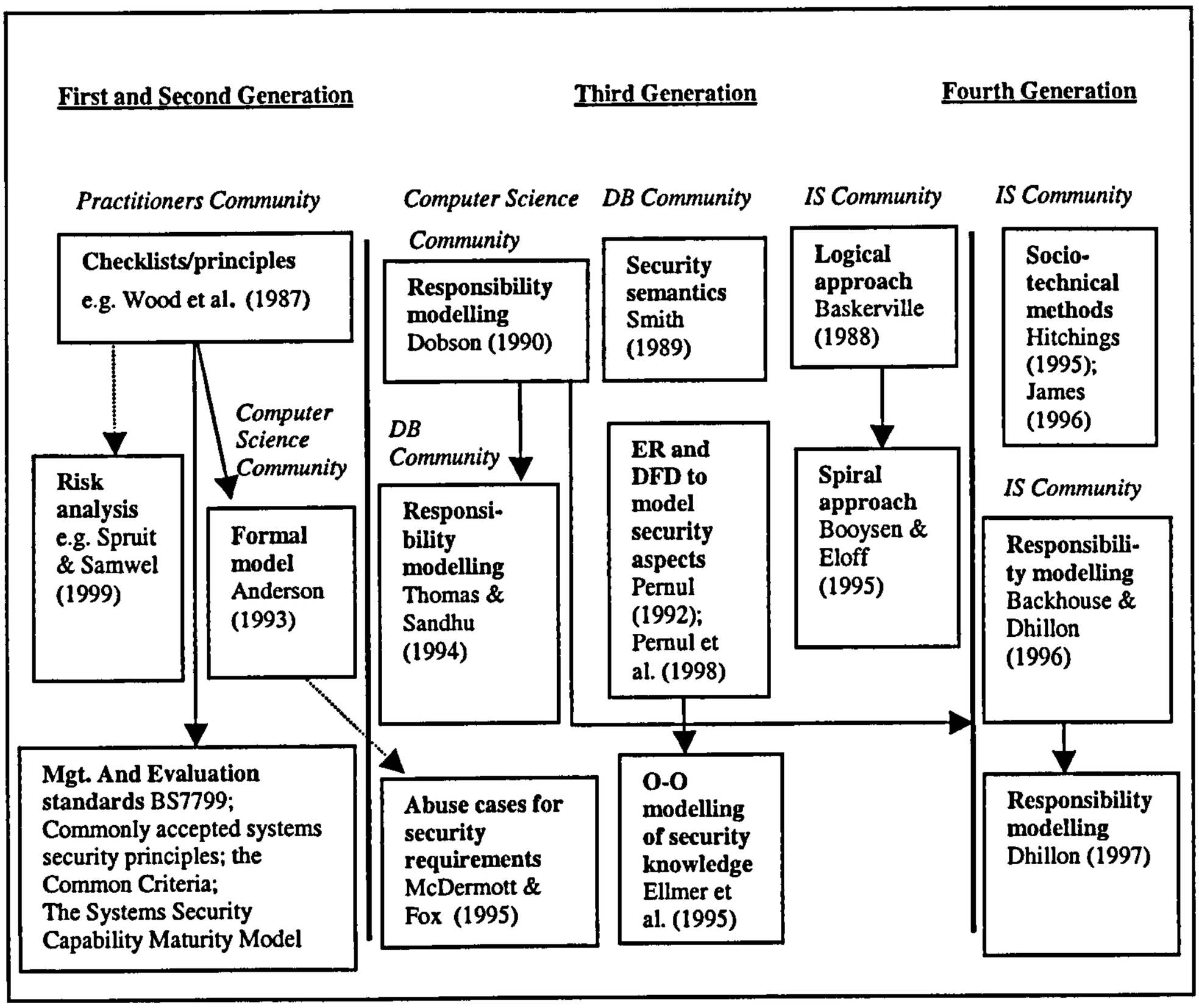


Table 1 An overview of approaches for secure IS development (Siponen, 2001)

First and second generation methods aim at finding out what can be done and actually dominate the principles, checklists, and most standards for secure systems development. Third generation approaches include modelling and fourth generation emphasize socio-technical design. Siponen (2001) supports the view that there have been only a few isolated (less-well known) approaches to consider the socio-technical aspects of information systems security management. The majority of IS security methods entails checklists, risk analysis, and evaluation methods. Although these approaches help in managing security, Siponen (2001) supports the need for IS security approaches to provide a holistic modeling support which can be integrated into modern IS development approaches, and the lack of approaches which focus on socio-organizational roles of IS security.

Hirschheim et al., (1995), Backhouse and Dhillon (1996), Hitchings (1996) and James (1996), suggest that although the value of most IS security methods, tools, and techniques is evident, their focus is on narrow, technically oriented solutions and they

ignore the social aspects of risks and the informal structures of organizations (see also the arguments proposed by Baskerville, 1991; Willcocks and Margetts, 1994; Straub and Welke, 1998; Siponen, 2000). Dhillon and Backhouse (2001) have also analyzed existing approaches within the socio-philosophical framework of Burrell and Morgan (1979) and in so doing, they suggest that a socio-organizational perspective is the way forward if information systems security is to be achieved.

Similarly, as the annual total of security-related incidents is on the increase, current means for managing information systems security have been unable to fulfil their promise. The application of various security risk management approaches seems inadequate in managing efficiently IS security risks, and overall the performance of an IT manager and group in managing risks efficiently remains limited.

Following these trends, the investigation in this dissertation adopts a socio-organizational approach to information systems security management. In doing so, it makes the consideration that, although IT (security) managers and groups have a variety of security risk management methods, tools and techniques available, they may not make an efficient use of them in the context of risk management activities. Thus, the research reported in this dissertation is based on the rationale that *security risks may arise due to failure to obtain some or all the goals that are relevant to the management of the integrity, confidentiality and authenticity of information through the internet banking channel.* To this end, the first objective of this research is to investigate whether IT (security) managers and groups set security goals in relation to the management of the integrity, confidentiality, and authenticity of information through the internet banking channel.

This research intends to offer an in-depth study of the goal setting process in the context of information systems security (ISs) management, with a focus on internet banking, by examining different socio-organizational aspects that may have an impact on the process. Based on the literature, however, this research identified a set of socio-organizational aspects such as trust, culture, and risk communication, that may play an important role on the level of goal setting within the information systems security context. To this end, it suggests a novel approach based on the *performance pyramid model* (Chapter 2). The model is actually distinguished by two main parts. In the first

part, it shows that there might be an interrelationship between trust, culture, and risk communication and that such aspects might have an important role on the level of goal setting with regard to information systems security management.

Based on existing literature findings, the second part of the model illustrates that at the level of goal setting in complex task environments, if people are assigned specific, challenging goals (given goal acceptance), their commitment to the goals tends to increase (Locke et al., 1981). In the same line of reasoning, the goal level, commitment, and performance have a complex relationship including both direct and moderator effects. That is, when the goal level is held constant it appears that there are direct effects of commitment to performance. In other words, the relationship between goal level and performance is stronger with high levels of commitment than with low. However, the relationship between the goal level, commitment and performance is not in the scope of this investigation but rather the scope is also to identify any possible determinants of commitment at macro level.

1.4 Research Motivation and Objectives

1.4.1 Research Motivation

Organizations wishing to survive in a highly competitive environment have to embrace information systems and technologies and ensure the availability and exploitation of high quality information. Thus, it is vital that adequate security and control procedures are introduced to ensure that the information embedded within organizational information systems retains its integrity, confidentiality and availability (Dhillon and Backhouse, 2001). To this end, the increased risk of information security problems has led to a growing awareness among researchers and practitioners to rethink their approaches to information systems security as there is an emphasis in recent years that IS security needs to adopt a socio-organizational perspective (as suggested by Baskerville, 1993; Dhillon and Backhouse, 2001; Straub and Welke, 1998; Siponen, 2001).

When deciding the area within which the research is pursued, a careful consideration was given into how much research already exists, the timeliness, research resources and nature of problems. A review of the literature has shown that many of the empirical studies have, indeed, covered a broad range of technical-oriented information security issues rather than focusing on the social, cultural aspects of information security management. Thus, the motivation of this research is to shed some light into different socio-organizational aspects, which can be used for the study of information systems security management. To this end, the focus of this research is the examination of different socio-organizational aspects in goal setting theory within the management of information systems security context with a focus on internet banking. This will be achieved by examining the possible interrelationship of different socio-organizational concepts identified in the literature such as trust, culture and risk communication and their possible effect on the level of security goal setting. The level of goal setting in this research is defined as the stage at which IT managers and groups are about to start the implementation of goals.

Moreover, if the relationship between the goal level, commitment and performance holds at a macro goal setting level the identification of any possible determinants of commitment will shed some light into the problems of commitment faced by IT managers and groups and thus, how to improve their performance in managing effectively security related risks.

1.4.2 Research Objectives

To reflect upon the research motivation the research objectives of the study have to be made clear:

1. To conduct a comprehensive literature review in the area of information systems security and internet banking so that a better understanding of the research needs can be obtained

2. To conduct a comprehensive literature review on different social organizational issues in order to identify theories and concepts that can be applied to the area of information systems security management

However, having reviewed the literature in both information systems security and different socio-organizational concepts, a theoretical model has been established. In order to investigate and deepen understanding of the possible interrelationship, interaction and impact of the different socio-organizational concepts of the performance pyramid model, in the context of information systems security, the extensive objectives of this research are:

3. To investigate whether IT (security) managers and groups follow goal setting processes with respect to the management of the integrity, confidentiality and authenticity of information through the internet banking channel

4. To investigate if there is any interrelationship between different socio-organizational aspects such as trust, culture and risk communication and their possible effect on the level of security goal setting

5. To investigate if there are any determinants of trust, culture, and risk communication and if there are to identify them, so that the performance pyramid model can be practically used

6. To investigate if there are any determinants of goal commitment at a macro-level and if there are to identify them.

1.5 The Emergent Research Methodology: An Introduction

A qualitative research approach having philosophical foundations mainly in interpretivism was deemed the most appropriate for this investigation. Based on the nature of this investigation, an interpretive epistemology is more appropriate as it can provide an understanding of different social organizational issues related to goal setting

in the context of information systems security management. In fact, many theorists argue that information systems are essentially social systems (e.g., human-computer interaction) and there is an increasing need to understand the social and organizational issues that may have an important input in the implementation and selection of information systems (Liebenau and Backhouse, 1990; Angell and Smithson, 1991; Land, 1992; Laudon and Laudon, 1996; Lee and Liebenau, 1996).

Schein (1992) also suggests that an interpretive research approach would provide richer data when used to describe an organizational culture. In doing so, an interpretive approach would provide a deeper understanding of the culture within organizations and IT groups in particular, which in turn, could be used to understand how IT managers and groups set security goals and why they may have different goal setting procedures.

Likewise, a qualitative research approach was chosen due to its potential to study things in their natural environment and provide an understanding of people's idiosyncrasies as well as the social and cultural contexts within which they live (Myers and Avison, 2001). As the process of goal setting is complex and dynamic, based on the organizations' information systems needs (Koskosas and Paul, 2004), qualitative research seems to be more appropriate as it focuses on understanding the complex socio-organizational environment of the phenomenon.

With regard to the research strategy, having considered the possible benefits of each available method i.e., action research, case studies, field studies, application descriptions, and ethnography, it was decided that the advantages offered by case studies are more suitable to the purpose of this research. There are different case study types including exploratory, descriptive, and explanatory based on the type of research questions asked such as "what", "how", or "why" (Yin, 1994). This research uses questions of the type "what" and "how" and thus aims to explore and describe.

Similarly, this research employed multiple case studies since the more replications there are, the more robust the findings (Yin, 1993). Herriot and Firestone (1983) point out that the evidence from multiple case studies is often considered more convincing, and the overall study more robust. To this end, a multiple case study approach was followed within the IT departments of three financial institutions. The choice of institutions based

in Greece was dictated by the access available to the researcher and the recent introduction of the internet banking product in the Greek banking market. The size of the institutions ranged from small (Alpha-Bank), to medium (Delta-Bank), to large (Omega-Bank). The reason for choosing banks of different sizes was to investigate whether the performance pyramid model can be applied to different IT group structures. For example, the IT department of Alpha-Bank consisted of 60 employees, of Delta-Bank 150 and that of Omega-Bank 410. Thus, the cases were actually chosen to replicate, extend and verify the literature findings on socio-organizational issues depicted on the performance pyramid model.

The research design of this investigation employed multiple data collection methods such as open-ended interviews, telephone interviews, archival documents, and observation. The use of multiple collection methods makes triangulation possible and this provides stronger substantiation of theory (Eisenhardt, 1989). Interviews are very useful as they allow the researcher to interact with case study participants and observe environmental settings. Nonetheless, the methodology and research design of this investigation are discussed and explained in more detail in Chapter 3.

1.6 Overview of the Research Contributions

This chapter presented the broader research context. It provided a brief background to the research problem in the area of information systems security and outlined the research approach in this dissertation based on the performance pyramid model discussed in the next chapter. In order to face the challenge of this research context the thesis argues for the relevance of the goal setting concept in information systems security management. Specifically, it is argued that an interpretive approach to goal setting is useful in order to understand the management of activities in the context of information systems security risks.

The main research contribution is to develop a socio-organizational model that can be used to analyse future research studies and shed light into the socio-organizational dimensions of information systems security. The research intends to demonstrate the use of socio-organizational aspects such as trust, culture, and risk communication in the

context of goal setting for an in-depth examination of the information systems security management phenomenon.

The theoretical contributions of this research are embedded in the socio-organizational context of trust, culture and risk communication as well as the theories of goal setting and goal commitment. In particular, the research considers a set of socio-organizational aspects, thus addressing an important limitation of their use in information systems security research. It provides an understanding of the interrelationship of trust, culture and risk communication and their role on the level of goal setting with regard to IS security management. Likewise, it explores the possible determinants of such socio-organizational aspects as well as the determinants of commitment at group level.

The practical contributions lie in the establishment of the socio-organizational model which can be used by IT (security) managers and groups to improve the efficiency of the goal setting process and consequently their performance in managing effectively information systems security in the context of internet banking.

1.7 Dissertation Outline

The dissertation is composed of seven chapters with each of them providing an understanding to various issues viewed to be critical for this research. The following paragraphs give a synopsis of the scope of each chapter and Table 2 gives a summary of the dissertation's organizational structure for easy of reference.

Chapter 1 begins by providing an introduction to the research problem and some important concepts in this dissertation. Then, it explains the reasons to investigate information systems security from a socio-organizational viewpoint since most IS security approaches though valuable, focus on narrow, technically oriented perspectives and they ignore the social aspects of risks and the informal structure of organizations. Ultimately, the motivation and objectives of this investigation are discussed and the chapter ends with the dissertation outline.

Having provided an introduction to the domain area and the research problem under investigation the dissertation then proceeds to a literature review on the theory of goal setting in **Chapter 2**. It investigates the nature and philosophy of goal setting and identifies socio-organizational issues that may have an impact on the process of security goal setting in the context of IS security management. Based on the literature review findings, chapter 2 suggests a novel model named, the *performance pyramid model*, which consists of, mainly, two parts. The first part illustrates three important issues in the process of security goal setting, these are: trust, culture and risk communication. The second part illustrates the relationship between goal level, commitment and performance. The chapter ends by giving the research directions based on the performance pyramid model.

In order to approach the research problem under investigation a research methodology has to be chosen. To this end, **Chapter 3** describes the methodology approach chosen for this particular investigation and discusses the various alternative research approaches existing in the literature. In doing so, it provides the justification for choosing an interpretive epistemology, the data collection methods, and the research design. The chapter also discusses current approaches in the context of information systems security.

In **Chapter 4** the performance pyramid model is applied to the case of the small structure organization in order to test the validity of the rationale and assumptions made in this research. The chapter gives also a brief background of the organization in the context of its history, business, infrastructure, management and organization on a global scale.

Chapter 5 describes and discusses the case of the medium and large organizations respectively in order to test the validity of the rationale and assumptions of the research to different organizational structures within the information systems security context. Similarly, the chapter gives a brief background of the organizations' history, business and management, infrastructure, as well as their recent developments. Some preliminary findings are also discussed in the socio-organizational context.

In **Chapter 6** the findings obtained from the organizations are analysed and discussed in relation to the findings achieved from the first case study organization in order to replicate, extend and verify the rationale and assumptions made within the context of the performance pyramid model. The chapter also presents and discusses the determinants of trust, culture and risk communication as they were reported from the interviewees within the organizations. The determinants of commitment at a macro level are also discussed and taxonomized into different categories.

Ultimately, **Chapter 7** gives a summary of the research findings and an overview of the research contributions in the context of theory, methodology, and practice. In terms of social organizational theories, the thesis advances their use in information systems security research particularly by establishing the interrelationship of trust, culture, and risk communication and their effect on the level of security goal setting and arguing for the necessity to understand their implications. In the light of the thesis overall contributions, the final chapter discusses also the limitations of the research approach and recommends some directions for further research.

Section	Focus	Comment
Chapter 1	Overview of the research	Background to the research problem, research rationale and assumptions, motivation and objectives
Chapter 2	Literature review on social organizational issues to define research questions and objectives	A synthesis of socio-organizational issues into the performance pyramid model
Chapter 3	Research methodology and design	Discussion of current IS security approaches and selection of a suitable research methodology
Chapter 4	Empirical investigation of goal setting within the case of Alpha-Bank: small-scale structure	An examination of the performance pyramid model rationale in the context of IS security management
Chapter 5	Empirical investigation of goal setting within the case of Delta- and Omega-Banks: medium- and large-scale structures	An examination of the performance pyramid model rationale in the context of IS security management: some preliminary findings
Chapter 6	Analysis of the case studies	A comparison and analysis of the research findings within context of the performance pyramid model
Chapter 7	Summary and conclusions	Summary of the findings, overview of research contributions, research limitations and directions for future research

Table 2 Structure of this Dissertation

Chapter 2: Literature Review on Socio-Organizational Issues

2.1 Introduction

Internet banking allows customers a very convenient and effective approach to manage their finances as it is easily accessible 24 hours a day, and even seven days of the week. When first introduced, internet banking was used as an information presentation medium in which banks marketed their products and services on their Web sites. With the development of secured electronic transaction technologies, more banks have come forward to use internet banking both as a transactional as well as an informational medium. In effect, internet banking users can now perform common banking transactions such as paying bills, transferring funds, printing statements, and inquiring about balances.

However, as mentioned in Chapter 1, the use of new distribution channels such as the internet increases the importance of security in information systems as these systems become sensitive to the environment and may leave organizations more vulnerable. Although, a number of valuable security approaches have been developed that help in managing security and in limiting the chances of an IS security breach, evidence shows that information security management needs to adopt a socio-organizational perspective (Baskerville, 1991; Willcocks and Margetts, 1994; Straub and Welke, 1998; Siponen, 2000; Dhillon and Backhouse, 2001).

Thus, this chapter reviews the social sciences literature for a suitable theory of knowledge that could be applied in the area of information systems security. The chapter provides an introduction to the theoretical concepts that form the basis of the socio-organizational model suggested in this dissertation. Understanding the theoretical concepts that lie beneath the chosen approach allows the establishment of assumptions for this particular investigation.

The next section introduces the concept of risk in order to provide a deeper understanding of the nature and theories underlying risk. Section three discusses the theory of goal setting and its influence on social learning theory. Sections four, five and six introduce the concepts of risk communication, culture and trust upon which the suggested model is discussed and explained. Section seven discusses the importance of goal commitment and its effect on performance. The chapter ends with a summary and a brief description of the literature findings.

2.2 The Concept of Risk

Although, every action taken by people on a daily basis incorporates some form of risk there is no single definition about risk. Computer scientists, economists, sociologists, risk analysts have their own concept and interpretation of risk. However, risk has been traditionally defined in terms of uncertainty. Based on this idea, risk is defined as uncertainty concerning the occurrence of a loss (Rejda, 1998). Similarly, Britain's Royal Society, based on a Group Study in 1992, defined risk in statistical terms as:

'The Study Group views 'risk' as the probability that a particular adverse event occurs during a stated period of time, or results from a particular challenge. As a probability in the sense of statistical theory, risk obeys all the formal laws of combining probabilities'.

However, when risk is defined as uncertainty or probability of an adverse effect there must be a careful distinction between objective risk and subjective or perceived risk. Objective risk is the relative variation of actual loss from expected loss while subjective or perceived risk is defined as a person's often very different anticipation of future events which is based on the person's mental condition or state of mind (Adams, 1995; Rejda, 1998). Objective risk can be measured statistically by some measure of dispersion such as the standard deviation or coefficient of variation.

Similarly, Vlek and Stallen (1981) support the idea that risk can be quantified and then measured, as the outcome of the probability of a loss or the size of a possible loss and is

equal to the variance of the probability distribution of all possible consequences of a risky action. They also support that risk is the semi-variance of the distribution of all consequences and the expected value of the distribution of all possible consequences.

However, there are approaches to risk other than the quantitative ones such as the qualitative or so-called economic approaches. In decision making the economic approach estimates the magnitude of risk in order to allow a comparison of the risks associated with alternative actions. When a risk event occurs, experiments show that individuals' perceptions of the magnitude of risk depend on how likely they think the event is and how serious they consider the effect to be (Hurst, 1998). Likewise, risk analysts measure the level of risk in terms of the probability (relative likelihood) of a possible outcome in a given time period, and of the magnitude (importance) of the consequences of that outcome (Merkhofer, 1987). To this end, risk may be represented as a probability distribution over adverse consequences.

In the social context, social theories of risk provide both an individualist and contextualist interpretation to risk events. Individualism analyses the thoughts and acts of an individual and is distinguished by knowledge and personality theory. Knowledge theory suggests that individuals respond to a risk event based on the knowledge and information they have while in the context of personality theory, it is personality which determines whether the individual is risk averse or risk taker (Wildavsky, 1990).

In the opposite, contextualism focuses on the culture, organization or life style in the context of their setting, e.g., cultural element, social structure, or institutional form rather than the individual itself (Krimsky, 1992). Kasperson (1992), Palmlund (1992), and Wynne (1992) have also focused on the interpretation of risk from a contextualist point of view. In this dissertation, the researcher defines risk in the context of security, within the contextualist paradigm as *failure to obtain some or all of the goals that are relevant to the management of the integrity, confidentiality, and authenticity of information through the internet banking channel.*

2.2.1 Risk Analysis vs. Risk Assessment

Generally speaking, risk analysis has been the cornerstone of security management and it has proven very useful in allowing organizations to justify the cost of new information systems security while avoiding the implementation of unnecessary controls. Risk analysis methods suggest that if countermeasures are developed and implemented in a logical sequential way then, negative risk events can be prevented while information systems can be made more secure. In similar terms, risk analysis techniques allow the definition of financial benefits versus the initial costs of an investment.

The popularity of risk analysis methods is well noticed through the work of various researchers such as Parker (1981), Fisher (1984), Birch and McEvoy (1992), Kailay and Jarratt (1994) although Courtney (1977), Wong (1977), and Fitzgerald (1978) were among the first.

Courtney (1977) for instance defines risk (R) in terms of probability (P) of an exposure occurring a given number of times per year and the cost (or loss) (C) associated with such exposure. Thus risk equals to: R= P x C.

Baskerville (1988; 1991; 1993) though argues that this approach is inefficient to quantify risk. According to him, risk probabilities (P) and loss estimates (C) are highly interpretative and these values are manipulated with positive and logical mathematical calculations noting that, with regards to the efficiency of security mechanisms, this approach lacks the ability to establish feedback. Similarly, Ansell and Wharton (1992) argue that quantitative approaches to risks convey little practical value although in relation to one-off decisions.

Moreover, Merten et al. (1982) look at risk analysis from a managerial viewpoint whereas Anderson et al. (1993) outline risk data repository for a 'dynamic risk evaluation'. Boockholdt (1987) argues that risk analysis is important in establishing security and integrity controls while Saltmarsh and Browne (1983) and Gallegos et al. (1987) differentiate between risk analysis and risk assessment, the former as a process of identification, and risk assessment as the degree of exposure. Based on this

differentiation then, Gallegos et al. (1987) support that risk analysis is useful in establishing the monetary value of risks.

Lichtenstein (1996) suggests that in the development of information systems, risk assessment is a two-stage process. The first stage defines the scope of risk assessment, which allows the identification of the information resources and then prioritises risks in respect of those resources. The second stage provides useful information in the context of risk-controls, which in turn can be used to make decisions such as whether to transfer risk by implementing safeguards. Moreover, even though organizations use different risk assessment methods at the initiation stage of information systems development the majority of these methods are based on economic or statistical criteria (Lichtenstein, 1996). The main characteristics of such criteria are based on qualitative measures such as usability, complexity, credibility, completeness, adaptability, and validity, with the exception of costs, which are defined by quantitative means.

2.2.2 Risk Assessment vs. Risk Management in the Social Context

Risk management can be defined as a systematic process for the identification and evaluation of pure loss exposures faced by an organization or individual and for the selection and implementation of the most appropriate techniques for treating such exposures (Rejda, 1998).

Risk management, however, encompasses disciplines from the natural, engineering, political, economic, and social sciences, and one of the key issues highlighted by the multidisciplinary of risk management is whether risk assessment as a scientific process can and should be separated from risk management.

Fundamental views of the role of science and society could actually provide the basis of the arguments for and against separation. At a certain point, the arguments of whether risk assessment should be isolated or integrated into risk management can be settled on the issue of whether science and the scientific process can be regarded as completely objective (Hester and Harrison, 1998).

With regard to science, there are two main schools of thought. Logical positivism suggests that science is objective and supports that scientific risk assessments should be kept separate from the social and political aspects of decision making. Conversely, cultural relativism argues that science and the scientific process are linked to subjective value judgements, that science is bound up with political and social institutions and therefore, is incomplete (Hester and Harrison, 1998).

Nevertheless, between the two positions of complete isolation and total integration a variety of other positions exist that base their arguments to a greater or lesser extent on the two extremes. Scientific proceduralism, for example, is perhaps one of the most persuasive notions which seeks to tread a somewhat cautious path between the two extremes. In particular, it recognizes explicitly that science is not completely objective and that subjective value judgments within technical risk assessments have to be acknowledged and dealt with in an effective way (Frechette, 1991). O' Riordan (1991) and Earl and Cvetkovich (1995) argue that one of the strengths of this approach is that it does not argue for a wholesale rejection of risk assessment but rather, it concentrates on a combination of robust scientific and technical aspects, effective communication and stakeholder involvement.

Hester and Harrison (1998) though argue that risk assessment is part of the risk management process and that risk management is a cyclical process which emphasizes the importance of feedback to the extent that the starting and finishing points for risk management, merge (Figure 1). According to them, there is no widely accepted theory for isolation or integration of risk assessment from the risk management process although traditionally, primarily linear approaches to understanding risk management have prevailed reflecting the separation of risk assessment from risk management activities.

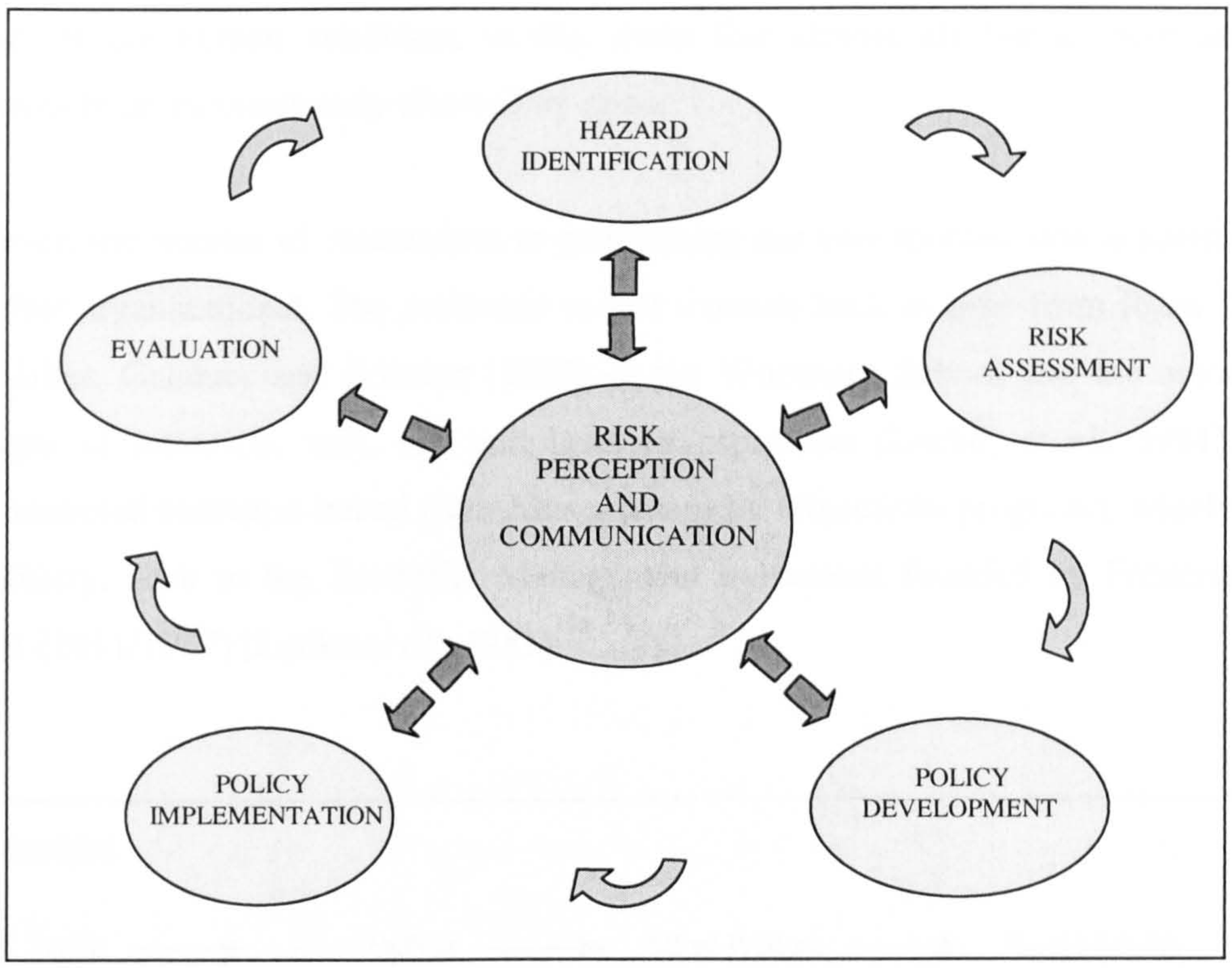


Figure 1 The Risk Management Cycle (Hester and Harrison, 1998)

2.3 Goal Setting in Context

2.3.1 An Introduction

The theory of goal setting falls within the broad domain of cognitive psychology and its literature is extensive. The theory, as the name implies, is based on the concept of goals and is an essential element of social learning theory (Bandura, 1997), which has become increasingly influential through time (Mitchell et al., 2000). Locke (1997) and Mitchell (1997) argue that even the literature on organizational behaviour modification can be interpreted largely within a goal setting framework and that it is the single most researched topic in the field of motivation.

Goals, however, can be viewed as internal psychological representations of desired states, which can be defined as outcomes, events, or processes (Mitchell et al., 2000). A goal encompasses terms such as intention, aim, task, deadline, purpose and objective. It

is part of the human condition, in the sense that almost all human activities are consciously or unconsciously directed by goals.

However, the interest of researchers in goal setting has two sources, one academic and the other organizational. The academic source extends back in time from Ryan (1970) and Miller, Galanter and Pribram (1960) to the Wurzburg School and the associated concepts of intention, task, set, and level of aspiration (Locke, *et al.*, 1981). The organizational source is traced from Management by Objectives programs, widely used in industry, back to the Scientific Management movement founded by Frederick W. Taylor (1911/1967) (Locke *et al.*, 1981).

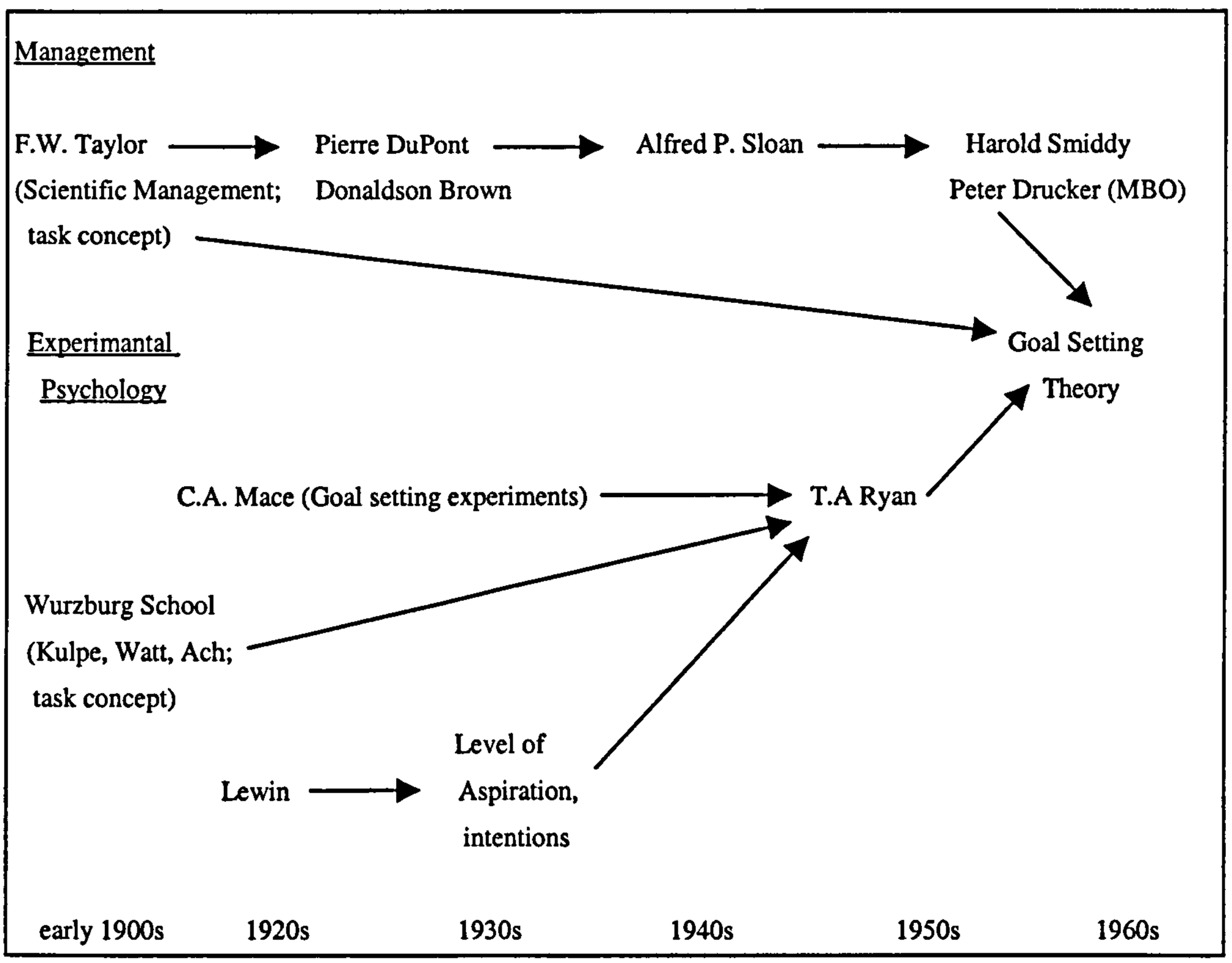


Figure 2.2 Historical Precursors of Goal Setting Theory (Locke and Latham, 1990)

The most direct influence on the theory of goal setting was the work of Ryan (1970) although goal setting theory has precursors that go back to the start of the century (Locke and Latham, 1990). Broadly speaking, there are two strands of influence linked

to the theory of goal setting: the theory of management (organizational) and the experimental psychology (academic) (Figure 2).

Frederick W. Taylor is believed to be the father of Scientific Management after his major work *Principles of Scientific Management* published in 1911 and one of the main contributors in the emergence of Management by Objectives (MBO) (Locke and Latham, 1990). MBO is a technique that attempts to co-ordinate and integrate individual and organizational goals at different levels and to reward performance for goal achievement (Carroll and Tosi, 1973).

Pierre DuPont was the first to use some of Taylor's ideas on accounting and cost control but it was actually Alfred Sloan to use MBO formally in order to motivate and evaluate his managers. Drucker (1954) though was the one to develop MBO into a management philosophy (Locke and Latham, 1990).

The second strand begun with the Wurzburg school in Germany in the early 1900s, of which members include Kulpe, Ach, and Watt. Lewin came in the 1920s as a main contributor in experimental psychology whose work influenced the studies of goal setting with an emphasis on the level of aspiration and participation in factory settings (Locke and Latham, 1990).

Another academic influence in experimental psychology was that by Mace (1935), as he was the first to compare the effects of specific, challenging goals with goals of 'do your best', and to compare goal effects in level of difficulty. Mace also argued that incentives such as feedback, supervision, and assigned standards affected performance through their effects on the individual's personal goals (Locke and Latham, 1990).

In order to understand and explain the effect of goals on action, however, it is necessary to understand the mechanisms by which goals produce their outcome. It has to be mentioned though that the category of actions the theory of goal setting is focused on, is performance on work tasks. Locke and Latham (1990) support that the three most direct goal mechanisms are primarily motivational and correspond to the three attributes of motivated action, which are: arousal or intensity, choice or direction, and duration. Goals affect arousal by regulating the intensity of effort individuals spend on a task and

duration by leading people to persist in their actions until the goal is achieved. Goals also affect choice by leading people to direct their attention and take action with respect to goal relevant activities.

However, as tasks become more complex, these mechanisms become progressively less adequate by themselves to ensure goal achievement, while the development of task-specific strategies becomes progressively more important. This indirect effect is primarily cognitive in the sense that a strategy is developed to use the energy-related resources (Earley et al., 1989).

The main assumption of goal setting research though is that goals are immediate regulators of human action although the degree of association between goals and action remains an empirical question because people may, for example, make errors, lack the ability to attain their objectives or have subconscious conflicts that subvert their conscious goals (Locke et al., 1981). For example, this might be the case in dynamically complex task environments such as software development (Rasch and Tosi, 1992).

2.3.2 The importance of goals with respect to work behaviour

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

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

In the first proposition, research shows that when individuals accept an assigned difficult goal task, performance tends to increase. In particular, Locke and Latham (1990) reviewed the results of four meta-analyses including 200 studies of which 90 percent support this proposition with an effect size on performance being approximately 10-15 percent increase as a result of goal level. In addition Tubbs et al., (1993) confirm

the same results while Gellatly and Meyer (1992) demonstrated that self-efficacy perceptions and higher arousal mediated the relationship between goal level and performance. Thus, the assumption is that difficult goals lead to greater arousal, effort and persistence, than do easy goals.

In the second proposition, research shows that when individuals are given goal specificity, task performance tends also to increase. Based on the same four meta-analyses, Locke and Latham (1990) report that over 90 percent of 200 studies support this proposition with an effect size on performance being approximately 8-16 percent increase as a result of goal specificity. In addition, Rodgers and Hunter (1991, 1994) using MBO programs and Pritchard (1995) with his PROMES system confirm also that specific goals have a positive impact on performance.

Although, the results of the above two propositions have been at an individual level, Locke and Latham (1990) based on a review of 41 independent studies on group level found also that over 90 percent of those studies support these two main propositions. 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. Weingart (1992) also asserted that goal difficulty and task component complexity influence group performance by affecting the group members' effort as well as the amount, quality and timing of their planning.

Some recent research results though show that the relationship between goal level-performance may not necessarily hold at a group level. For example, Finnegan (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, while Koskosas and Paul (2003a) report that group size has different impact on the process of goal setting mainly due to differences in the socio-organizational contexts. In addition, Wegge (2000) found moderating effects from participation in goal setting, group cohesion and group conflict. The majority of results, however, show that the two

propositions hold for both individual and group levels in laboratory and field studies as well as in different types of tasks.

Following these trends there is an emphasis in recent years that more research is needed at the macro goal setting level. To this end, this investigation takes a macro-level goal setting point of view and supports that an efficient goal setting process at a group level will improve the process of information systems management in the context of internet banking security. Consequently, the main research question becomes:

1. Do organizations set goals relevant to the management of the integrity, confidentiality and authenticity of information through the internet banking channel?

2.4 Risk Communication in Context

2.4.1 Definition of Risk Communication

Communication, in simple terms, could be described as an interactive process of sending and receiving messages among individuals, groups, and organizations including some form of feedback. Although, there are numerous definitions for the term 'communication', the researcher adopts DeVito's (1988, p.14) definition that covers the essentials of the communication as the act: "*communication refers to the act, by one or more persons, of sending and receiving messages that are distorted by noise, occur within a context, have some effect, and provide some opportunity for feedback*".

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

"*Risk communication is an interactive process of exchange of information and opinion among individuals, groups, and institutions. It involves multiple messages about the*

nature of risk and other messages, not strictly about risk, that express concerns, opinions, or reactions to risk messages or to legal and institutional arrangements for risk management" (NRC, 1989, p. 21).

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 (Krimsky and Plough, 1988).

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

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

2.4.2 The emergence of risk communication

Risk communication emerged from risk perception as the general public concerns about hazards were different to those of the experts, i.e., the scientific and policy making communities (NRC, 1989; Slovic, 1990). The difference, in particular, was that experts tended to focus on measurable, quantified attributes of risks while the public tended to

focus on the qualitative value-laden attributes of risks such as fairness and controllability (Groth, 1991).

Sandman (1987) uses the term 'outrage' to incorporate many of the qualitative dimensions of risks while 'hazard' is the quantitative, measurable aspect of risk. According to him, although the public seems concerned with 'outrage' at the expense of 'hazard', the experts often tend to ignore 'outrage' at their own danger. He also points out that if the public's legitimate concerns are not being addressed by the risk management process, the outrage level will be greater than when the public concerns are taken into consideration.

Thus, risk communication was developed as a way to communicate effectively the experts' assessments of risks to the public so that the public would understand the real nature of risks and at the same time, to diminish the tension among parties with different perceptions of risks (Jaeger et al., 2001). To this end, this investigation recognizes that an efficient communication of risks will be partly affected by a certain (confident) level of risk perception, IT employees may have on security issues.

Risk communication though implies an intentional transfer of information. As such, the specification of what kind of goals and intentions are associated with the risk communication efforts is necessary (Jaeger et al., 2001). Similarly, the National Research Council (1989, p. 10) suggests four key elements to improve risk communication, which are: 1) goal setting, 2) openness, 3) balance, and 4) competence.

1) In goal setting, NCR argues on the necessity to establish realistic, achievable goals and to determine the roles of the recipients of the organization's risk messages and ultimately, to show the contribution to improved understanding of issues and actions.

2) By openness NCR means that organizations, in particular, should communicate in an effective manner about risks with the affected outsiders. To this end, this two-way process should have a sense of open exchange in a common undertaking and an early and continuous interchange including the media and other intermediaries.

3) In order to keep balance and accuracy of risk messages, risk managers should (a) hold the message preparation accountable in order to detect and reduce any distortions, (b) keep a review of the underlying assessment and when possible the message by independent experts, (c) contingent draft messages to outside preview to determine if message receivers detect any omitted distortions, and (d) prepare a report for comment on risk assessment and risk reduction assessment.
4) Finally, risk managers should proceed to the subject matter and risk communication by taking steps to ensure that the preparation of risk messages becomes an intentional competitive undertaking without ignoring scientific quality.

Risk communication should not be viewed as a factor that always reduces conflict or smoothes risk management because management decisions may benefit some but not others (NRC, 1989). Although, effective communication of risks may not always improve a situation, ineffective or poor risk communication will almost always make harm (NRC, 1989).

In the context of goal setting, with regard to information systems security, the message circulated among the members of an IT group is the security goal (Koskosas and Paul, 2003b). At group level, the communication of security goals is not as simple because goals must be communicated to different individuals, in many forms and often over a period of time (Koskosas and Paul, 2003b). Even though goal communication may be effective, it still may not be complete and adequate throughout the organization (Donaldson, 1985).

However, this investigation supports the rationale that an efficient communication of risks, at group level, plays an important role at the level of goal setting with regard to information systems security. Thus, part of this investigation is based on the assumption that an efficient communication of risks:

1) plays an important role at the level of goal setting, in the context of information systems security management, with regard to internet banking.

2.4.3 Contribution/Weaknesses in Prior Research

Prior studies on the adoption of e-commerce have not simultaneously considered risk communication and goal setting as important determinants of internet banking security.

Risk communication between the members of an IT group has not been specifically addressed in the context of internet banking security goal setting. Previous research has mostly dealt with consumers' risk perception as part of the risk communication process. However the relationship between risk communication and goal setting as important aspects of ISs management in the context of internet banking has not been studied, yet.

Finally, the concept of risk communication is undeveloped and further research is needed.

2.5 Culture in Context

2.5.1 Definition of culture

Although relatively new as a concept in organizational behavior, organizational culture is widely referenced in academic literature, and business journals, and has attracted the attention of researchers in recent years. A reason for such interest may be the belief that organizational cultures provide a sense of control, in terms of unifying the way employees process information and behave within the organization, which increases the predictability of organizational behavior (Trice and Beyer, 1993). While measures of organizational cultures and their effects on organizations are considered as highly problematic (Martin, 1992; Alvesson, 1993), many studies support the assumption that culture is a measurable characteristic of organizations (O' Reilly and Chatman, 1996). However, these studies focus on the consequences of organizational behavior and processes rather than interpreting the meaning of different organizational cultures (Sorensen, 2002).

While there are varying definitions of culture, Schein's definition of culture serves as the theoretical "paradigm" for this investigation. Schein (1992) divides organizational culture into three levels: 1) at the surface are "artifacts", which are the visible organizational structures and processes, yet difficult to understand; 2) the second level is the "espoused values", which are the strategies, goals and philosophies of the leadership; 3) the third level, and most important for Schein, is the basic assumptions and values, which includes unconscious beliefs, perceptions, thoughts and feelings of the organization. These basic assumptions form deeper underlying dimensions of organizational culture such as the nature of human relationships and activity, the nature of humans, and the nature of time, reality and truth (see Appendix A1). Moreover, Schein suggests that groups' tasks within cultures are divided into external and internal, as shown in Table 3, below.

External Adaptation Tasks	**Internal Integration Tasks**
Developing Consensus on:	*Developing Consensus on:*
The core mission, functions and primary tasks	The common language
The specific tasks	The group boundaries
The basic means to be used in accomplishing the goals	The criteria for allocation of status
The criteria to measure results	The criteria for friendship
The remedial strategies if goals are not achieved	The criteria for rewards
	Concepts for managing the unmanageable

Table 3 The external and internal tasks facing all groups (Schein, 1990)

2.5.2 The effects of strong cultures

Most of the literature on organizational culture focuses on the hypothesis that strong cultures enhance organization performance (Deal and Kennedy, 1982; Burt et al., 1994). A strong culture can be defined *as "a system of shared values (which define what is important) and norms that define appropriate attitudes and behaviours for organizational members"* (O' Reilly and Chatman, 1996, p.160) and this is the definition of culture strength applied in this investigation. This hypothesis, however, is

grounded on the belief that organizations benefit from having highly motivated employees dedicated to common goals (Deal and Kennedy, 1982; Kotter and Heskett, 1992). Likewise, having widely shared and strongly held norms and values lead to performance benefits such as: enhanced co-ordination and control within the organization, increased employee effort, and improved goal alignment between the organization and its employees (Sorensen, 2002). Thus, a culture can be considered strong if those norms and values, which are at Schein's third level of culture definition, are widely shared and fiercely held throughout the organization (Kotter and Heskett, 1992; O' Really and Chatman, 1996). Deal and Kennedy (1982) though argue that this definition of culture strength does not explain which are those values and norms that might enhance organizational performance.

Strong cultures, however, may not always provide benefits for organizations and this might be the case in organizational learning (Weick, 1985; Schein, 1992). As an example, organizations with strong cultures may not recognize the need for change because such organizations are too focused in understanding the world and thus may be unable to observe changes in environmental conditions. On the contrary, March (1991) suggests that organizations with cultural weaknesses and willingness to learn from their members (cultural exploitation), are better able to understand and cope with any changes in environmental conditions. Similarly, even if organizations with strong cultures are willing to respond to any changes in environmental conditions, the transfer of knowledge and fresh ideas becomes in a rather sluggish way (Tushman and O' Reilly, 1997).

Nevertheless, the majority of research findings support that strong cultures benefit organizations by allowing social control, which may provide an agreement on certain behaviors within the organization; therefore, any possible "breaches" of behavioral norms may be identified and corrected immediately (Kotter and Heskett, 1992). Organizational cultures assist people to make their own interpretations of organizational events and assumptions about organizational processes (Sorensen, 2002). In strong cultures employees are motivated to perform at a high standard, as they feel free to participate in the organization's activities (O' Reilly and Chatman, 1996). In addition, strong cultures provide clarity of goal achievement as well as better co-ordination and control of activities, which in turn, provide a certain course of action by employees on

the organizations' business strategies (Cremer, 1993). When there is clarity of goal achievement, employees feel more certain about the course of action they should follow, whereas goal alignment provides an agreement between different parties about the organization's best interests (Kreps, 1990; Cremer, 1993). Ultimately, in strong cultures employees are motivated to perform at a high standard as they feel their actions are freely chosen (O 'Reilly and Chatman, 1996).

Even though the assumptions of the effects of culture strength have been considered in terms of the content of organizational values and norms (Sorensen, 2002), research findings show also positive evidence of culture strength in terms of the degree of agreement and commitment to organizational values and norms (Kotter and Heskett, 1992). For example, Denison (1990), using both qualitative and quantitative data, found that organizational effectiveness is increased as a result of agreement enclosing organizational values. Burt et al., (1994), using Kotter and Heskett's data, investigated the effect of culture strength on market context and came to the conclusion that the benefit of strong cultures was increased in highly competitive markets. Moreover, in strong culture organizations new members adopt faster to organizational values and norms due to explicit codification of beliefs and to greater normative pressures (Harrison and Carroll, 1991).

Thus, it seems that overall, the assumptions and effects of strong cultures play an important role in the context of goal alignment and clarity of goal achievement within organizations, which indicates the importance of culture strength in setting organizational goals. In the same line of reasoning, culture strength may also play a significant role in the process of goal setting with regard to information systems security in terms of having better control and co-ordination of activities in the context of risk management. Consequently, as culture strength provides better control and co-ordination of an organization's activities, the communication of messages between people and different units within the organization is also likely improve.

To this end, this investigation supports the rationale that a strong culture, at group level, plays an important role at the level of goal setting with regard to information systems security and that, culture strength will provide the conditions under which an efficient

communication of security related risks will occur. Thus, part of this investigation is also based on the assumption that a strong group culture:

1. provides the conditions under which an efficient communication of risks will occur
2. plays an important role at the level of goal setting, in the context of information systems security management, with regard to internet banking.

2.5.3 Contributions/Weaknesses in Prior Research

Prior studies on the adoption of e-commerce have not simultaneously considered culture and goal setting as important determinants of internet banking security.

Although culture has been studied in the context of e-commerce, culture within a different context, that of an IT group, has not been addressed in the context of information systems security goal setting. Previous research has mostly dealt with consumers' culture in e-commerce and culture as an organizational phenomenon. However, the relationship between culture and goal setting as important aspects of information systems security, in the context of internet banking, has not been studied, yet.

2.6 Trust in Context

2.6.1 Definition of Trust

Trust is a social phenomenon although with a multidisciplinary view. Thus, the issue of trust can be categorised based on how trust is viewed in different disciplines along different dimensions. Personality psychologists tend to view trust as an individual characteristic while social psychologists tend to view trust as the behavioural expectation of some parties involved in a transaction (Bhattacharya et al., 1998). Sociologists and economists tend to focus on how institutions are established and incentives are used to reduce uncertainty associated with transactions among relative parties (Bhattacharya et al., 1998; Lewicki et al., 1998). Rousseau et al. (1998) argue that it is necessary to integrate the differing views of trust across disciplines and

consider that trust may be a "meso" concept, which integrates both the individual and institutional level views of trust development.

However, trust is important in a number of different ways as it enables co-operative behaviour (Gambetta, 1998), promotes adaptive organizational forms (Miles and Snow, 1992), facilitates rapid formulation of ad hoc work groups (Meyerson et al., 1996) and promotes effective responses to crisis (Rousseau et al., 1998). In an earlier influential line of 'trust' research, Deutsch (1962) uses the term to refer to co-operative behaviour within groups. Gambetta (2000) argues that the higher the level of trust the higher the likelihood of co-operation, although co-operative behaviour does not depend on trust alone, and the optimal threshold of trust will vary according to the occasion. Although, the more the trustor believes in the goodwill and reliability of the trustee, the more confidence in co-operation he will harbour.

In a similar vein, Currall and Judge (1995) defined trust as an individual's reliance on another party under conditions of risk and dependence. The existence of risk, in particular, is necessary in sociological, psychological and economic conceptualisations of trust (Williamson, 1993). According to Mayer et al. (1995) trust is the willingness to assume risk, while trusting behaviour is the assumption of risk. Thus, a higher level of trust in one party increases the likelihood that one will take a risk with that party (e.g., co-operate, share information) and/or increases in the amount of risk that is assumed whereas, in turn, risk taking behaviour is expected to lead to positive outcomes (e.g., individual, group performance).

The relationship between dependence-trust is also a necessary condition in order to achieve trust, as the interests of one party cannot be achieved without reliance on another (Rousseau et al., 1998). Sheppard and Sherman (1998) argue that although risk and dependence are necessary conditions for trust to be achieved, the nature of risk and trust changes as dependence increases.

Likewise, Rousseau et al. (1998, p.395) based on a "multiplex" point of view suggest that trust is widely defined as: *"trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another"*. Other psychology researchers tend to use slightly different variations of

this definition, operationalizing trust as the "willingness to be vulnerable" (Mayer et al. (1995)), "willingness to rely" on another (Doney et al. (1998)), "perceived probabilities" (Bhattacharya et al. (1998)) and "confidence", "positive intentions/expectations" (Hagen and Choe, (1998); Lewicki et al. (1998); Robinson, (1996); Das and Teng, 1998). In this investigation, the researcher defines trust *as confidence and positive expectations of one party (individual) within an IT group that another party is willing to co-operate in setting efficiently security goals with regard to the management of the integrity, confidentiality, and authenticity of information through the internet banking channel.*

The focus of this investigation is on trust between the members of an IT group is setting efficiently goals with regard to the management of the integrity, confidentiality and authenticity of information through the internet banking channel. The purpose, at one level, is to integrate a particular viewpoint of trust with other socio-organizational aspects such as culture and risk communication, as this investigation takes the standpoint that such aspects and their possible interrelationship with each other might play an important role in the process of goal setting.

2.6.2 The benefits of trust

The issue of trust has attracted particular attention through the years, due to the numerous benefits it offers to organizations (Kramer, 1999). Although, a significant amount of researchers have devoted attention to examining the potential benefits of trust, they have devoted less attention to examining the conditions under which trust provides these benefits (Dirks and Ferrin, 2001). Theorists of trust support the view that trust may work as an independent variable (cause), dependent variable (effect), or interaction variable (moderator) (Rousseau et al. 1998). For example, trust is used as a potential cause in choice scenarios framed around social dilemmas when economic outcomes are expected (Rousseau et al. 1998).

Further, there are two fundamental perspectives that explain how the benefits of trust, emerge. The first perspective explains the effect of trust in a straightforward manner.

That is, trust results in direct effects such as more positive attitudes, higher levels of co-operation, and higher levels of performance (Dirks and Ferrin, 2001). Many studies, in particular, argue that trust determines the performance of a society's institutions and it is a propensity of people in a society to co-operate in order to produce socially efficient outcomes (Coleman, 1990; Gambetta, 1998). Most theories of trust reflect on this idea and on the positive effect of trust on workplace attitudes, behaviours and performance (Mayer et al., 1995; Jones and George, 1998). For example, researchers examined the direct effects of trust on behavioural and performance outcomes such as communication and information sharing, organizational citizenship behaviour, effort, conflict, negotiation behaviours, individual and group performance and found positive effects of trust (Larson and LaFasto, 1989; Smith and Barclay, 1997; De Dreu et al., 1998; Dirks, 1999).

Dirks and Ferrin (2001) though after a review of 29 studies on direct effects of trust on workplace behaviours and performance outcomes found that in many of the outcomes the evidence is less robust. Some studies revealed a significant positive effect while others did not but overall, the results showed that the effects of trust on work behaviours and performance are unlikely to be straightforward.

The second perspective explains the effects of trust in an indirect (moderate) manner. That is, trust provides the conditions under which certain outcomes, such as co-operation, positive attitudes, confident perceptions and higher performance are likely to occur (Dirks and Ferrin, 2001). Although, this indirect (moderate) effect has received less attention than the direct effect of trust, Rousseau et al. (1998) observed that several researchers that investigated the issue of interpersonal trust in work relationships have positioned trust as a moderator.

Dirks (1999) found that trust did moderate the relationship between group members' motivation and group processes and outcomes. More 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. Mishra and Spreitzer (1998) who investigated both the direct and moderate effects of trust on downsizing, found that the remaining employees' behavioural

responses will be determined directly by trust as well as by the interaction of trust with empowerment and work design.

Likewise, Heide and John (1992) argue that without a minimum level of trust, it is very difficult to agree on goals, to impose rules, and to conduct teamwork. They further supported that having a confident level of trust an effective control is more likely to occur, as individuals understand each other better and are more willing to exercise mutual clemency.

In line with the research findings on trust, this investigation supports the rationale that a high level of trust, at group level, plays an important role at the level of goal setting with regard to information systems security. Considering also that the higher the level of trust, the higher the likelihood that one individual is likely to co-operate and share information, which are partly characteristics of a strong culture and communication, this investigation supports further that trust has an indirect (moderate) effect. In doing so, trust will provide the conditions under which a strong culture and an efficient communication of security risks are likely to occur. Thus, part of this investigation is based on the assumption that a high level of trust:

1. provides the conditions under which a strong culture and an efficient communication of risks will occur
2. plays an important role at the level of goal setting, in the context of information systems security management, with regard to internet banking.

These assumptions are based on the idea that trust has an indirect effect by causing various possible determinants of work group behaviour to achieve a strong group culture and an efficient communication of security risks. Micro-theorists of workplace behaviour suggest that work behaviour is caused by needs, goals, or incentives (Kanfer, 1990), while macro-theorists of work behaviour focus on determinants such as roles, rules, structure, culture and norms (Perrow, 1986). However, Dirks and Ferrin (2001) suggest that trust should be viewed as an influence to the type or degree of behaviour that such determinants result in, as it makes possible to assess the potential behaviour of two or more parties that depend on each other.

2.6.3 Contribution/Weaknesses in Prior Research

Prior studies on the adoption of e-commerce have not simultaneously considered trust and goal setting as important determinants of internet banking security.

Although trust has been studied in the context of e-commerce, trust among the members of an IT group has not been specifically addressed in the context of information systems security goal setting. Previous research has mostly dealt with consumers' trust in e-commerce and trust as a social phenomenon. However the relationship between trust and goal setting as important aspects of ISs management in the context of internet banking has not been studied, yet.

Finally, the broader theoretical issues of how trust may have a moderating role have received little attention.

2.7 The Concept of Goal Commitment

2.7.1 A definition of goal commitment

The major finding in goal setting research is that difficult goals lead to higher performance levels than do easy or vague goals (Locke et al., 1981). This finding though depends on the assumption of commitment to those difficult goals. Locke et al., (1988, p.23) state that *"it is virtually axiomatic that if there is no commitment to goals, then goal setting will not work"*. Thus, goal commitment is a key factor in producing positive performance and commitment needs to be high.

Locke and Latham (1990) further argue that it is difficult to demonstrate the effect of goal commitment on performance because in the majority of studies goal commitment has been easily achieved. They support that a small amount of variability that has been found was, in most of the cases, unrelated to performance. Similarly, the relationship between commitment and performance may be negative, when multiple goal levels are used (Locke et al., 1984).

According to Locke et al., (1981) commitment is the determination to try for a goal and the persistence in pursuing it over time. In this investigation, the researcher defines commitment as *a state of mind that holds individuals and organizations in line of behavior* (Staw, 1982*) and encompasses psychological factors that force individuals to take action* (Kiesler, 1971).

Moreover, the relationship of commitment to performance is well documented by two main propositions. First, if the goal level is held constant or if individuals are given the same challenging goal, commitment could have a direct, positive effect on performance. Wright (1989), for example, found both direct and indirect positive effects of commitment on performance while Locke et al., (1994) found a significant relationship between commitment and performance even when the personal goal level was controlled. This positive relationship applies to difficult assigned goals, while for easy goals it may be negative since those with low commitment to easy goals may set higher goals for themselves. Those with high commitment to easy goals would stop when the goal is attained (Locke and Latham, 1990).

The second proposition argues that when the goal level differs among individuals, commitment could moderate the goal effect on performance. Wofford (1992), for example, found that in a high-commitment condition the discrepancy between goal-performance was smaller in subjects with medium to high goals, than in a low-commitment condition. He also found that high commitment was best predicted by task difficulty, the intention to which individuals felt they could attain the goal and their actual expectation of goal attainment. Thus, the relationship between goal level and performance is stronger with high commitment than with low commitment.

In line of the research findings, so far, the assumptions and possible relationships between different socio-organizational aspects can be illustrated into a model. Figure 3, shows a synthesis of such aspects into a model named, the performance pyramid model. At the first level of the pyramid lies the level of trust. Trust is at the first level due to the assumptions earlier made in this dissertation, specifically, that a high level of trust will (moderate) provide the conditions under which a strong culture and an efficient risk communication are likely to occur. Also, the model shows that the ultimate role of trust will be at the level of goal setting, as the importance of trust in setting goals has been

previously aforementioned. In this dissertation, the "level of goal setting" is frequently used to denote the stage at which a group or team, is about to start the implementation of goals.

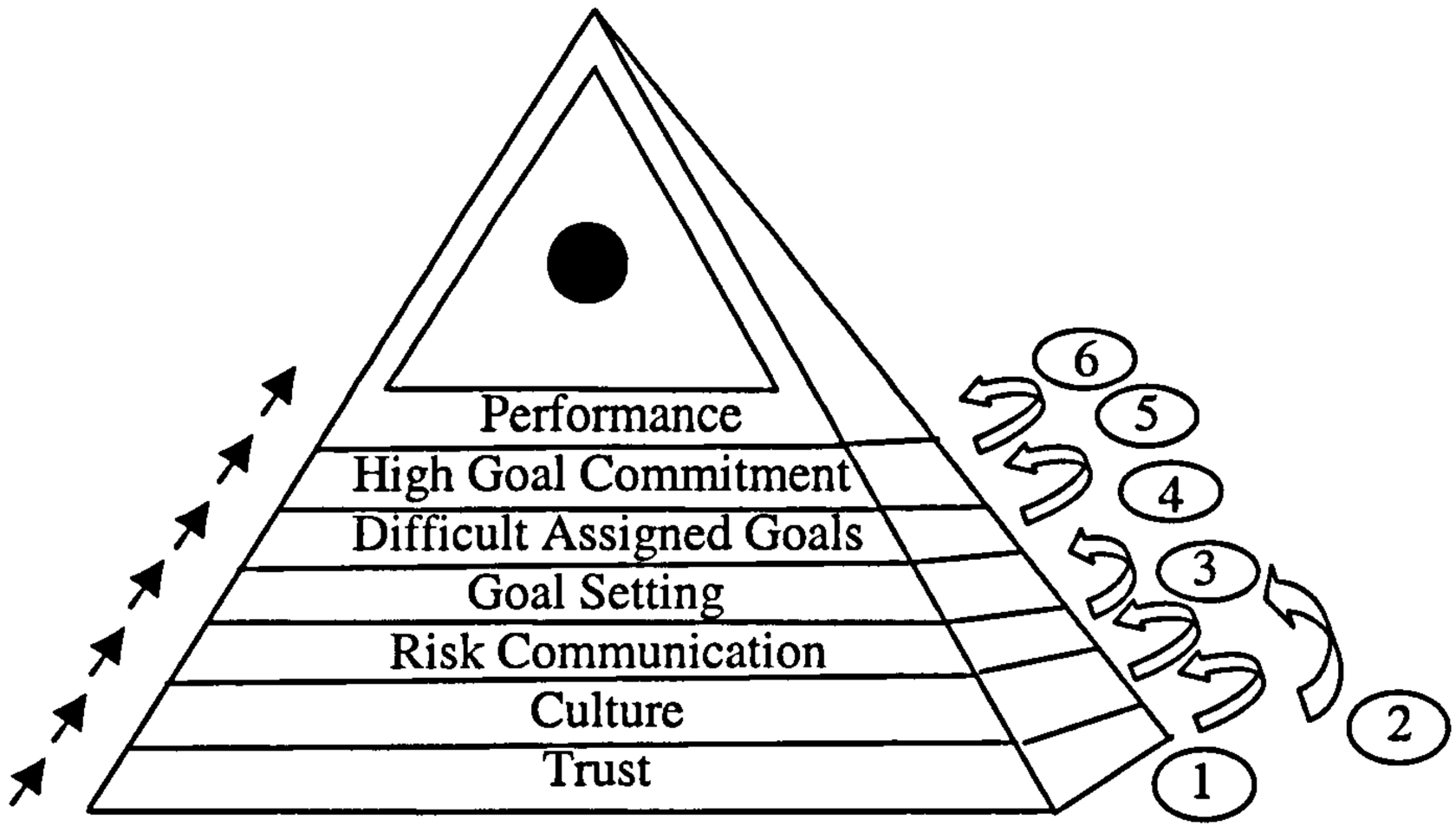


Figure 3 The Performance Pyramid Model (PPM)

At the second level is culture, and denotes its importance in providing the conditions under which an efficient communication of risks, in the context of information systems security, is likely to occur. The model shows also the twofold role of culture strength in having an important role at the level of goal setting.

Risk communication is at the third level of the pyramid, and shows its important role in goal setting. These social organizational aspects are depicted at different levels in the performance pyramid model because they show the different roles they might play at the level of goal setting and due to the rationale and assumptions made about their possible interrelationship. The arrows also indicate the direction of the social organizational aspects towards the upward levels of the pyramid until performance is achieved.

The second part of the pyramid, shows that when the goal level is held constant, if individuals are assigned specific, difficult goals (given goal acceptance), individuals' commitment to goals tends to increase (Locke et al., 1981). In the same line of

reasoning, as the goal level, commitment and performance have a complex relationship including both direct and moderate effects, the performance tends to increase if commitment is high and the goal level constant (Latham and Locke, 1991). The rationale for using this research findings however is that, if individuals within an IT group are given specific security goals, their commitment will increase and consequently the performance of the group. However, in order to have an efficient and constant level of goal setting, the previous socio-organizational aspects of the pyramid model such as trust, culture and risk communication must be given priority. In other words, their overall effect is important at the level of goal setting with regard to information systems security management.

However, Locke and Latham (1990) argue that as there is indeed a relationship between goal level and performance, it is important to understand the determinants (factors) that may influence commitment. Although, the relationship between goal level, commitment and performance is out of the scope in this dissertation, the scope indeed is to investigate if there are any determinants of commitment, at group level, with regard to information systems security management. Thus, this investigation aims to:

1. Identify if there are any determinants of commitment at group level with regard to information systems security management.

Locke and Latham (1990) have made an attempt to identify the determinants of commitment at an individual goal level. These are included in Table 4 and although they are applied at a micro (individual) level, some of them could also be applied at a macro (group) level as a group is consisted by a number of individuals. The determinants are mainly divided into two categories: 1) factors that affect perceived desirability or appropriateness of trying for a given goal, and 2) factors that affect perceived capability of attaining a given goal.

In the first category, the main principle of the factors is that they cause the individual to believe on the importance of the goal and to eliminate any possible conflict between goals. Authority, for example, was found to be one of the most significant determinants of commitment while peer group influence, in terms of group cohesion, facilitates commitment to achieve higher group performance (Locke and Latham, 1990).

Similarly, in the second category the main principle behind the factors is that they cause individuals to believe they can reach the goal. Goal difficulty, for example, is believed to have a significant effect on commitment through expectancy and self-efficacy (Locke and Latham, 1990).

FACTORS AFFECTING PERCEIVED DESIRABILITY OR APPROPRIATENESS OF TRYING FOR A GIVEN GOAL OR GOAL LEVEL	
Authority	- communicates legitimacy - implies rewards and punishments - conveys self-efficiency information - conveys normative information - fosters sense of achievement - implies opportunities for self-development - poses challenge to prove self - maintains physical presence - furnishes support - exhibits trustworthiness - provides rationale - exerts pressure - is knowledgeable and likable
Peer Group	- exerts pressure - provides role modeling - presents competition
Publicness Incentives and Rewards Self-rewards Punishments Valence and instrumentality Ego involvement Conflict Satisfaction Personality Goal intensity	
FACTORS AFFECTING PERCEIVED ABILITY OF ATTAINING A GIVEN GOAL OR GOAL LEVEL	
Expectancy, Self-Efficacy, Task Difficulty Authority- self-efficacy information, trust Role Models- (same as authority) Competition Attributions Goal intensity	

Table 4 Factors Affecting Goal Commitment, (Locke and Latham, 1990)

2.7.2 Commitment on IS projects

Commitment is also necessary for the successful development of information systems projects (Markus, 1981; Kwon and Zmud, 1987) as it boosts an organization's effectiveness by dedicating the right resources to IT investments (Weill and Olson, 1989). By contrast, lack of commitment may even cause a project to be abandoned (Ewusi-Mensah and Przasnyski, 1991; 1994; 1995).

Although, commitment is necessary for successful project outcomes, managers may invest sometimes more resources than necessary to an IS project if they think the project is about to fail (Neumann, 1994). This might be the case, for example, with individuals who have a high level of personal responsibility for a failing project (Staw and Ross, 1987). Similarly, projects may fail if commitment is too sluggish or if the champion of the project decides to depart before project completion time (Reich and Benbasat, 1990).

However, when managers are too committed in investing the organizations' resources into failing projects, this is the so-called phenomenon of escalation of commitment (Staw, 1981). According to Staw and Ross (1987) the escalation of commitment is characterised by three main features: costs of investing additional resources into a certain course of action, opportunities for withdrawal, and uncertainty about the consequences of persistence and withdrawal.

Davis and Bobko (1986) used the theory of self-justification to explain the escalation of commitment effect and found that when managers have to choose among project withdrawal, project modification, or project persistence, they are likely to choose the last option. Similarly, Brockner (1992) argues that the self-justification theory results in managers refusing to admit an incorrect decision originally taken on a project and thus, they keep investing in the project in the hope of ultimate success. Other theories that were used to explain the escalation of commitment effect include the expectancy and self-presentation theories (Brockner, 1992), prospect theory (Garland, 1990), and decision dilemma theory (Bowen, 1987).

However, Ross and Staw (1987) in an attempt to identify the determinants of commitment to IS projects have taxonomized them into four categories (see Appendix A2). The first category is *project determinants* whose focus is on the objective features of projects and reflect their costs and benefits (Brockner, 1992). Examples include large payoffs, large closing costs, or ambiguous performance data. The next category is *psychological determinants*, which emanate from an individual's personality and affect his/her beliefs about the consequences of a possible action. For example, a manager may be emotionally detached with a project and continue to support the project even after his departure (Newman and Sabherwal, 1996). *Social determinants* emanate from group values and affect the individual's decision to a certain course of action (Brockner, 1992), while *structural determinants* represent the contextual conditions surrounding the project (Newman and Sabherwal, 1996).

2.7.3 Contribution/ Weaknesses in Prior Research

Prior studies on the adoption of e-commerce have not simultaneously considered commitment and goal setting as important determinants of information systems security management.

Although commitment has been studied in the context of IS project development, commitment to security management goals has not been specifically addressed in the context of internet banking.

The determinants of commitment at group level with regard to information systems security management have not been investigated yet.

2.8 A Synthesis of Social Organizational Concepts into PPM-model

Following the trends over the last few years on the approaches developed in the context of information systems security (ISs), it is obvious that these approaches lag behind in terms of defining the social organizational aspects of security risks. Although, the value of these approaches is evident, they tend to focus on narrow, technically oriented solutions and they ignore the social aspects of risks and the informal structure of organizations.

To this end, this investigation adopts a socio-organizational approach to IS security management and suggests the performance pyramid model which is mainly based on the concept of goals. The model can be used by IT (security) managers and groups to improve the efficiency of the goal setting process and consequently their performance in managing effectively information systems security in the context of internet banking.

On the basis of the performance pyramid model, shown in Figure 3, is the level of trust, which denotes its importance in relation to the next socio-organizational aspects. The investigation in this dissertation supports the assumption that trust has a moderate role, that is trust:

1. provides the conditions under which a strong culture and an efficient communication of risks will occur.
2. plays an important role at the level of goal setting, in the context of information systems security management, with regard to internet banking.

This rationale, however, is based on the idea that trust has an indirect (moderate) role by causing various possible determinants of work group behaviour to achieve a strong group culture and an efficient communication of security risk messages.

At the second level of the performance pyramid model is the level of culture. Having discussed the effects and assumption of strong cultures, in section 2.5.2, the investigation in this dissertation supports the assumption that a strong culture:

3. provides the conditions under which an efficient communication of risks will occur.

4. plays an important role at the level of goal setting, in the context of information systems security management, with regard to internet banking.

Risk communication is at the third level of the performance pyramid model. The definition of risk communication is based on US National Research Council (1989, p.21) definition as "an interactive process of exchange of information and opinion among individuals, groups, and institutions. It involves multiple messages about the nature of risk and other messages, not strictly about risk, that express concerns, opinions, or reactions to risk messages or to legal and institutional arrangements for risk management". Thus, this investigation supports that an efficient communication of risks:

5. plays an important role at the level of goal setting, in the context of information systems security management, with regard to internet banking.

Having discussed the rationale and assumptions of trust, culture and risk communication at the goal setting level, this investigation seeks further to identify if there are any determinants of trust, culture, and risk communication so that the performance pyramid model suggested in this dissertation can be practically used. Thus, this investigation intends also to identify:

6. if there are any determinants of trust, culture and risk communication.

The importance of goal setting as a process for the selection and implementation of security controls has been discussed, in section 2.3.2. The performance pyramid model further asserts that in complex task environments, such as risk management, if people are assigned specific, difficult goals (given goal acceptance), people's commitment to goals will increase (Locke et al., 1981). In the same line of reasoning, as the goal level, commitment and performance have a complex relationship including both direct and moderate effects, performance tends to increase when the goal level is held constant and commitment is high (Latham and Locke, 1991).

However, the relationship between goal level, commitment and performance is not in the scope of this investigation. The ultimate scope is indeed the identification of any

possible determinants to commitment, at group level, with regard to information systems security management. Thus, this investigation intends to identify:

7. if there are any determinants of commitment at group level with regard to information systems security management.

2.8.1 Collectivist and individualistic patterns

Locke and Latham (1990, p.153) assert that goals can be set in at least three ways: either they can be assigned, they can be set participatively, or they can be self-assigned. To this end, the way goals are being set may have a different impact in societies or organizations with different culture in terms of whether the society/culture is individualistic or collectivistic.

Individualism/collectivism concerns the relationship between the individual and the group with the two values usually presented in the literature as representing opposing ends of one dimension.

Individualists cultures are those where *"individuals are loosely connected, and everyone looks after their own interests or those of their immediate family"* (Hofstede, 1994, p.132). However, individuals have personal goals that may not extent with those of their in-groups and if there is a conflict they put their personal goals first (Singelis et al., 1995). People in individualistic societies feel autonomous and members of these societies emphasise the 'I' and 'this interests me' (Triandis, 1995). In such cultures, the stress is on individuals' goals while motional dependency is emphasised and people prefer a loosely-knit social framework.

Collectivism refers to the opposite pattern, representing cultures *"in which people from birth onwards are integrated into strong, cohesive in-groups, which throughout people's lifetime continue to protect them in exchange for unquestioning loyalty"* (Hofstede, 1994, p133). In collectivist societies the group is important and there is a need for group solidarity and shared activity (Hui and Triandis, 1986). Members of

these societies emphasise the 'we' and obligations and duties can override personal preferences (Triandis, 1995). While collectivist societies are keen to protect and help their in-group members they are not necessarily much helpful to people outside this group. Group boundaries are explicit and firm with collectivism representing an 'in-group egoism' (Hofstede, 1994).

Table 5 depicts some examples of individualism/collectivism in different countries across the globe. For example, Greece, Great Britain, and the United States rate individualism highly, while Asian, Latin American and African nations are more collectivist.

	Individualism - Collectivism	**Power Distance**	**Masculinity versus Femininity**	**Uncertainty Avoidance**	**Confucian Dynamism**
HIGH	USA	Malaysia	Japan	Greece	China
	Australia	Guatemala	Austria	Portugal	Hong Kong
	Great Britain	Panama	Venezuela	Guatemala	Taiwan
LOW	Panama	Denmark	Netherlands	Denmark	Philippines
	Equador	Israel	Norway	Jamaica	Nigeria
	Guatemala	Austria	Sweden	Singapore	Pakistan

Table 5 Top three and bottom three scores on Hofstede's (1994) cultural dimensions

However, when a group of people belongs either to the individualism or collectivism paradigm, it makes a fundamental consideration from the social sciences point of view since this may cause discrepancy on the level of goal setting and on how people communicate with each other. Erez (1986), for instance, conducted some case studies in Israel, which is a collectivist society and found that participation in goal setting is more effective than assigned goals as compared to United States of America. Erez (1986) found also that assigned goals produced higher commitment and performance in the private sector than did produce in trade unions and commune.

The investigation in this dissertation, as will be explained in chapter 3, adopts a case study approach within the IT departments of three financial institutions in Greece mainly due to the investigator's availability of access. Greece based on Hofstede's cultural dimensions belongs to the individualism paradigm. Although, it is not in the scope of this research to examine the effect of goal setting to different societies, it is

important to mention that the results obtained from the case studies may have different effect to societies with different socio-organizational context.

2.9 Summary and Discussion

The chapter began with a definition of risk from the social sciences point of view. Social theories of risk provide both an individualist and contextualist interpretation to risk events. Individualism analyses the thoughts and acts of an individual while in the case of contextualism, the culture, organization and lifestyle, are more important than the individual himself. However, the researcher defined risk within the contextualism paradigm *as a failure to obtain some or all the goals that are relevant to the management of the integrity, confidentiality and authenticity of information through the internet banking channel.*

The chapter then discussed risk analysis and assessment as one of the most influential tools for the design of security mechanisms and whether or not risk assessment should be isolated from risk management. As concluded, there is no widely accepted theory of isolation or integration of risk assessment from the risk management process, although traditionally linear approaches to understanding risk management have prevailed reflecting the isolation of risk assessment from risk management activities.

Next, the theory of goal setting was introduced and its importance with respect to work behaviour was discussed. The importance of goals to work behaviour is well documented by two main propositions: 1) increases in the difficulty of assigned goals (given goal acceptance) lead to increases in performance, and 2) specific, difficult assigned goals result into higher performance than instructions of 'do your best' or no assigned goals. The majority of research reported support both of these two propositions.

The chapter then introduced the concept of risk communication and it was argued that an efficient communication of risks should not be viewed as a factor that always reduces conflict or smoothes risk management because management decisions may

benefit some but not others. Although, effective communication of risks may not always improve a situation, ineffective or poor risk communication will almost always make harm.

Culture was defined based on Schein's three cultural dimensions and the effect of strong organizational cultures was discussed, in section 2.5.2. Strong cultures provide enhanced co-ordination and control within organizations, increased employee effort, and improved goal alignment between the organization and its members. In addition, strong cultures benefit organizations by allowing social control, which may in turn provide an agreement on certain behaviours within the organization.

Similarly, the concept of trust and its significant role in work relationships was also discussed. As argued, trust has multiple benefits for organizations such as more positive attitudes, higher levels of co-operation and higher levels of performance. As a result, trust was based on the first level of the suggested performance pyramid model to denote the priority of its importance in relation to the other socio-organizational aspects.

Section 2.7 discussed the concept of goal commitment and its determinants both on a micro/macro level and on IS project development. Commitment was defined as a state of mind that holds individuals and organizations in line of behaviour and encompasses psychological factors that force individuals to take action. Further, the relationship of commitment to performance was documented by two main propositions: 1) if the goal level is held constant or if individuals are given the same challenging goal, commitment could have a direct positive effect on performance, and 2) when the goal level differs among individuals, commitment could moderate the effect of goals on performance. That is, when the goal level is held constant, high commitment will increase performance. The majority of the research reported supports both of these propositions.

At last, section 2.9 introduced a synthesis of the socio-organizational aspects illustrated in the performance pyramid model, and summarised the rationale and assumptions of this investigation.

Chapter 3: Research Methodology and Design

3.1 Introduction

This chapter describes and discusses the methodological as well as philosophical assumptions underlying the research approach chosen for the nature of this particular investigation. Burrell and Morgan (1979) and Walsham (1993) argue that it is necessary to understand the theoretical concepts used as a basis of a methodology approach as it would allow researchers to indicate the philosophical assumptions lying behind the chosen approach.

To this end, a qualitative research approach having philosophical foundations mainly in interpretivism, was deemed the most appropriate for this investigation. A multiple case study approach was employed. In all cases, data was collected through a variety of methods including interviews, archival documents, and observation. The use of multiple collection methods makes triangulation possible and this provides stronger substantiation of theory (Eisenhardt, 1989).

The research in this dissertation analyses information systems security from a social sciences point of view and argues that security risks may *arise from failure to obtain some or all the goals that are relevant to the management of the integrity, confidentiality and authenticity of information through the internet banking channel.* Hence IT managers and groups through an efficient level of security goal setting will determine the level of security to be implemented.

The chapter begins by examining the extent to which IS security research approaches have been studied. Then, it discusses qualitative research within the IS literature and explains the rationale for choosing an interpretive approach for the particular nature of this investigation and the philosophical assumptions that lie beneath the research design. That will provide a deeper understanding of the chosen methodology as compared to other methodological approaches within the IS security literature.

3.2 Research in Information Systems Security

This section discusses existing research in information systems security and identifies key characteristics of particular research approaches. The aim is to justify the chosen research approach for the purposes of this investigation in relation to other approaches in information systems security literature.

Various approaches to information systems security have been developed, ranging from checklists, evaluation methods, and risk analysis to more recent approaches based on social organizational perspectives. These approaches are reviewed in the following sections.

3.2.1 Security within the Positivist Paradigm

Checklists

Checklists are one of the most widely used methods for addressing information systems security (Backhouse and Dhillon, 1996; Dhillon and Backhouse, 2001). They are designed to cover all possible threats to a computer system and to identify the existence of possible controls to be implemented. Checklists are based on the idea of "what can be done rather than what needs to be done" (Baskerville, 1993) and examples include disaster recovery planning, access and change controls, encryption, contingency planning and physical security (i.e., IBM (1972); SAFE Checklists (Krauss, 1980); Computer Security Handbook (Hutt et al., (1988); AFIPS Checklist for Computer Centre Self-Audits, (1979)). Although, AFIPS Checklists address similar issues to other checklists, they incorporate threats and related defences into a 'core' style framework (Baskerville, 1993), and are used towards computer audit centres (Dhillon and Backhouse, 2001).

Powell and Klein (1996) argue that checklists are barely related to human expertise and are used as a basis for risk identification. Although, the value of checklists is evident, checklists by nature focus exclusively on procedures and ignore the social aspects of risks, leading to analytical instability (Dhillon, 1995).

Risk Analysis

As discussed in Chapter 2, risk analysis methods attracted the interest of many researchers some of which include Parker's programme (1981), Fisher's methodology (1984), Krueger's (1993) 'functional control matrix' for risk assessment, or Birch and McEvoy (1992) with Structured Risk Analysis methodology. These methods are based on the belief that if countermeasures are developed and implemented in a logical (i.e., mathematical) sequence it would be possible to develop secure information systems. Most risk analysis approaches are statistical and scientific in nature and apply methodologically structured steps. As an example, Birch and McEvoy (1992) with the use of Structured Risk Analysis methodology define information systems in terms of data structures, data processing and system events. The main principle is to see the correspondence between threat and vulnerability.

Other risk analysis approaches include those by Loch et al., (1992) who developed a four-dimensional IS security model focusing on threat identification and Von Solms et al., (1993) who used risk analysis to develop a 'process approach' to information systems security management.

Baskerville (1988) based on DeMarco's structured systems analysis and specification approach suggests that structured security analysis and design methodology can be applied in a similar way as a structured systems analysis. He actually attempts to accomplish controls in the logical design phase of an information system by the use of formal heuristics.

However, a number of automated risk analysis packages have been emerged through the years. RISKPAC (Computer Security Consultants, 1988), which seeks to provide a balance between qualitative and quantitative risk analysis, is based on a questionnaire system that calculates annualised loss expectancy on the basis of simple if-then logic. CRAMM (CCTA Risk Analysis Management Methodology) and MARION are based on data of previous insurance claims from which logical deductions occur through a relational database (Birch and McEvoy, 1995). PARA (Practical Application of Risk Analysis) is also used to implement risk management techniques which are proven to be beneficial to organizations in terms of costs. It

allows the evaluation of applications or systems and whether or not risk analysis should be applied.

The majority of risk analysis approaches are based on the same philosophical ground and focus on the quantification of risks rather than on a more holistic approach.

Evaluation Methods

Another category in information systems security is evaluation methods which are used to measure security effectiveness by levels of security implementation. Early work on establishing various levels of security implementation was sponsored by the US Department of Defence to prevent unauthorised access and disclosure of information. The most widely used model among others was the Bell La Padula Model (Bell and La Padula, 1976) which is a rational method with a discretionary access control used to prevent illegal disclosure of information.

After the introduction of La Padula model, other evaluation approaches and criteria were also developed such as the ITSEC, TCSEC and BS7799. ITSEC (Information Technology Security Evaluation Criteria) was the result of an attempt to balance information systems security standards across Europe and in 1990 the first draft was issued called the 'White Book'. However, the 'White Book' has drawn criticisms as it fails to take a holistic viewpoint of the organization as it is extremely static (Dhillon and Backhouse, 2001). TCSEC (Trusted Computer Systems Evaluation Criteria) provide an evaluation form of criteria to computer vendors in order to develop trusted computer systems while BS7799 (British Standard) is being used to address security management issues in organizations.

Similarly, Chokani (1992) proposes the INFOSEC (Information Security) approach which is based on an improvement of TCSEC criteria although the approach itself distinguishes the technical from the organizational context as it is discrete event-oriented. SECURATE was also another evaluation tool developed by Hoffman et al.,

(1978) which is actually a design and selection process. The approach uses fuzzy set theory and criticises the statistical validity of fuzzy metrics.

Although, the evaluation approaches and techniques have worked adequately for the US Department of Defence, they have limited application to commercial environments because they were developed for a military organization and business organizations represent a different reality when it comes to compatibility and coherence concerns (Dhillon, 2001). Therefore, the characteristics of these prevailing approaches do not offer sufficient solutions to effectively address the security of information systems.

3.2.2 Security within the Interpretist Paradigm

Some new research directions consider the use of traditional interpretive social theories in information systems security. For example, Willcocks and Margetts (1994) developed a framework based on Pettigrew's contextualism, which underlines the importance of social and qualitative aspects of information systems security. Although, contextualist research is useful in understanding the historical and cultural events, it fails to explain the reasons for why these events occur (Murray, 1989).

As mentioned in Chapter 2, risk analysis and assessment have been some of the most influential tools for designing security mechanisms. However, Baskerville (1991) and Beck (1992) believe that although risk analysis is beneficial when used for predictive modelling, over-reliance on it as a technique for information systems security design may have also some negative consequences. Baskerville (1991), for example, argues that risk analysis is subjective in nature and thus subject to social misuse. He further argues one of the weaknesses of the risk analysis method is that the probability calculation can be meaningless if the original estimates are incorrect while it should be used as an effective communication tool between security and business management professionals.

In a similar vein, Straub and Welke (1998) even though they suggest the use of an earlier generation of tools and techniques such as risk analysis, they adopt an interpretive research approach as the mode of analysis to develop managerial guidelines for coping with systems risks. They position the use of risk analysis within the scope of an organization and suggest merging the earlier approaches with the 'threat tree analysis'.

Backhouse and Dhillon (1993; 1994; 1996) have also followed an interpretive approach to information systems security using semiotics and communication acts and they argue that security breaches occur when communication breaks down. They analyse communication break downs by looking on the 'informal' side of organizational actions and they are interested in finding out what happens rather than what should happen.

Generally speaking, the interpretivist approaches to information security assume the organization as an 'agent' or 'culture' as opposed to 'structure' (Hirschheim and Smithson, 1988). Dobson (1991) and Strens and Dobson (1993) provide explanations of peoples' roles, actions, goals and policies. To this end, they argue that an ideal security policy should clearly define the responsibilities of different stakeholders within the organization.

3.2.3 Security within the Use of Critical Theory

Critical social theory is a school of thought, which focuses on the improvement of human conditions. It is an alternative approach to information systems research within the interpretive paradigm (Ngwenyama, 1991). The primary difference though between traditional social theory and critical social theory, is the researcher's attitude towards the world and his work. In traditional social theories, the emphasis is in understanding and preserving the status quo while critical social theories seek to change the status quo. Further, critical social theories focus on the emancipation of

individuals whilst rejecting the disconnection of value and inquiry (Ngwenyama, 1991).

Various researchers that used concepts based on this paradigm include but are not limited to, Lyytinen and Klein (1985), Lyytinen and Hirschheim (1989), Ngwenyama (1991), Ngwenyama and Lee (1997). For example, Lyytinen and Hirschheim (1989) adopt Habermas' social action theory to understand and describe information systems. Habermas (1972) suggested that a critical approach with a broad notion of rationality is necessary in order to maximize society's benefits of technological advancements. Habermas (1987) classified human inquiry into three knowledge interests: technical, practical, and emancipatory. Technical knowledge concerns the human need for understanding the natural and social world, practical knowledge focuses on understanding social forms of life, traditions, social behaviour and relations while emancipatory is concerned with the freedom of physical and mental restraints (legal, social, political, intellectual or moral).

Social critical theory though is not a research methodology in terms of how to do research but rather it is being used to emphasise the role of interpretive and hermeneutic methods in social research content (Lyytinen and Klein, 1985).

Although, social critical theory is not very popular within the context of information systems security there have been a few attempts in recent years to extend its possible use. For example, Webler et al., (1992) use critical theory to locate the activities of risk identification and risk assessment in the context of social theory and provide normative directions to correct possible deficiencies intrinsically associated with such activities. Angell (1994; 1996) has also criticized positivist approaches to security on the basis of 'profound uncertainty', 'sheer complexity', and 'linear thinking' and that logic, rationality and technology lead to the alienation of humans.

3.3 Qualitative Research in Information Systems

The ontology of this research with regard to security is that, security should not be treated as something tangible and concrete but also as a social, organizational issue. To this end, a qualitative research approach was selected for the particular needs of this investigation. Miles and Huberman (1994) describe qualitative research as research based on words rather than numbers. Qualitative research approaches study things in their natural environment and provide an understanding of people's idiosyncrasies and the social and cultural context within which they live (Myers and Avison, 2001). Examples of qualitative methods include action research, case study research, and ethnography while qualitative data sources include observation and participant observation, text documents, interviews, and questionnaires and the researcher's feelings and reactions.

The types of research that a qualitative research approach would be appropriate is well documented by Marshall and Rossman (1999), as it follows:

- Research that examines in-depth complexities and processes
- Research on little-known phenomena or innovative systems
- Research that seeks to explore where and why policy and local knowledge and practice are at odds
- Research on real, in relation to stated, organizational goals
- Research on informal and unstructured linkages and processes in organizations
- Research for which relevant variables have yet to be determined
- Research that cannot be carried out experimentally for practical or ethical reasons

This investigation can be categorised as research that studies in-depth the complexities of different socio-organizational aspects in the goal setting process within the context of information systems security management.

The reason that qualitative research approaches are gaining ground may be attributed to three particular benefits they offer (Benbasat et al., 1987, p.371): First, the researcher can study information systems in a natural setting, learn about the state of the art, and generate theories from practice. Second, a qualitative research approach

provides an understanding of the nature and complexity of the processes involved. Third, it provides the ground for research in areas in which few previous studies have been carried out.

Qualitative research, however, has also a number of problematic characteristics. For example, Smithson and Cornford (1996) argue that there are some particular drawbacks to qualitative research. When the research is focused on small number of cases (e.g., single-case study) it becomes difficult to generalise in a wider context. Similarly, as the data is rich and complex, it is faced with a number of interpretations, whereas the researcher bias is under constant threat. In addition, researchers involved in dynamic cases that change frequently (e.g., goal setting), face problems in trying to make controlled observations, controlled deductions (e.g., using mathematical and statistical methods) and predictions. In effect, these cause problems to the validity and verifiability of the research.

In a similar vein, Miles and Huberman (1994) argue that qualitative research approaches entail some problematic characteristics, in terms of qualitative data, which distinguish them from quantitative ones. In particular, qualitative data is based on documents with a textual richness which can be lost at the stage of aggregation or summarisation. As time observations continue in the long-term, data may become obsolete and longitudinal as well as unstructured and unlimited since it concerns human behaviour in terms of their perception about phenomena. Likewise, Lee (1991) argues that qualitative analysis is problematic in nature due to lack of control, enhanced generalisations as well as deduction and repetition of results.

However, having considered the advantages and disadvantages of a qualitative research approach, this investigation employed a qualitative approach because it allows the in-depth study of the complexities of different socio-organizational aspects of the process of goal setting within the context of information systems security management. The research reported in this dissertation has used a cluster of different socio-organizational aspects, which can be part of a broader theory or the establishment of a cluster of relationships, whose effect can be illustrated in the form of a model. Likewise, the research attempts to make generalisations by drawing on specific implications for information systems security from a socio-organizational

point of view. The use of empirical data will provide rich insights about a wide range of different topics such as trust, culture, risk communication, goal setting and commitment in the context of IS security management. Ultimately, the use of data triangulation, as it is discussed in section 3.5.4, will provide the validity and reliability of the research findings required.

3.3.1 Justification for choosing an interpretive epistemology

The term interpretivism is defined as "studies that assume that people create and associate their own subjective and intersubjective meanings as they interact with the world around them" (Orlikowski and Baroudi, 1991, p.6). That actually means, interpretive studies seek to understand the actual, relativistic meaning of phenomena in terms of the meaning people assign to them.

There were four fundamental motivations for adopting an interpretive approach to this investigation. First, and perhaps the most important, interpretive research could provide an understanding of social factors inherent in IS security goal setting as it focuses on human thought and action in socio-organizational contexts. In fact, many theorists argue that information systems are social systems (Land, 1992; Laudon and Laudon, 1996; Lee and Liebenau, 1996). This line of argument draws credence from the work of those who equate an information system to an organization, i.e. information systems are essentially social systems (e.g. human-computer interaction) and there is an increasing need to understand the social and organizational issues that play an important role in implementing and selecting information systems (Land, 1992). Thus, the analysis of the performance pyramid model in Chapter 2, shows that socio-organizational issues such as trust, culture and risk communication need an approach based on individuals' knowledge, beliefs, and feelings rather than an approach purely 'based on numbers'.

The second reason for selecting an interpretive epistemology relates to the complex dynamic process of goal setting. An interpretive research does not predefine dependent and independent variables, but focuses on the complexity of human sense making as the research proceeds (Galliers, 1987). For example, this investigation

focuses on the assumption that if information systems security goals are being efficiently set, *"why IS/IT managers fail to achieve the required levels of security for information systems?"*. Therefore, the question becomes, *"what are the issues that may have a negative impact on the level of security goal setting?"* or *"How the process of goal setting, if necessary, can be improved?"*.

An interpretive approach has the potential to explain of 'what is really happening within organizations' (Avison et al., 1999) and is qualitative in nature, as opposed to research aimed at establishing causal relationships or statistical generalisations (Chua, 1986). Schein (1992) also suggests that an interpretive research approach would provide richer data when used to describe an organizational culture. Consequently, an interpretive approach would provide a deeper understanding of culture within IT groups, which in turn, could be used to understand how IT groups set security goals and why they may have different goal setting strategies.

Finally, the issue with regard to generalisations is overcomed by using Walsham's (1995) comments that interpretive case studies offer four types of generalisations. These are presented in Figure 4 below. In addition, the possible bias that the interpretive researcher may be associated with, could be overcome by data triangulation.

Type of generalisation	Description
Development of concepts	Development of a new or an integrated cluster of concepts which can be parts of broader theory
Generation of theory	Development of a theoretical framework that can guide future studies in the same research areas
Drawing of specific implications	Provision of 'tendencies' which may prove a useful insight for related work in other organizations and contexts within particular domains of actions
Contribution of rich insight	Use of empirical data to provide rich insights about a wide range of different topics

Figure 4 Types of Generalisations (Walsham, 1995)

3.3.2 Phenomenology and Hermeneutics within Interpretivism

When the motivation of a particular investigation is to understand the experiences of human beings in terms of a particular process such as security goal setting, the use of phenomenology method seems the most appropriate to use. Phenomenological research explains phenomena in relation to human experiences, i.e. things learned through intuition and imagination (Moreno, 2001). In this investigation, the subject under scrutiny is the socio-organizational phenomena of security goal setting under the influence of risk management experienced within IT groups.

Interpretive research within the tradition of phenomenology is concerned with the description (Galliers, 1987) and analysis of everyday life (Beynon-Davies, 1997). It provides the identification of themes and social meanings related to the phenomena of interest by concentrating on the aspect of individual experiences (Moreno, 2001). Its actual claim is that knowledge is not the physical but the 'realm of pure thought' (Mingers, 2001). Similarly, phenomenology is based on the 'intuitive grasping of essences of phenomena' whereas the essences are more concerned with issues of *how* and *why* rather than *which* and *what* (Hirschheim, 1992), while a phenomenological disposition involves giving up the natural science attitude and its assumptions (Mingers, 2001).

Denzin and Lincoln (1998) argue that hermeneutics is used for the analysis of texts and emphasize how the existing understanding and prejudice of a phenomenon shape the iterative process. However, hermeneutics is being viewed as a cohesive strand of phenomenology since exploration of meanings and essence of experiences should result into a text form, which needs to be interpreted. Similarly, Gadamer (1975) argues that since language is essential for, and between people, then any reading or hearing of a text constitutes a hermeneutic act of giving meaning to it through interpretation. Klein and Myers (1999) and Bleicher (1989) support that hermeneutics could be used either as a solid philosophical foundation required for interpretivism or as a mode of data analysis.

In this research, the notion of the hermeneutic circle was also utilised. The notion of the hermeneutic circle in understanding the part (i.e., specific sentence or act) is, that

the inquirer must grasp the whole i.e., values, beliefs, institutional context, language, etc. and then back to the whole. Thus, to understand a phenomenon it must be placed in a larger context within which it operates and then, letting the researcher's grasp of this particular phenomenon influence the researcher's comprehension of the whole text. In this dissertation, the interpretation of the text (from the case studies) is made at a detailed as well as at a more general process level.

In the context of hermeneutics, theorists support also the notion that socio-historically inherited bias or prejudices are not taken as characteristics or attributes a researcher must avoid or manage in order to come to the 'real' understanding of phenomena (Schwandt, 2000). That actually, means that understanding a phenomenon requires the engagement of the one's biases. To this end, in this dissertation the researcher's personal views, to some extend, during the analysis of results.

3.4 The Research Design

3.4.1 The Case Study Method

The use of a case study represents a way to systematise observation and focuses on an in-depth understanding of the phenomenon within its context (Cavaye, 1996). Eisenhardt (1989) explains that a case study used as a strategy focuses on understanding the dynamics inherent in social settings. To this end, a case study approach seems more adequate to investigate the dynamics of security goal setting within IT groups since goal setting is a dynamic process that changes due to continuous changes in social and market needs.

Case studies are used for an extensive examination of a phenomenon in its natural setting, by employing multiple methods of data collection to gather information from one or more entities i.e. people, groups, or organizations (Benbasat et al., 1987). Table 6 below, depicts a list of key characteristics of case studies.

▪ Phenomenon is examined in a natural setting ▪ Data are collected by multiple means ▪ One or few entities (person, group, organization) are examined ▪ The complexity of the unit is studied intensively ▪ Case studies are more suitable for the exploration, classification and hypothesis development stages of the knowledge building process; the investigator should have a receptive attitude towards exploration ▪ No experimental controls or manipulation are involved ▪ The results derived depend on the integrative powers of the investigator ▪ The investigator may not specify the set of variables in advance ▪ Changes in site selection and data collection methods could take place as the investigator develops new hypotheses ▪ Case research is useful in the study of 'why' and 'how' questions because these deal with operational links to be traced over time rather than with frequency or incidence ▪ The focus is on contemporary events

Table 6 Key Characteristics of Case Studies (Benbasat et al., 1987)

There are different case study types including exploratory, descriptive, and explanatory based on the type of research questions asked such as "what", "how", or "why" (Yin, 1994). This research uses questions of the type "what" and "how" and thus aims to explore and describe. For example, some of the questions are of the type *"what is the interrelationship between trust, culture and risk communication"*? or *"how IT managers and groups set security goals with regard to information systems security management, with a focus on internet banking"*? Roethlisberger (1977) argues that the major advantage of case studies is their provision of rich evidence of the subject under investigation and their use to explain research questions such as 'why' and 'how' (as Benbasat et al., 1987 also suggest). In addition, Benbasat et al., (1987) assert that case studies are particularly well applied to IS research as the interest is shifted from technical to organizational issues.

3.4.2 Multiple Case Studies

The next issue under consideration was whether to employ single studies or multiple case studies. Theorists support the view that a single case study should be employed when exploring a previously unresearched subject (Yin, 1994) or for theory testing by confirming or refuting theory (Markus, 1989). Single case studies allow closeness to the phenomena of study and the possibility for rich description and insight (Cavaye, 1996; Conford and Smithson, 1996; Walsham, 1995). Single case studies though may not provide sufficient data on security goal setting issues since goal setting is a

dynamic process which changes on a regular basis and different organizations may apply different goal setting strategies.

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, deepen understanding and explanations. 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 vigorous on issues of cause and effect within units of analysis. Although, multiple case studies may not provide rich descriptions as does a single case study, multiple case studies allow the analysis of data across cases. To this end, a multiple case study approach was deemed more promising since it would allow the examination of different levels of IS security goal setting within different organizations.

However, in terms of the number of studies necessary to employ for the purposes of a particular investigation Eisenhardt (1989) supports an appropriate number of cases between four and ten although recent evidence supports that a large number of cases would enhance generalisability (Creswell, 1998). Further, Dyer et al (1991) suggest an appropriate number of cases based on how much is known about the phenomenon under study and how much new information is likely to be achieved through an extension of the number of cases.

This investigation employed three case studies within the IT departments of three financial institutions in Greece as this would allow the examination of data across cases within different IT group structures. The institutions ranged from small (Alpha-Bank) to medium (Delta-Bank) to large (Omega-Bank) financial institutions respectively, based on their financial assets. The reason for choosing these banks according to their assets is to investigate if the suggested performance pyramid model applies to different IT group structures. For example, the IT department at Alpha-Bank consisted of approximately 60 employees while at Delta-Bank 150 employees and 410 employees at Bank Omega. Indeed, the differences in IT group structures had different effects on IS security group goal setting level as will be explained in more detail in Chapter 4, 6.

The process of negotiating organizational access and collaboration required patience and determination. An important factor in gaining access to the case studies was the promised benefits (e.g., individual feedback, collective findings) to the participant banks. The banks were personally contacted by the researcher and face-to-face arrangements included description of research requirements, estimation of time/resources as well as the expected outcomes and benefits to the banks' IT departments. The sample represents a private bank (Alpha- Bank)[1], a semi-public (Delta- Bank) bank and one public (Omega- Bank). The investigator had no power to influence any situation within the banks' IT units and access was provided only for observation and without revealing the banks' identity respectively. However an interchange of knowledge took place between the investigator and the IT groups. Figure 5 below outlines the research design in this dissertation.

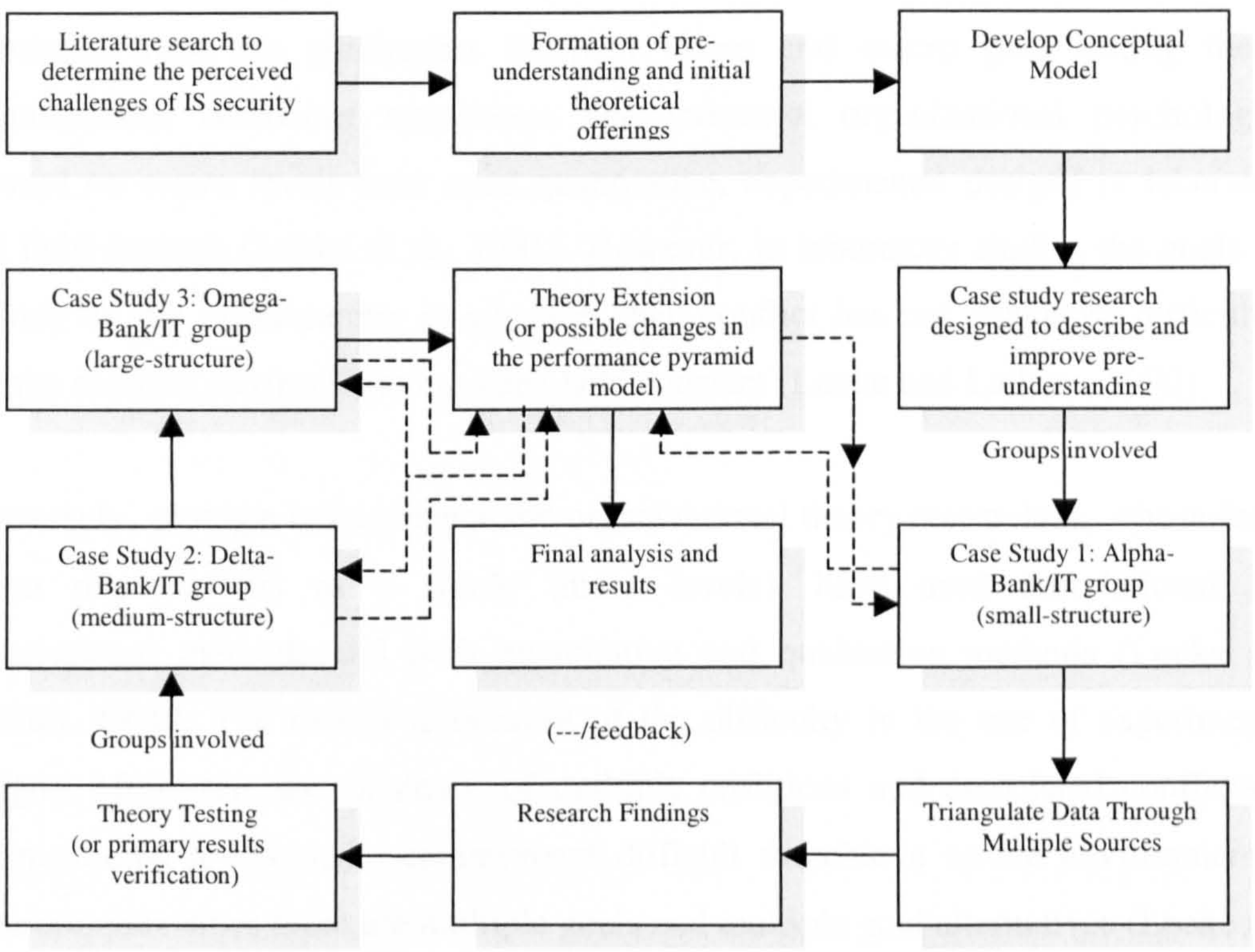


Figure 5 Outline of the Research Design

[1] The Three Case Studies in this dissertation are described as Alpha- Bank, Delta- Bank, and Omega- Bank respectively, for confidentiality reasons as it was required from the Banks.

3.4.3 Goal Setting Within a Case Study Approach

It is widely accepted that goals are important in regulating human action at both the micro (individual) and macro (organization/group) levels. As mentioned in Chapter 2, goals at the micro level affect action by directing attention and effort, prolonging effort over time, and motivating people to develop relevant task strategies (Locke and Latham, 1990). Goals also serve as a benchmark against which performance feedback can be evaluated (Locke and Latham, 1984). These functions have also a parallel effect on macro goal setting levels. Bradford and Cohen (1984) assert that goals serve a unifying function by mobilizing and directing organization's member efforts toward a common task. It is also claimed that an organization's goals direct its planning process influencing both its mission and strategy (Pearce and David, 1987) and that such goals serve as a standard by which to measure success (Parsons, 1960).

Although, there are similarities between micro and macro goal setting theory organizational behaviour researchers and industrial organizational psychologists focused on micro levels have used quantitative, experimental designs in laboratory and field settings (Locke et al., 1981). However, in laboratory studies the goals are defined by the experimenter in advance, goal conflict has not generated difficulties and the external environment has been held constant (Locke and Latham, 1990).

Conversely, strategic management and organizational theory researchers, whose focus is on organizations as a whole (macro-levels), have used correlational and observational methods and both quantitative and qualitative methods (Locke and Latham, 1990). The reason is because of the difficulty in the use of experimental designs. Moreover, the existence of multiple coalitions and associated conflicts at organizational levels make commitment difficult to achieve as the environment is more complex since there are multiple goals and multiple goal alternatives (Locke and Latham, 1990). Also in macro levels goals are studied in relation to business unit strategies rather than task strategies as in micro levels. These differences between micro and macro goal setting research are depicted in Table 7 below.

ISSUE	MICRO	MACRO
Unit of Analysis	Individual (some groups)	organization or division
Academic Specialty	organizational behaviour industrial-organizational psychology	strategic management organizational theory
Methodology	experimental	correlational or observational
Design	laboratory and field	field settings
Setting	settings	
Analysis	quantitative	qualitative, some quantitative
Time span	mostly short	long
Goals and Tasks	relatively simple, bivariate	complex, multivariate
Commitment & Conflict	routine, no conflict	problematic, high potential for conflict
Strategy focus	task	corporate or business level

Table 7 Micro-macro Goal Setting Patterns (Locke and Latham, 1990)

However, organizational goals have not been studied within case studies and particularly, in the context of information systems security. Most of the approaches include correlational or observational and field settings. The use of goal setting, at a macro-level, as part of a case study strategy method is important as it will provide the ground for discussion of the suitability of the research method.

3.4.4 Data Collection Methods

Multiple data collection methods allow stronger support of the research findings especially when multiple case studies are being employed. Thus, the design of this investigation employed multiple data collection methods as it is important in case research studies (Benbasat et al., 1987). Eisenhardt (1989) argues that the use of multiple data collection methods allows data triangulation which could provide stronger and cohesive substantiation of theory. Denzin (1989) describes triangulation such as an alternative to validation rather than a tool or strategy. Thus, any finding from the case studies is likely to be more convincing and accurate if it is based on various sources of information (Yin, 1994). This investigation used various methods

for data collection such as documentation, archival records, interviews, observation and physical artefacts. Table 8 below shows the strengths and weaknesses of each source of evidence within case studies and the methods used in this investigation.

Source of Evidence	Strengths as identified by Yin (1994)	Weaknesses as identified by Yin (1994)	This study used
Documentation	▪ Stable-can be reviewed repeatedly ▪ Unobtrusive-not created as a result of case study ▪ Exact-contains exact names, references and details of an event ▪ Broad coverage- long span of time, many events and many settings	▪ Retrievability- can be low ▪ Biased selectivity, if collection is incomplete ▪ Reporting bias- effects (unknown) bias of author ▪ Access- may be delivered blocked	▪ Organizational reports ▪ Reference material downloaded from internet ▪ White papers
Archival Records	▪ [same as previously for documentation] ▪ precise and quantitative	▪ [same as previously for documentation] ▪ accessibility due to privacy reasons	▪ deliverables of past projects on IS security development and implementation ▪ organizational charts, budgets
Interviews	▪ targeted- focuses directly on case study topic ▪ insightful- provides perceived causal inferences	▪ Bias due to poorly constructed questions ▪ Response bias ▪ Inaccuracies due to poor recall ▪ Reflexivity- interviewee gives what interviewer wants to hear	▪ Structured interviews ▪ Semi-structured interviews ▪ Unstructured interviews
Direct Observation	▪ reality- covers events in real time ▪ contextual- covers context of event	▪ Time consuming ▪ Selectivity- unless broad coverage ▪ Reflexivity- event may proceed differently because it is being observed ▪ Cost- hours needed by human observers	▪ Formal meetings with interviewees for gaining further insights
Participant Observation	▪ [same as above for direct observations] ▪ insightful into interpersonal behaviour and motives	▪ [same as above for direct observation] ▪ bias due to investigator's manipulation of events	▪ Simple participant
Physical Artefacts	▪ insightful into cultural features ▪ insightful into technical operations	▪ Selectivity ▪ availability	▪ Hardware and software equipment

Table 8 Strengths and Weaknesses of Data Collection Methods (Yin, 1994)

3.4.4.1. Interviews

Interviews as a data collection method are the primary data source in qualitative studies under an interpretivist epistemology. Denzin and Lincoln (1998) also support interviews as an important tool of qualitative researchers for data collection. Walsham (1995) argues that interviews allow the researcher to access participants'

interpretations with regard to their actions and events as well as to their views and aspirations of themselves and other participants. He further argues that interviews are important as they allow researchers to step back and examine in more detail the participants' interpretation. This aspect plays also a vital role in deciding upon the interview process.

Moreover, the interviews in this investigation were based on a broad list of research issues as well as topics gathered from literature sources. A questionnaire list was usually sent to the interviewees a few days in advance. The reason of sending a questionnaire list was to provide the interview participants with a view of the subject under investigation and allow them enough time to prepare. The time needed for interviews was not easily available due to the highly sensitive nature of security as well as the dynamic activities of the IT groups, and so the researcher attempted to exploit any possible advantage. In addition, the questionnaire list provided information needed for the appropriate selection of the interview participants.

The average duration of the each interview was approximately two hours. All the interviews were face-to-face, and when necessary telephone calls followed up to confirm something about the data that was unclear. In most cases the conversations were tape- recorded. In fact, tape-recording was not allowed at Bank Omega (large-structure) as the IT manager was not confident enough due to the highly sensitive issue of security. Instead, the researcher was allowed to keep notes based on the conversations. Tape-recordings were used in the other two cases as they offer benefits that are not always available with other forms such as note taking of data collection.

Interviews were viewed as the 'text' in the hermeneutic process (Boland, 1985). The key to this process is the development of different, alternative meanings for IS security until there are no further absurdities, incomplete or inconsistent points in the researcher's understanding. Thus, the interview material was subjected to the elicitation and understanding of facts about IS security goal setting within IT groups. The interpretation continued on to attitudes, opinions, impressions and beliefs of the participants within a socio-organizational context. Several other issues that were also important in part of the researcher's attitude include: to develop a climate of trust with the interviewees, to make them feel important to the research, not to prejudice

responses and assist them reconstruct the past and describe the present by providing questions for guidance.

With regard to the number of interviewees this investigation included seven people from Alpha-Bank, seven people from Delta-Bank, and eight people from Bank Omega. In particular, the interviewees included: (1) at Alpha-Bank: the IT manager, four deputy IT managers, and the managers from the audit and e-banking units respectively, (2) at Delta-Bank: the IT manager, the alternative networks deputy manager, two IT employees, the organization deputy manager, the marketing plans deputy manager, and the manager of the strategic marketing unit, (3) at Omega-Bank: the IT manager, the IT deputy manager, two IT employees, the organization manager and deputy manager, the audit manager and the strategic plans manager. In all of the three organizations there were not specific security staff members but rather the IT managers and deputy managers were the people with in-depth knowledge on security issues. However, the IT groups were also in close collaboration with third party security contractors with whom there was an exchange of knowledge and experience on IS security. Table 9 below shows the design of data collection based on interviews.

Organization	**Type of Interview**	**Respondent position**	**Number/type of Interviews**
Alpha-Bank	▪ Face-to-face ▪ Telephone	IT manager	Two(structured/ unstructured)
Alpha-Bank	▪ Face-to-face ▪ Telephone ▪ e-mails	Deputy manager data center	Two (structured/ unstructured)
Alpha- Bank	▪ Face-to-face ▪ Telephone	Deputy manager networks	Two (structured/ unstructured)
Alpha- Bank	▪ Face-to-face	Deputy manager systems	Two (structured/ unstructured)
Alpha- Bank	▪ Face-to-face ▪ E-mails	Deputy manager alternative communication channels	Two (structured/ unstructured)
Alpha-Bank	▪ Face-to-face	e-banking manager	One (unstructured)
Alpha-Bank	▪ Face-to-face	e-banking employee	One (unstructured)
Alpha- Bank	▪ Face-to-face	Audit manager	One (unstructured)
Delta- Bank	▪ Face-to-face ▪ Telephone ▪ E-mails	IT manager	Two (structured/ unstructured)
Delta-Bank	▪ Face-to-face ▪ Tele-phone	IT employee	Two (unstructured)
Delta-Bank	▪ Face-to-face	IT employee	One (unstructured)

Delta-Bank	▪ Face-to-face ▪ E-mails	Organization deputy manager	One (unstructured)
Delta- Bank	▪ Face-to-face ▪ Telephone ▪ E-mails	Marketing plans deputy manager	Two (structured/ unstructured)
Delta-Bank	▪ Face-to-face ▪ E-mails	Alternative networks deputy manager	One (stuctured/ unstructured)
Delta-Bank	▪ Face-to-face	Strategic marketing manager	One (structured/ unstructured)
Omega- Bank	▪ Face-to-face	IT manager	One (unstructured)
Omega- Bank	▪ Face-to-face	IT deputy manager	One (unstructured)
Omega- Bank	▪ Face-to-face ▪ Telephone	IT employee	Two (unstructured)
Omega- Bank	▪ Face-to-face ▪ Telephone	IT employee	One (unstructured)
Omega-Bank	▪ Face-to-face	Organization manager	One (structured/ unstructured)
Omega-Bank	▪ Face-to-face	Organization deputy manager	One (unstructured)
Omega-Bank	▪ Face-to-face	Audit manager	One (unstructured)
Omega- Bank	▪ Face-to-face	Strategic plans manager	One (unstructured)

Table 9 Data Collection Design through Interviews

The questions asked include issues of trust, culture, risk communication, goal setting, IS security, group commitment and other various questions that contained technical as well as organizational elements. The total time period of interviews lasted approximately three months. Table 9 shows also which prospective interviewees received the questionnaires, under the term structured interviews, and Appendix B1-5 includes a list of the questionnaires. Structured interviews were used for primary data clarification while unstructured interviews dealt with free style conversations. It has to be mentioned, that unstructured interviews gathered more data for analysis as the interviewees felt more confident and relaxed to answer the questions using their own expression style.

3.4.5 Data Analysis

Data analysis is the most vital stage of the research strategy and it has to be carried out with careful consideration. One problem, by using qualitative data is that the methods of analysis may not be adequately formulated (Miles and Huberman, 1994). Thus, the contextual and data richness should be presented as much as possible, and a clear chain of evidence should be established. The research should start with the definition of objectives and questions, assumptions and design choices, specific data uncovered and ultimately, to results and conclusions (Benbasat et al., 1987, p.377).

In this research, the analysis of the case studies is based on the performance pyramid model suggested in chapter 2, facilitated by the use of within case analysis (Yin, 1984) and cross-case patterns (Miles and Huberman, 1994). In case analysis, detailed case study write-ups are stated and from the descriptions, a familiarity with each of the settings is provided. This is achieved in chapters 4, and 5 by providing in-depth descriptions of the settings and processes within which IS security goal setting is experienced by the three organizations as well as the interrelationship and effect of trust, culture and risk communication in goal setting. By doing so, a contextual richness is established so that questions with regard to the *what* and *how* of issues become clear. Chains of evidence are also shown (chapters 4, and 5) by using quotation marks in order to demonstrate the exact nature of results and illustrate that the actual interview responses were received and are not the researcher's interpretations. To confirm that the correct interpretations of results have been achieved, the triangulation method was utilised.

With regard to cross-case patterns suggested by Miles and Huberman (1994), there is a variety of alternatives. One alternative is to chose a pair of cases and define similarities and differences between them each time. Another one is the selection of categories or dimensions, and define similarities and differences within group or divide the data by source of data. The socio-organizational aspects of the performance pyramid model, can be viewed as categories or different dimensions and that was the option chosen for this investigation. In this way, the data can prove more reliable in relation to the socio-organizational aspects of the performance pyramid model within different case studies. This is achieved to some extent in chapter 5, although an in-

depth analysis is utilised in chapters 4 and 6. However, cross-case patterns were similarly used within each case study in order to find similarities and/or differences between people's perceptions about procedures and organizational values and beliefs. For example, one of the questions asked was: *"Do you believe trust is important in setting goals efficiently within the group"*? or *"What is the role of trust to culture and risk communication"*?. Then, each answer of the prospective interviewees, for the same type of questions, was placed into a context in order to identify the degree to which their perceptions were the same or different. In doing so, the researcher was provided with useful insights of the phenomena under study and thus, a clear understanding of the perceptions, values and beliefs as well as organizational procedures was obtained.

3.4.6 Data Triangulation

An important key to successful interpretation of data achieved through qualitative analysis is the means by which the research findings are validated and reliable. Thus, triangulation provides the means by which to validate the results of a particular investigation. There are mainly five types of triangulation including data, investigator, theory and methodological triangulation, and interdisciplinary triangulation (Denzin, 1978; Janesick, 2000). Data triangulation means the use of multiple data in a study while investigator triangulation means the use multiple researchers or evaluators. Similarly, theory triangulation means the use of multiple perspectives to interpret a single set of data while methodological triangulation is the use of multiple methods to study a single problem. Ultimately, interdisciplinary triangulation makes use of multiple disciplines. The present research used data triangulation, theory, methodological, and interdisciplinary. These triangulation methods are depicted in Figure 6 below.

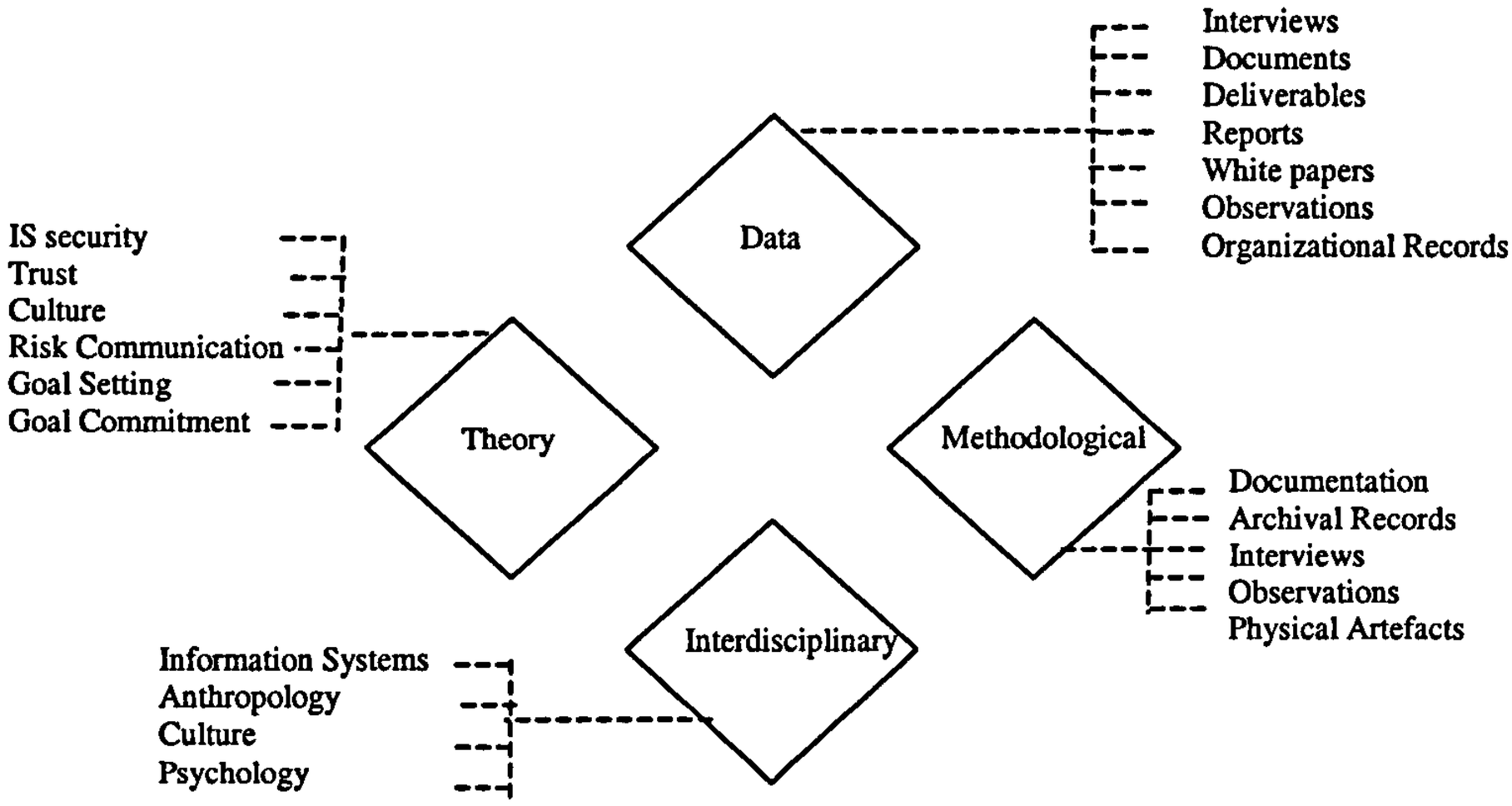


Figure 6 Types of Triangulation Used in the Research

Thus, Figure 6 shows that at the triangulation of data various sources used include documents, interviews, observations, deliverables, reports, white papers, and organizational records. Triangulation of theories emanate from information systems security, trust, culture, risk communication, goal setting, and goal commitment. Methodological triangulation includes documentation, archival records, interviews, observation, and physical artefacts while interdisciplinary contains information systems, anthropology, culture, and psychology.

3.5 Summary

The chapter examined and identified key characteristics of the existing research approaches in information systems security and distinguished them as positivist, interpretive, and critical theory. The principal goal was to justify the chosen research approach for the purposes of this investigation in relation to other approaches within the IS security literature. In providing a detailed consideration of the issues related to the practical search for knowledge, the chapter described and discussed the methodological as well as philosophical assumptions underlying the research approach for this investigation.

The ontology of this research with regard to security is that, security should not treated as something tangible and concrete but also as a social, organizational issue. To this end, a qualitative research approach having philosophical foundations mainly in interpretivism, was deemed the most appropriate for this investigation. Generally speaking, the interpretivist paradigm is gaining ground in information systems field, which further can provide useful insights into the social context of information systems security. Likewise, the use of qualitative analysis allows the investigation of less well-known phenomena, i.e., trust, culture and risk communication in the context of goal setting, examines dynamic complex processes, i.e., goal setting in the context of risk management, and most important the examination of a phenomenon in its natural setting.

Next, the chapter analysed the types of existing research strategies and the reasons for selecting a case study strategy. Multiple case studies were used to describe and provide a deeper understanding of goal setting within IS security. The use of various methods for data collection was discussed as well as their suitability in this particular investigation. To this end, the research methodology and design should illustrate the suitability of the chosen research approach, which will be determined in Chapter 6 and concluded in Chapter 7.

Chapter 4: Description and Discussion of the Alpha-Bank Case

4.1 Introduction

This chapter describes and discusses the case of Alpha-Bank used for the purpose of this investigation. In doing so, the purpose of this investigation in broad terms is: (i) to validate the rationale and assumptions of the research by verifying that the theoretical issues within the performance pyramid model are obtainable in practice; and (ii) to present a model which can be used to analyse future research studies and shed light into the socio-organizational perspectives of information systems security.

The empirical findings and analysis results drawn from the case of Alpha-Bank will provide the ground for analysis, comparison and discussion of the results obtained from cases with different organizational structures such as Delta and Omega-Bank, discussed in Chapter 5 and analysed in Chapter 6.

This chapter gives a brief background of Alpha-Bank in the context of its history, business, infrastructure, management and organization on a global scale as well as its recent developments. It describes and analyses goal setting within its 'real life context' as part of the risk management process. Then, it investigates the possible interrelationship and effect of different socio-organizational aspects on the process of goal setting with regard to internet banking security.

The case study approach within an interpretive epistemology provides the ground for discussion of the suitability of the chosen strategy in this research which will be further extended and discussed in Chapters 6, 7. It has to be mentioned, that the time period of this investigation was approximately three months starting in the middle of August 2002 and ending in October 2002. Likewise, the investigation used the case of Alpha-Bank to validate the rationale and assumptions made in chapter 2 and in so doing, to clarify and further develop the questioning techniques used in the cases of Delta-Bank and Omega-Bank.

4.2 Case Study One- AlphaBank

4.2.1 Background to the Organization

Alpha-Bank is a private-owned bank established in 1991 by a group of Greek businessmen with its headquarters mainly located in the North part of Greece. Their vision was:

"to create a contemporary and flexible financial organization which would totally cover the banking needs of their customers-partners and would dynamically claim a substantial portion of the Greek banking market".

At the end of fiscal year 2001, the bank owned total assets of more than Euro 2.47 billion and profits of more than Euro 340 million. Alpha-Bank employed more than 1,283 people (2001 figures) out of which 54% men and 46% women with an average age of 37 years. Alpha-Bank's organizational chart is depicted in Appendix D1.

Oriented in offering full-scale services to both its individual customers (deposit products, loans, credit cards) and to small and medium size enterprises, Alpha-Bank has developed intense activity in financing sectors such as corporate and investment banking, shipping, treasury management and private banking. Alpha-Bank was the first bank in the Greek Banking Market to offer internet banking services through the Web.

Today the Alpha-Bank Group with a branch network of 60 has developed active participation in the Athens Stock Exchange through its subsidiary Alpha-Bank Securities S.A. while having a strong presence in the field of mutual funds through its subsidiary Alpha-Bank Mutual Funds Management Co. S.A. Likewise Alpha-Bank Leasing provides all forms of leasing while the insurance needs of its customers are being met by its subsidiary Alpha-Bank Insurance Agency Ltd., which continuously expands its collaborations and enriches its range of products.

In order to maximise productivity and to improve the existing business process the organizational structure was adopted to suit current market needs. As such two new departments, Business Process Re-engineering and Human Resources Development,

completed the bank's organizational structure with the aim of maximizing performance, strengthening and better communicating the corporate culture and improving productivity. As the IT manager of Alpha Group stated:

"Human resources and technology are the cornerstones in which the Bank has based its success and on which it secures its future".

Business Process Re-engineering could enable an organization to increase its efficiency, reduce costs and make more effective use of technology (Mumford, 1996). In fact, it is believed that organizations that did not introduce business process re-engineering may face problems in the future (Hammer and Champy, 1993).

Likewise, the development of human resources within a secure and dynamic work environment is one of the bank's permanent strategic goals. The enrichment and renewal of all training programs are led by the latest market developments and aim to help the bank's employees become well trained and well equipped. For this purpose the bank's training program in year 2002 was redesigned, enriched and adapted to the needs of the market. At the same time, the bank seeks to provide a work environment geared towards growth, development and fair compensation.

4.2.2 Electronic Banking

Alpha-Bank was the first bank to introduce electronic banking in the Greek banking sector and even today the bank maintains its leadership by continuously introducing new products and services through its Web-site. Electronic banking in Alpha-Bank is actually focused on three categories: customer relationships, individual customer and professional relationships, and alternative networks.

4.2.2.1 Corporate Customer Relationships

Alpha-Bank in order to improve its products and services towards its customers has enriched its internet banking services, and in particular the Web Teller service-transactions via the internet- with the extra service of electronically paying VAT and

IKA (social security). In the area of internet commerce, the Webshop- secure and instant payment for on-line purchases from electronic shops with the use of credit cards- has been improved on many technical and functional levels with an emphasis placed on the security of data exchanged between e-shops and the bank.

Moreover, the bank has launched new products since 2001, some of which are deemed to be very innovative in as much as they appear in the Greek market for the first time. These are included in Table 10 below.

- **Alpha-Funds B2B**: Electronic Business to Business buying and selling of Alpha-Bank Mutual Fund units and relevant accounts with direct debit-credit of the customers' accounts.
- **Alpha-Payment**: Electronic salary payments and mass payment orders via the internet.
- **Alpha-Properties**: On-line search service exclusively for the bank's property portfolio through which users can express an interest to buy.
- **Alpha-Prepay**: A prepaid card service for on-line internet purchases. An important tool for the increase in sales of those companies operating electronic shops. This service makes internet shopping available to those customers who either do not own credit cards or who are reluctant to use them for security reasons.

Table 10 Electronic banking products and services for B2B

The bank also has recently introduced third mass payment orders to other banks, ticket sales for events and travel, while the IT group is rethinking its on-line equity service and the creation of business-to-business service for transactions on the Athens Stock Exchange.

4.2.2.2 Individual customer and professional relationships

In this category, Alpha-Bank paid careful attention to Web Trader transactions- real time information on the Athens Stock Exchange (ASE) and in the on-line execution of orders combined with direct debit/credit of investors' accounts. Similarly, Alpha has introduced new products and services to its customers, which are included in Table 11 below, while aims to create the first global financial portal in the Greek banking market.

- **Alpha-Funds B2C:** Electronic Business-to-Consumer buying and selling of Alpha Mutual Fund units and relevant accounts with automatic on-line link to the investor's account.
- **Alpha-Properties:** On-line search service exclusively for the bank's property portfolio through which users can express an interest to buy.
- **Alpha-Prepay:** Prepaid cards for on-line purchases. A product which provides individual customers with an alternative payment method for e-shopping in the event that they do not own credit cards or are reluctant to use them for security reasons.

Table 11 Electronic banking products and services for B2C

4.2.2.3 Alternative Networks

The main focus of Alpha-Bank's IT group is to develop existing infrastructures and to increase its 'know-how' in order to launch new, leading edge services and payment systems for its customers. To this end, electronic banking had a steady growth of 115% in the number of customers-users in 2001 as compared to the previous year. The total number of transactions executed over the bank's system increased by 55% in year 2001, and the value of these transactions grew by a massive 345% as compared to the year 2000. Further, the electronic banking department has introduced in year 2002 new alternative networks such as Mobile banking and Voice (telephone) banking.

Moreover, Alpha-Bank has recently improved its e-banking infrastructures through the re-organization and transfer of all systems necessary for the operation of a second server in Athens. This was done in order to allow for better access to the bank's site through a more even distribution of the workload between Northern and Southern Greece. This resulted in faster access times and improved service.

In the context of security, all on-line services at Alpha-Bank run on the SSL-128bit security protocol that is used internationally. Access procedures to the bank's electronic services are based only on two access codes. For all transactions requiring additional security the system provides a TAN- Transaction Authentication Number- while the IT department reviews new advanced security systems based on digital certification and e-tokens.

The bank's Web-site has been also improved as a result of a complete technical, functional and visual overhaul carried out by the e-banking department. It is more user friendly and provides easier access to information on the Group's products and services. The bank's specialised services are easily accessible and are split into four basic categories: e-banking, e-investments, e-commerce, and e-properties. The site offers a whole range of new services such as an easy browser guide, an automatic loan calculation model, currency converter and on-line information updates.

Similarly, at the end of 2002 Alpha-Bank had 67 new ATM's with which it has achieved almost 100% availability which resulted in a 40% increase in cash withdrawals by the bank's customers and a 50% increase in cash withdrawals by customers of other banks through DIAS system.

4.2.3 Information Technology and Bank Operations

Technology in Alpha-Bank is being viewed as the vehicle with which it will be able to achieve its goals, as the means that will bring increasing returns, reducing costs and obtaining the best response time. The evolution of information technology has many applications in the financial sector and creates a new environment in which banks can function. The main characteristics of this new environment are the reduction of costs in providing services, the geographical proximity between buyer and provider of financial services which is no longer a requirement as well as the speed and quality of these services provided.

However, the IT department at Alpha-Bank is consisted of 60 employees with an organizational structure shown in Figure 7 below. It has to be mentioned though that the term IT department is going to be used interchangeably with the term IT group for reasons of convenience.

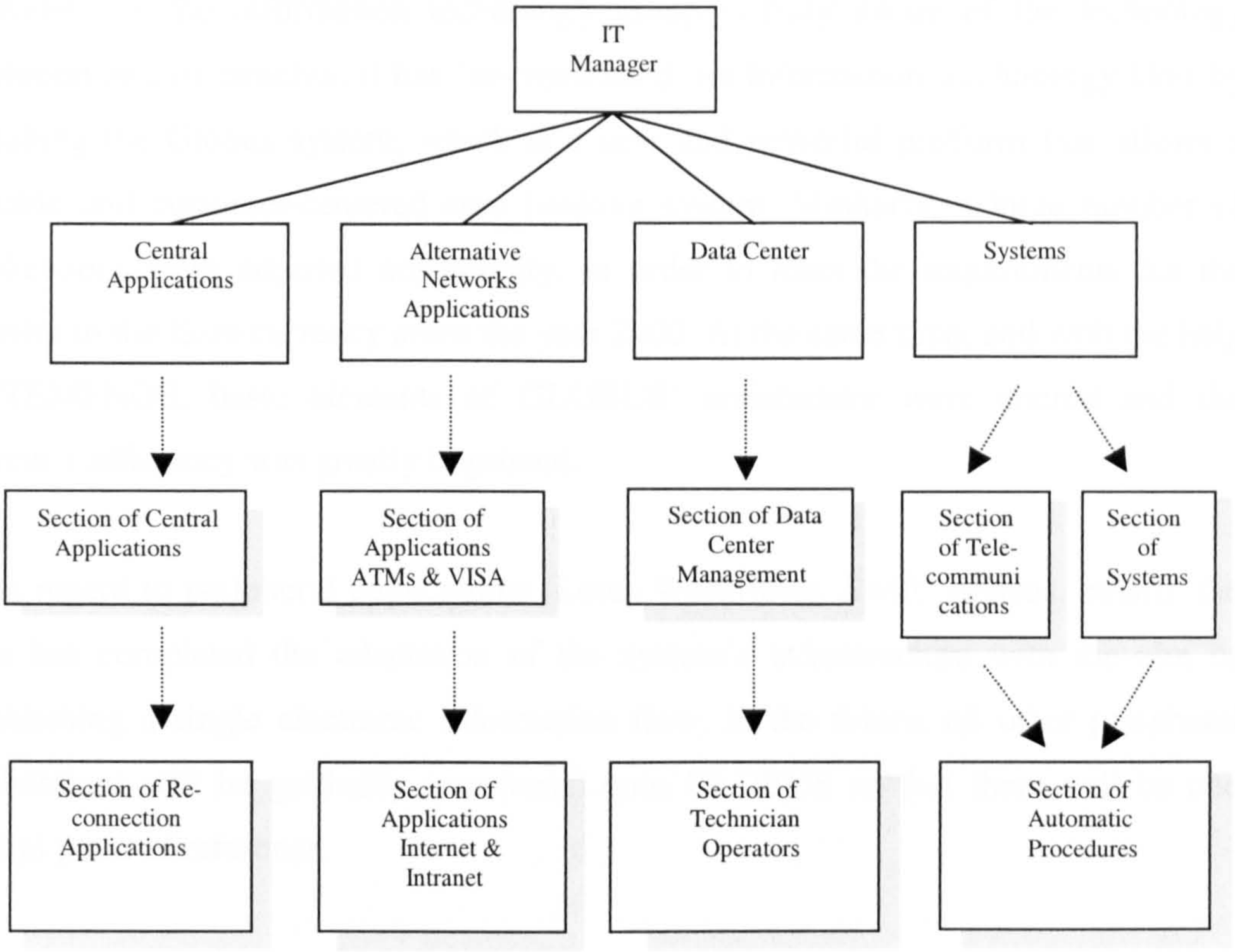


Figure 7 Alpha-Bank IT group organizational structure

At Alpha-Bank the information technology department is subdivided into four main units. These are: 1) the unit of central applications, 2) alternative networks, 3) data center, and 4) systems. The main goal for the central applications unit is the qualitative and quantitative improvement of services at the minimum cost. This unit controls all the software applications and programs based on which Alpha-Bank operates. The unit of alternative networks focuses on new applications such as Mobile- Banking, Telephone- Banking, and network applications such as Internet and Intranet. Similarly, data center defines the procedures based on which the business part is processed. It is the part of information technology that controls and manages the operation of the central system. The systems unit is responsible for the administration of the central system and of the tele-communications network. The main goal for this unit is to make systems and tele-communications run at faster response times and at lower costs. This unit is also responsible for any changes to communication protocols e.g. from G25 to TTP or Frameline.

However, as the information technology group is fully aware of the technology evolution and its benefits, it has 're-engineered' its Information Technology Unit by installing the Globus system, which is a new and powerful platform that allows a flexible and customer-centered core banking system. Similarly, a large number of applications were adjusted accordingly, in order to meet the requirements for the transfer to the Euro currency since the year 2000. At the same time, and with the help of TEMENOS, basic elements of GLOBUS' architecture were altered and the system's efficiency was greatly improved.

With regard to peripheral applications (Lotus Workflows, Swift, Abacus, email), the Unit has completed the adaptation of the system's infrastructure with the aim of establishing a single electronic information flow. In the future, all other peripheral applications will be gradually transferred onto GLOBUS so that there will be one central point of reference.

Alpha-Bank has established the Operations Department with the aim of aligning the organization with its business overall expansion plan. The projects undertaken during each year can be mainly divided into: 1) growth related activities, and 2) support related activities. In growth related activities, Alpha-Bank in year 2001 has completed the platform for on-line loan application while in support related activities it has created and launched a Help Desk for staff support.

4.2.4 The Risk Management and e-banking Units

The Risk Management Unit is responsible for the bank's security policies and one of the main procedures is the improvement of the protection of Fixed Assets and Cash. A relevant manual was written in 2001 covering security policy and internal procedures. The Department also in 2001, with the support of the Regulatory Reporting Unit, installed a new system for automatically measuring the bank's Capital Adequacy Ratio in order to ensure more systematic monitoring. This system calculates market and counter party risk in accordance with Presidential Decree/TE 2397/96.

The e-banking unit consists of 15 employees and is located in Athens. This unit is actually responsible for the Web interface and any Web applications, and for the strategic development of products and services available through alternative on-line banking channels such as ATMs, mobile and voice (telephone) banking. The e-banking unit could be seen as the marketing unit of all the financial products and services available through the bank's Web site. In addition the unit is involved with security policies over the internet as well as other on-line applications.

4.3 Case Findings

4.3.1 The Process of Goal Setting within AlphaBank

Goal setting is a consistent process of Alpha-Bank's strategic vision and it is the basis upon which the bank depends in order to achieve its initial commitment. In particular, Alpha-Bank each year concentrates its efforts towards a global set of actions, which will enable the maximization of its profits gained from opportunities in the Greek market. The significance of goal setting within Alpha-Bank was better described by the manager of Audit Department who stated:

"Goal setting is vital for any profit-oriented organization. A profit-oriented organization can be assumed successful when it meets the demands of its shareholders. Thus, our main goal as a financial organization is to satisfy the demands of our shareholders in terms of profit maximization by setting reasonable goals and putting forward our commitment to them. Without goals the identity of the organization will be lost in the long-run due to intense market competition".

To this end, each and every following year Alpha-Bank takes actions towards an ambitious and global approach to the evolving-market and to the needs of its customers-partners. An example of the nature of the bank's overall strategic goals for the year 2002, is given in the following:

- *Innovation of products and services in the area of consumer-credit and e-banking.* The bank must increase its activity in the area of small and medium sized corporate services by making use of its branch network, its centralised support services and penetrating into the investment banking sector.

- *Innovation of distribution channels.* The bank must create different types of branches in order to better cater to the needs of local markets with a view to improve the bank's income/expense ratio.

- *Innovation in the development and growth of human resources.* Alpha-Bank has to design in-house programs with a view to develop human resources and improve the organization's business processes.

- *Activate cross-selling across the whole Group.* The bank must train all production units in all the Group's products and refocus its approach from pure single-product selling to providing overall financial services and solutions. In addition, the bank must set up systems and procedures for proper goal setting, monitoring and compensation of cross selling by the bank's staff. Similarly, Alpha-Bank must create a customer reward system for those customers who either increase their relationship with the bank or introduce new customers.

- *Continue to pursue efforts to reduce costs.* Alpha-Bank must continue, through increased centralised services, automated procedures and redesigning of existing structures, to create flexible procedures capable of limiting the bank's costs and freeing up time for the bank's staff. The bank must continue its efforts to systematically reduce costs within a framework of selective expansion and generalised reduction of its discretionary expenses. Additionally, the bank must improve the management of its business risks through the application of a VAR (value at risk) model in order to achieve a technically reliable estimate of credit risks and market risks arising from its operations.

These strategic goals give an overall view of how Alpha-Bank sets a broad frame of reference according to which its strategic vision is further developed and implemented. The overall goal of all these actions at Alpha-Bank is to achieve profitability through a selective credit policy and to greatly increase the product per average customer. *This broad strategic vision was presented in a board meeting by the Vice President of Alpha-Bank at the end of year 2001 with the scope to alert the organization's members for the bank's 2002 goal planning activities* (as reported by the Audit manager in 2002).

Given this example, it can be seen that the goals of each year at Alpha-Bank are being set at the end of the previous year. The described process of goal setting is the following. The Vice-President at the end of each year gathers the directors of board and the managers of each banking division to discuss current market trends, as well as the current status of the bank against its competitors. This is a discussion in a friendly environment where everyone feels free to express his/her opinion on the current course of action taken by the organization. In the meeting, the strategic issues of the bank are discussed and then the participants select the most important issues that need further discussion and development. When the nature and scope of the issues have been established then the managers of each banking unit have to set and provide a proposal to the board of members for any possible investments needed. However, the board of directors have to decide which projects need immediate funding and which should be considered at a later stage. The decision depends on the benefits each project is promised to deliver, which is why there is quite often competition between the banking units to have a great share of the funding.

As the process of goal setting was described, the researcher asked the interviewees if there were any important factors that may affect goal setting. All of them replied that an important factor in goal setting is the clarity of goal achievement as well as the top-management's commitment and support (Ross and Staw, 1985; Keil, 1994). As stated, managers play a critical role in the achievement of goals through their continuous support and through an effective explanation to their group of how to achieve those goals. Therefore, by asking what were the important factors in goal setting, as will be discussed later on, other issues such as trust, culture, and communication came to the forefront. Using the same style of questioning resulted in a better construction of data findings than previously.

4.3.2 Security and Internet Banking Goals in the Context of Risk Management

Having described the process of goal setting within Alpha-Bank in broad terms, this section describes the stages of security and internet banking goal setting as part of the risk management process within the information technology unit. It has to be mentioned though that the IT group is responsible for the security of information

systems in terms of development and management and for the monitoring of the overall bank's information technology infrastructure.

However, goal setting within the IT group of Alpha-Bank comes either from the top levels of the hierarchy downwards or from the bottom levels of the hierarchy upwards (see Appendix C1). In particular, goals within Alpha-Bank are always translated into projects. Every project therefore is actually a goal that any banking unit has to achieve. For example, if the board of directors believes that the bank should further reduce its operating costs by introducing alternative technology banking means, the decision is transferred to the IT department in the form of a goal and then the IT group starts the goal initiation phase. The IT manager more specifically explained:

"In the goal setting paradigm, goals are considered as projects, for each of which there is a project team. Such goals have life cycles, and involve planning, development and termination. Goal setting within the Alpha-Bank IT group may be considered in terms of risk management within the context of management projects".

When goals are being introduced, the IT manager selects the members which will represent the group and which will be involved in the particular project. This is the so-called *initiation phase*, shown in Figure 8 below. This phase is also applied to cases where it is the IT group's decision to set a specific goal. In this case the IT manager who is usually the project leader has to provide a report to the bank's board of directors. The report is explaining the benefits of the proposed resolution and if the board in turn agrees on the project's development and implementation, then the IT manager starts the goal initiation phase. An example of such an abstract report having overall information systems/technology goals for the year 2001, is given in Appendix C2. To conclude, goals start from downwards towards the upward levels of the organizational hierarchy and vice versa. Either way the procedures are implemented in the same way.

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

Figure 8 Security Goal Setting in the Context of Risk Management (Alpha-Bank)

In the context of information systems security, the IT manager has to explain the *method* to the selected group and *plan* of the security risk activities. In particular, the IT manager explains what is expected of the group, what is the estimated project time, and what the results should be. If any group member has any questions the IT manager is liable of answering in order to provide clarity of goal achievement and of the goal setting process within the context of security risk management activities. The IT manager will conclude by making regular appointments for interviews and group meetings.

Likewise, the design of information systems security within the Alpha-Bank IT group starts always from the external environment with the procedures concentrating step by step into the internal environment. In particular, the issue of security goals within the IT group is distinguished into: (a) physical security artefacts, i.e., the central operation system, or security cameras on buildings, and (b) internal security: the procedures according to which security steps are being followed. The first category includes security goal activities with regard to all hardware equipment, building security specifications as well as access controls. In the second category, the IT group follows procedures according to which the on-line activities of the bank's employees are scrutinised by an operating system in order to maintain and control security levels.

Such activities include access codes, passwords and monitoring of the employees' access to specific sites and documents.

The next phase of security goal setting is that of execution. This phase includes several steps such as identification of risks, pre-selection of identified risks, final risk identification, control of activities, and risk monitoring. The first step is the identification of risks in broad terms. The IT manager arranges interviews within the group to discuss all possible risk sources and then based on a checklist the IT group commonly decides on the relevant risk factors. Every risk factor can be assumed as a sub-goal. Specifically in the interviews each member comes up with his/her personal identification of relevant risk factors and the group sets respectively security goals. As the IT manager explained: *"a crucial part of this process is to determine what are the risks, and what are the opportunities"*. At this stage the risk identification activities are usually broad in scope and involve the team members' knowledge, experience, and use of a checklist.

With regard to internet banking security the IT group uses a checklist which consists of five clusters of risk categories. This checklist is shown in Appendix C3 and includes: (a) internet banking policy, (b) internet banking and physical security risks, (c) internet banking auditing, (d) identification of customers in an electronic environment, and (e) electronic commerce. In each cluster, a series of relevant risk factors and threats is identified. The checklist includes a sample of the most well-known risk factors since possible risk events may exist in a wider context.

The next step for the group is to identify the risk factors that need more careful consideration and select between 'important' and 'unimportant' risks. This distinction facilitates the evaluation of risk factors. This stage is particularly necessary since the financial resources spend on the projects are limited and have to be fully exploited. After the risks have been differentiated the group has to estimate the ratio of risk likelihood, the possible consequences, and the timing needed.

Similarly, after the important risks have been identified and estimated in terms of their likelihood, impact, and timing, the group via a joint meeting decides on the final selection of risks. When each of the possible risk factors is defined, the checklist is

used to provide the ground for discussion into the potential of each risk factor. This stage helps to identify the acceptability of possible risk events so that decisions can be made on whether to accept the risks, or set goals to minimize them.

The next step is to apply control activities to ensure that the security goal setting plan so far as part of the risk management process will actually accomplish its objectives. That means if objectives are not being met the group has to reconsider its actions in order to rectify the situation. Such a control takes place through regular group meetings and discussions.

Risk monitoring is the last step of the execution phase, which actually monitors the status of the previously identified risks. At this stage, the group decides whether to continue the monitoring of risk factors previously identified, or to formulate additional measures for existing risk factors.

Finally, the last phase of setting security goals within the process of risk management is the evaluation of risk activities planned. In particular, the IT manager gathers the members of the group to produce a report, which will provide the information from which lessons can be learned for future activities. For example, the report includes each relevant risk factor and the measures associated with it. The report concludes with the selected risks based on their high likelihood ratio, time-schedules, financial budget, and then if necessary, the IT manager assigns responsibilities to each member participating in the group.

Nevertheless, goal setting within the Alpha-Bank case and in particular within the IT department is consistent with the overall risk management process. A goal has been defined in terms of a project whereas within each project there are different sub-goals. The management of internet banking security risks is based on a checklist provided in Appendix D3, and shows that in every cluster of the list there are different risk factors according to which the IT unit sets security goal activities. Thus, based on the case of Alpha-Bank, security goal setting is an active process within the IT group which answers the first question of this investigation of whether organizations follow goal setting procedures.

4.3.3 Security Risk Events in the Context of Internet Banking

The process of goal setting with regards to security and internet banking risks was previously discussed in the context of risk management. However, security issues within the Alpha-Bank IT group are processed on the same principles as any other risks. The difference though with security issues within the context of internet banking is that the IT group uses a standard checklist which depicts all possible areas of threats that are likely to occur through the use of internet banking channel. This checklist, shown in Appendix D3, is based on past knowledge and experience as well as on current market trends.

However, during the interviews within the Alpha-Bank IT unit, three main security risk events with regard to internet banking were mentioned. These security events were part of the security and strategic development of products available through the internet banking channel. These events mainly concerned the introduction of smart cards in the context of user security, firewalls in the context of network security, and server monitoring in the context of server security respectively.

The first security risk event was the introduction of smart cards for transactions over the internet on behalf of the Alpha-Bank e-banking department and it was seen not only as part of the overall bank's business strategy but also as a security concern. Smart cards are credit-card sized plastic cards that have embedded microcomputer chips. They embody the type of authentication where one is identified by what one possesses. They are usually used in place of coins or tokens in mass-transit toll collection or for mobile phone security and access and even for network login. However, the issue was whether smart cards should be used in conjunction with a PIN (Personal Identification Number) for an extra layer of security.

The second security event as part of a security routine process was concerned with the use of firewalls. Firewalls are an essential part of network security. They are used to protect the internal network from external threats that can compromise data, assets and resources. A firewall is usually deployed so that everyone entering or leaving the bank's network must pass through it. Firewalls can be classified according to the firewall's intended use, its system architecture, and the way it uses filtering

technology. However, the security event that the Alpha IT group was concerned with, was whether to move deliberately the Web and e-mail servers, onto a third network that is set apart from the internal network but is still not completely on the outside. In this way, more access can be granted to them while still affording them some protection. This type of firewall network architecture is known as a "multi-homed firewall with a perimeter network".

Finally, the last security risk event was that of the server monitoring. Server monitoring is the implementation of a system that keeps vigilance over the health and status of a server. The more critical a server's function is, the more important monitoring becomes. As mentioned in section 4.2.2.3, the Alpha-Bank IT unit aims to improve its e-banking infrastructures through the re-organization and transfer of all systems necessary for the operation of a second server in Athens. In this way the IT group will ensure better access and response times and a more even distribution of the workload between Northern and Southern Greece.

However, the IT unit considered the substitution of its current monitoring method with the SNMP method in order to improve its intrusion detection systems. SNMP is actually a protocol that allows a program to either retrieve or receive information from a network node. SNMP actually utilizes a process called "traps". A device may have information it can share, such as device functionality and status, intrusion attempts, reboots, etc. This information is defined in a file called a MIB (Management Information Base). It can send an SNMP trap with this information to a server. Once the server receives the information, anything can be done with it, such as alerting the administrator by way of a pager or simply saving it to a log file. SNMP is mainly used to monitor the status of hardware although it can also be used to monitor the status of applications. Nevertheless, there was an argument between the e-banking unit and the IT group as another intrusion method could be used in conjunction with the current monitoring method while reducing implementation costs.

In the following, the issues of trust, culture and risk communication are discussed and analysed in the context of the performance pyramid model.

4.4 The Issue of Trust Within Alpha-Bank

In order to understand issues of trust within an organizational setting the use of an interpretive epistemology was employed. The hermeneutic circle was used to display and validate the theories, discussed in Chapter 2, underlying the performance pyramid model. During the interviews in Alpha-Bank there were issues that had to be defined properly in order to provide a clear insight into the research agenda. For example, when questions on the role and effect of trust on goal setting were provided to the interviewees then, the background literature assisted in providing definitions for reference.

As the interview technique took place between each respondent and the interviewer, it became clear how the construction of the questions focusing on trust, could be improved and become more precise. For example, when an interviewee was asked about the importance of trust within the IT group, it was brought to the attention of the researcher from the replies that trust was a sensitive issue with a multiple effect on the level of goal setting. Thus, by asking how trust affects goal setting within the group, different dimensions of trust were brought to the forefront such as trust to the IT manager, trust to other colleagues within the group, or trust to the higher levels of the hierarchy. All these dimensions together had an ultimate effect on the level of trust between the members of the IT group. However, using the same style of questioning resulted in a better data construction than previously. The study of Alpha-Bank assisted in refining the research techniques and clarifying issues that were not clear thus, avoiding any risks associated with the research data collection techniques.

Trust was an important issue within Alpha-Bank and it was considered as the basis upon which the organization has built its reputation. Alpha-Bank is the smallest organization, among the three case studies, established in 1991 with a business environment towards family-oriented values and beliefs. That means, the Alpha-Bank Group gives an extraordinary credit to relationships based on trust due to the fact of a small number of employees fully dedicated to the strategic vision of the bank, and due to the bank's new foundation. Given the fact that Alpha-Bank was one of the newly established banks in the Greek market in the last decade, its organizational structure is

oriented towards the investment of human resources, which creates the basis for a mutual trust relationship among its co-members.

When the interviewees within the IT department of Alpha-Bank were asked to define the importance and meaning of trust to them and to the group as a whole, they gave some of the following interpretations of trust:

"Trust, in professional terms, is the belief that the IT group members will give their best to an overall group effort to accomplish a given task" (Deputy manager networks) or

"trust means that one can rely on another to produce efficient work outcomes" (IT employee) or

"the intensity to depend on the team whereas the team depends on the intention of the individuals making the team to succeed" (e-banking manager) and

"the expectation that your efforts will be recognized and appreciated by the group" (e-banking employee)

Within Alpha-Bank there was a widely held belief that the people can depend on each other and to the top-management's support in order to overcome any possible obstacles. In the interviews held with the IT staff it was continuously mentioned that top-management support plays a critical role in the establishment of trust within the group. Moreover, the majority of the IT group members had worked together since the establishment of the bank and therefore trust was based on a long-term relationship between the employees.

Likewise, the IT employees through the years have co-operated successfully in a number of projects that results into confidence among them which further makes them believe they can depend on each other. The fact that the IT department has successfully completed a great number of projects assigned to the group has created increased levels of trust among co-members. As one of the IT deputy managers said:

"We worked together for more than 10 years now, and we've learned how to put things together and come up with the best possible solutions. It is not only the fact that we trust each other but also we have developed a certain level of confidence through successful project development and implementation which further led us to understand our potential as a group first and then as individuals".

Similarly, Alpha-Bank's employees and in particular the members of the IT group are also socialising together with their families outside the work environment. It is quite often that the IT manager organizes family group meetings such as dinner parties or social events, in order to bring closer the IT employees and their families and know with each other better.

Moreover, the IT manager at Alpha-Bank argued that trust can be viewed either in its social context or in its professional context. On the professional side, he said:

"The phenomenon of trust is established through transparent relationships and certainly not through decisions which cancel each other out every time e.g., if there is a decision that a particular project will be undertaken by one team and then the project manager changes his mind, this will create feelings of mistrust and disappointment in part of the initially chosen team. Thus the project manager has to explain his decisions to the team as well as what are the expectations of the team so as to maintain a level of integrity and confidence to his team in the long-run".

By asking if there are any other reasons for having high levels of trust, the respondents replied that another reason was due to the input of the human resources department. The human resources department is mainly divided into: 1) the department for development activities, which is responsible for the staff training i.e. educational seminars, organizational reports, educational sponsorships, and 2) the management part of human resources, which is responsible for staff recruitment, salaries, bonuses, staff insurance, health care.

It was argued that the human resources department plays an important role in establishing trust among employees since it is responsible for the promotions and monetary rewards allocated to the staff. As an example, the IT manager said:

"The human resources department has an important input in establishing and maintaining trust between members. When an employee is committed to his work and his performance is superior, you (as a manager) have to reward him otherwise your employee will lose interest in the long-term and may even give up his job for something else while the organization will lose a valuable and committed employee. Thus the human resources department through the promotions and rewards equally distributed to employees maintains their confidence and trust at high levels. An inefficient human resources department could have negative consequences and could even cause breaches in trust levels".

The IT manager also stated that trust is difficult to achieve as it takes time and effort to establish, while it is so easy to lose.

4.4.1 Trust in the Context of Culture and Risk Communication

Culture was also an important issue at Alpha-Bank, which will be discussed in more detail in section 4.4.4. The fact that Alpha-Bank was established in 1991 makes it a new organization with a fresh culture and innovative ideas, which are based on the beliefs and ambitions of the bank's employees. As one of the IT deputy managers put it:

"We feel part of this organization as the majority of us work together since the bank's establishment and our ambitions have been developed parallel with the bank's vision which was further developed from our personal input. Now, if we consider that our salaries have been increased in the last few years more than any other bank employees get, I think our input is being well appreciated".

However, all the interview respondents stated that trust plays an important role in the establishment of culture and it is a propensity of people within the organization to co-operate in order to produce positive work outcomes. In particular, the IT manager said:

"Trust is a perspective of culture within an organization. If people within an organization trust each other in their work relationships then the first thing to observe is that the culture must be strong independent of whether culture has other perspectives as well. Thus if an organization wants to improve the consistency of its culture, it has to start from the level of

trust between its employees. This is because when high levels of trust exist in an organization, the employees are more willing to co-operate and co-ordinate their activities in order to successfully complete a given task with effect, the organization to achieve more consistency within its culture and consequently more strength".

It has to be mentioned though that the interviewees within Alpha-Bank were provided with a definition of the issues under investigation and the rationale and assumptions behind the model were explained. For example, when questions were phrased in examples such as *"do you think trust has an effect on culture strength"*? Before the respondent replied, a clarification of culture was provided for purposes of clarity and focus on each issue under concern. This also assisted the research for the next case. In the next case, the question was clarified by providing the definition of culture strength provided by O' Reilly and Chatman (1996). In this way the investigation ensured the avoidance of any possible misunderstanding of the issues under study and the clarity of data achieved.

At Alpha-Bank all the interviewees within the IT department stated that although culture strength does not necessarily depends on trust alone, high levels of trust will indeed allow the identification of culture strength characteristics and in so doing, it will provide the conditions under which the group culture will become stronger. On the contrary, an organization may have a strong culture in terms of manuals and procedures but that does not necessarily mean that the employees have trust in each other and in the top-management. When the interviewees were asked how trust could provide those conditions under which a strong group culture will occur, they stated that when their efforts are recognized by the top-management then through positive attitudes, higher levels of co-operation and co-ordination of activities, culture strength will improve.

Likewise, trust had also an effect on the communication of security risk messages within Alpha-Bank. The interview respondents stated that the existing levels of trust within the IT group contributed to an efficient communication of risk messages with regards to the security of internet banking. In particular, the issue of internet banking security was characterised as highly sensitive and the development and implementation of security projects needed a good communication level between

project participants which was finally achieved due to the high degree of inter-dependence between them. A certain level of trust through multiple successfully implemented IT projects caused a mutual interdependence between the project participants, which was positively reflected on the way they communicated within the group. One of the IT employees in particular said:

"When you know you can trust your colleagues with whom you participate and especially the project manager, there is no reason to be suspicious of any decisions made during project development and implementation and therefore you are more confident to communicate and pass your knowledge and experience to others".

From the above it seems that a certain level of trust among the IT employees had an ultimate effect on the efficiency of risk communication. The trust IT employees place on top-management was reflected on the way they behaved within the IT group and communicated the risk messages among each other.

The investigation further focused on questions of risk perception in the context of internet banking security. The interview respondents characterised the security of internet banking as incontestable with a number of risk related opportunities and threats, which indicated a certain degree of people's perception on security issues. Based on the replies from the interview respondents, it was clear that the IT people within Alpha-Bank had a certain level of confidence on internet banking security risks, as they exhibited full awareness and knowledge of the risks entailed in internet banking. The data center deputy manager said:

"A reason that there is a certain level of good communication within Alpha-Bank and in particular within the IT group is the fact that the employees attend educational seminars every so often in order to keep up with the current market trends. In the case of the IT department every single member is fully aware of his/her responsibilities by constantly making appointments with the IT manager to discuss issues of high concern such as the security of internet banking. In the context of security I believe everyone's risk perception is based on the right criteria which is further reflected in project development and implementation".

As more information was obtained from practical experiences and opinions of the interview participants, other issues became clear for the issue of trust and risk communication. The communication of risks within the Alpha-Bank IT group was also efficient due to an efficient circulation of information between different banking units without undermining the activities of the IT group with regard to security. Although, there were different political agendas within different banking units, their overall effect was controlled. As argued, the efficient co-ordination of different group activities and information exchange was also a result of trust between different groups within the bank with an ultimate effect on communication. In saying so, each group within Alpha-Bank was focused as much as possible in within group activities while avoiding to come across over the activities of the IT group.

To confirm that the opinions and results being obtained were not those of few people, and that a biased view was not being obtained, the method of triangulation, where reference to bank reports and archival documents, was used. The reports entailed information about the different groups' activities and the degree to which their activities were related to the activities of the IT group in security projects. This proved to be beneficial since the information provided by one source was limited and therefore any possible gap was overcome.

4.4.2 Trust in the Context of Goal Setting

Goal setting was a consistent part of Alpha-Bank's overall strategy and as argued it was a process upon which the bank further develops its vision. Goal setting within the Group was very important and this was reflected in the participation of all the banking units in goal setting and most of all, in the participation of the majority of its employees. In particular, the participation of employees in decision making was considered very important and had a positive effect on the level of trust within and between the different units. As a result, the confidence levels between the employees were high since participation meant that their opinion was taken into consideration by the top-management and at the same time, they believed they made a contribution to the overall bank's success. This was not the case however in the next two case studies as will be discussed in Chapters 5 and 6.

Within the IT department people believed that trust plays an important role at the level of security goal setting in terms that one party (individual) can depend on another to co-operate in order to produce positive work outcomes. The interview participants stated that the trust they put in each other in terms of dependence on a given task, had an important effect on goal setting. In particular the IT manager said:

"It is important to have people that you know you can depend on to get the job done. In addition when we have to set some goals, knowing each other's capabilities and potential within the group makes things easier for you (as a manager) and then you can proceed to problems' solutions in a more efficient way. Trust gives you a sense of what your team is capable of and when you know that goal setting becomes more efficient".

With regard to the security risk event of firewalls, the IT manager argued that at the project goal initiation phase the level of trust between the members of the chosen team is important and has a significant role on the available options chosen. In particular, the issue of internet banking security is considered as highly sensitive since the internet is an open environment and any possible attack may originate from everywhere. Having trustful people in the team with internet expertise and people where the team can depend on, is very important in choosing the best available options.

In the case of firewalls the IT manager further replied: *"we were thinking to move the Web and the e-mails servers onto a third independent network in order to increase the level of firewall security. Because we had a number of significant projects at that time we thought to postpone the decision at a later stage as the e-banking and audit units were uncomfortable with the project available time and costs. However, as the deputy manager explained the benefits over the costs we felt that we should trust his expertise and move on with the project. Finally the project was successfully implemented and proved to be of vital importance to other applications as well".*

Thus, having knowledgeable and trustful people in the group saves time and effort of unwanted situations in project development and implementation and especially trust between the people in the project team has a positive effect on the efficiency of goal setting process. On the contrary, having people who do not have the necessary skills

and knowledge in internet banking projects may lead even to project postponement times or even to project failure. To this end, the IT manager plays a key role in project outcomes as he is responsible for choosing the right people for the project.

Similarly, all the interview participants stated that trust in the IT manager is very important for the successful implementation of projects as he must be supportive and assign reasonable and efficient goals to the group. One of the IT employees in particular said:

"The project leader, whereas in most of the cases is the IT manager, is a key success factor for any project development and implementation and is the one that the team depends on. When the manager is someone you know you can trust and that everything he does is for the good of the team then people's performance in terms of focus and motivation to achieve a given goal becomes higher".

Thus, based on the replies obtained from the interview participants, trust plays an important role in goal setting as it is a motivation for people to co-operate and efficiently co-ordinate their activities in order to succeed.

4.5 The Issue of Culture Within Alpha-Bank

The cultural environment within Alpha-Bank was characterised by the interviewees as strong, whereas within that culture each banking unit had its own sub-culture that exhibited similar attributes of the overall organization's culture. As mentioned in Chapter 2, organizational cultures is believed to provide a sense of control in terms of unifying the way employees process information and behave within the organization, which increases the predictability of organizational behaviour (Trice and Beyer, 1993).

While there are varying definitions of culture, Schein's typology of organizational culture was used in order to define the culture within Alpha-Bank and in particular within the IT department. Schein (1992) divides an organizational culture into three main levels which are- artifacts, values, and assumptions. A set of questions asked to the interviewees with regard to culture is being shown in Appendix B3. In the

following a description of the Alpha-Bank/IT group culture is provided which is derived from the interviews, the investigator's observations, and some analysis of secondary data such as white papers, reports, and documents.

The IT department of Alpha-Bank was housed in modern spacious offices located outside the city of Thessaloniki in a private owned building with high physical security measures. An indication of the department's high importance was the guard outside the building, video cameras used to control access inside/outside the building, and the passwords or identities required from visitors in order to gain access to the building. The IT staff was dressed in a casual way and each member was speaking to his/her colleague with his/her first name.

The IT staff had a combination of the neutral reference to the clients as "customers" and the more social welfare orientation of "partners". While staff members seemed to intentionally use the language of "partners", they used the term "customers" in more informal conversations. Yet, the IT manager described how the use of the term "customers" is more to conform to the language of business than a reflection of how Alpha-Bank personnel view the customers. In fact, all the interviewees- especially the e-banking unit manager and the audit manager- frequently used the term "our partners" and all they meant customers. Accordingly, the language of the IT department can be referred to as social welfare oriented.

Alpha-Bank has gone to great lengths internally to produce clarity and consensus on its functions with a similar effect on its banking units. The bank not only has a mission statement and accompanying "value statement", but it is also producing a "code of ethics" among individuals who may possibly come in dispute. That was a precautionary step in part of the bank to avoid any possible future conflict and to make sure that there is a standard process to settle things down in the occurrence of such possible case. As the audit manager stated:

"Sometimes organizations who expand their business and become even bigger lose some of their identity on the way to transformation. Although this is inevitable, the existence of ethic codes helps to minimize any possible conflicts of interests among people and different units

within the bank and these codes and norms have to be constantly updated and controlled. In this way, you make sure the culture of the organization remains strong and cohesive".

One of the values of Alpha-Bank is its human attitude towards the customers. All interviewees believed that customers have a share of the bank's success through their loyalty and that are capable of rewards. As the e-banking unit manager said: *"Loyal customers are worth a loyalty reward"*. To this end, the bank is having under its supervision a new reward scheme for its customers which reflects this value.

Consistent with a human attitude towards customers was a wider value about the bank's mission. The bank and its staff were motivated by a value that their organization be a humanizing element within the traditional banking system. The IT manager stated that the bank's relationship to its customers was to *"serve as a humanizing element"* in the way to create a contemporary and flexible financial institution which would totally cover the banking needs of its customers-partners and would dynamically claim a substantial portion of the Greek banking market.

Another value in Alpha-Bank was in staff relationships. Collegiality and teamwork among staff was valued, especially by senior staff. In fact, most interviewees stressed the value of participation by the staff. As the IT manager said*: "Staff has to participate since its contribution is vital"*. Consistent with the sense of participation is a collegiality among the staff. In addition, staff members are encouraged to innovate. As one of the IT deputy managers said: *"There are times the IT people want their own space to innovate; they feel their job is highly innovative and want to prove that"*. However, only two of those interviewed did not relate collegiality as an assumption of culture.

Moreover, an assumption of Alpha-Bank's organizational culture was about its core mission. Embedded as part of the way Alpha-Bank operates was the assumption that providing information and financial advice to the customers is the core mission. All the interviewees stated that the core mission was information and financial advice. As the audit manager said: *"Our mission is to provide information and financial advice to our customers-partners so that they can increase their wealth"*. The bank emphasised this by having more staff assigned to the information and financial advice

services process and through an on-line option on its Web-site. To this end, the bank had established a new mutual funds scheme to assist customers to increase their returns with lower market risk.

The second major assumption that defines the organizational culture of Alpha-Bank and in particular of the IT group was that Risk Assessment is a Group process. The interview respondents replied that risk assessment was best done on a group basis. While the researcher's questions focused on the dichotomy usually associated with discussions on security risk assessment (i.e., whether risk assessment should be separated from risk management), all respondents indicated the assumption that risk assessment was best done on a group basis and it was part of the risk management cycle.

4.5.1 Culture in the Context of Risk Communication

The culture within Alpha-Bank was described as consistent with a set of values and beliefs and oriented towards the investment of its human resources. As stated, culture strength had a positive effect on the communication of security risk messages within and between banking units. In particular, the interview respondents stated that the culture strength within the group, in terms of co-ordination and co-operation of activities, had an effect on how the messages were transmitted, received and embedded in the context of internet banking security.

From the interview replies, it seems that the people within the IT group had a great sense of duty and that the culture allowed them to use their individual intellect which was reflected on the communication between them. One of the IT employees said:

"Having freedom of individual intellect allows you to communicate efficiently your knowledge and experience to the group as compared to organizations with stubborn cultures where everyone has to ask permission for any activity".

The communication within Alpha-Bank was taking place through various means. These included e-mails, telephone, and sometimes tele-conferencing. This was often the case between the IT group and the e-banking unit since the first group is located in

the Northern part of Greece while the second located in Athens. In fact, the IT department was investigating new means of communication and tele-conferencing was at an experimental phase. The use of e-mails however was the most common mean of communication between different banking units due to easy of use.

As the questions were focusing on other aspects of communication, it became evident that the size of the IT group structure was also beneficial to the overall communication effect within Alpha-Bank. For example, when the IT systems deputy manager was asked the type of question *"do you think there are other means though which culture has an effect on communication"*? he replied:

"The communication within the IT department is also very efficient because the group is consisted of 60 employees who have daily contact within the group. Therefore, the group is flexible enough due to its small-scale structure which has also an impact on the way communication takes place".

With regard to the communication of firewalls, smart cards and server monitoring, the systems deputy manager said:

"We suggested these security related projects to the auditing and e-banking units as a standard security routine process by sending them in advance an e-mail attachment. The audit manager got back to us asking the details of the particular projects and then we sent to him the proposals with all the details but we also sent in advance the same copies to the e-banking unit".

From the above quote, it appears that the communication of messages was efficient since the IT group always kept the other units of the bank aware of any project development. The IT group was passing the messages efficiently in order to avoid any confusion among teams and the manner by which the messages were circulated was straight-forward. This however was a result of a strong consistent culture within Alpha-Bank and between different business and technology units since the co-operation and co-ordination of activities was efficient.

In addition, the participation of the IT employees in decision making with regard to internet banking security had a positive effect on the way security communication messages were transmitted and embedded within the group. As the IT employees felt that their opinion was important they communicated with each other more efficiently. The efficient communication of security risk messages was also reflected on the way the IT manager and group managed the security risk activities. For example, at the goal execution phase the IT manager arranges regular meetings within the group with regard to internet banking security. Based on a checklist, shown in Appendix D3, the group discusses all possible risk sources and decides on the relevant risk factors. At this stage, it was agreed that the efficient co-operation and co-ordination of risk activities is a result of the strong culture within the IT group, which was further reflected on the efficient communication of messages between participants.

4.5.2 Culture in the Context of Goal Setting

The culture within Alpha-Bank had also an effect on the efficiency of the goal setting process. All the interviewees stated that the cohesive strong culture within the IT group plays an important role on the level of security goal setting. Given the meaning and definition of strong cultures to the interviewees, they all agreed that in strong cultures goal alignment is easier to achieve (Sorensen, 2002) which eventually has an effect on the way security goals are being set.

Moreover, in Alpha-Bank IT group the people were motivated to perform in a high standard as they felt free to participate in the group's overall activities. As previously explained, the strong culture of Alpha-Bank provided an efficient co-ordination of activities between the employees, which ultimately provided clarity in goal achievement (Cremer, 1993). The IT manager in particular said:

"When the culture within the organization is strong, there is an efficient co-ordination of activities and clarity in goal achievement. Certainly there are benefits of having a strong, cohesive culture and I believe one of the benefits is reflected in goal setting".

In a strong culture, people know a certain course of action which ultimately has a positive effect on how security goals are being set. With regards to the security of internet banking an IT employee said:

"Goal setting within the IT group is based on the same principles with the overall goal setting procedures followed by the bank although the issue of security requires a more delicate approach due to the negative consequences of the subject matter. Similarly, the security of internet banking is a very sensitive issue and having a strong culture provides goal alignment within the team, clarity of goal achievement and a purposeful action from the staff in dealing with possible security risk threats".

As argued, the strong culture within the IT group provided a motivation for employees to dedicate their efforts to common group goals (Deal and Kennedy, 1982; Kotter and Heskett, 1992) which was also reflected in the process of internet banking security goal setting. On the risk event of server monitoring the e-banking manager said:

"We thought to transfer all systems for the operation of a second server in Athens in order to allow for better internet access and response times through an even distribution of the workload between Northern and Southern Greece. At the project initiation phase we allocated different activities between the e-banking unit, the IT group and the audit department. The project estimated time was 2 months and we finished successfully on time. That was, I believe, the result of an efficient co-ordination of activities between the units which further can be attributed to the strong cohesive culture of Alpha-Bank and due to the efficient circulation of messages between the units".

As previously mentioned, the strong culture within Alpha-Bank can be attributed to the small size of the organization and the flexibility it allowed in decision making and internal procedures.

4.6 The Issue of Risk Communication Within Alpha-Bank

With regard to the risk communication, the researcher intended to identify several issues. Initially, the researcher intended to identify how the process of risk communication was taken place within Alpha-Bank. As mentioned, the IT group

worked in one place and therefore there was no potential to utilise e-mail and other forms of electronic communication within the group. Face-to-face communication was the main mode employed and assisted in clarifying issues in a fast and reliable way.

Thereafter, as more information was obtained both from the literature survey and the practical experiences, other issues became vital for the investigation. Issues such as what was the perception of security risks by IT employees, what other factors may had an input in good communication among the members of the organization. From the interviews within the IT group, it appears that the communication of risks was efficient also due to a certain, confident level of risk perception in part of the IT employees. One of the reasons for the good communication within the Alpha-Bank IT group was the fact that the employees have an educational background which was argued to have an important input in how people perceived security risks. In particular, 30% of the bank's employees hold a Bachelors Degree, 6% have attended postgraduate studies and hold a Master or PhD and 19% have Diplomas or Certificates from private Colleges. The e-banking unit manager specifically said:

"The fact that many people within Alpha-Bank hold a degree it is an overall advantage to the bank and the manner we proceed to decisions with a particular effect on the communication between us. Having education skills saves you time and effort and provides focus to the problem itself".

The communication of security risk messages with regard to internet banking was efficient due to the knowledge skills of the IT and e-banking units on the product. Although, there were not security people within the group, programmers and/or IT people had knowledge on specific security issues. The majority of the IT employees were attending educational seminars on e-commerce and internet banking applications and they were aware of the possible security threats coming on-line. For example, when one IT employee was asked on the importance of internet banking security he replied:

"The security standards in on-line transactions have been upgraded so much nowadays that I believe going to a branch is more risky than executing a financial transaction through the

internet. A few years ago I had my reservations about the security of internet banking but now I think it is safer than ever".

However, the IT group in Alpha-Bank had also close links with third party consultants on security issues with whom an exchange of knowledge and expertise was taking place. When the IT manager was interviewed on the security of information systems and internet banking, he mentioned that the bank was in the process of recruiting new people with specific security skills in an attempt to establish an in-house software development sub-division focusing exclusively on security issues. The IT manager and group were also in close contact with Universities and Colleges in order to exchange knowledge on current security trends and because the bank co-operates in a number of projects with the academic community. When the IT manager was asked to provide an example of how the exchange of knowledge may have an effect on the efficiency of risk communication he replied:

"The communication of security within the IT group is efficient because all of my people keep up with the latest security trends especially on internet banking issues and have the required knowledge on security issues with regard to internet banking. Although you can't predict any security threats, you can be prepared. The problem however could be part of the hardware/software developers in failing to meet the product specification standards or mistreating confidential information. However, if this is the case, we hold policies and procedures against which we are protected and thus the communication becomes easier".

The research questions then focused to any possible problems of communication within the IT group, e.g., if there were any factors affecting the perception of risks within and between different banking units. In doing so, it was revealed that the perception of risks within different units of Alpha-Bank was not always the same. For example, the business units were more concerned with credit and interest rate risks rather than technology risks. As the researcher asked on the impact of such differences on communication, the respondents replied that those differences were under control in the sense that each unit did not come across over the activities of the other units. On this issue the manager of the audit department commented:

"It is quite a phenomenon every time we have to discuss upon funding the different units within the bank struggle to get a great share of funds. This is where sometimes a conflict may arise due to different investment needs but the ultimate impact is minimal because we know what is the overall benefit for the bank".

Thus, it is obvious that differences in risk perception did not pose any serious obstacles in communication because everyone knew the potential of each different banking unit and particularly that of the technology group.

4.6.1 Risk Communication in the Context of Goal Setting

As the interview process continued, the researcher focused on questions of the general type *"does an efficient communication of risks have an important role or input in the process of security goal setting"*? Although, that was initially a general question, it obtained instant response on the issue under concern. The IT manager stated that an efficient communication within the group was necessary at the project implementation stage, as the exchange of know-how must be communicated efficiently among the project participants.

In the event of smart cards though there was an argument between the e-banking and IT units which was based on whether to apply a PIN (Personal Identification Number) with the introduction of smart cards. There are mainly two types of smart cards, those that require contact with a reader and those which need to be in close proximity to an antenna. A contact card has a small gold chip on its surface which stores information while the contactless card has a microchip embedded within it and an antenna coil which makes contact with a receiver some distance away using radio frequency signals. When the e-banking manager was asked upon the event he replied:

"In the beginning we thought (the e-banking unit) that using a PIN would be unnecessary since smart cards with microchips are fairly secure and that customers on top of that would feel inconvenience in using them because they would have to remember an extra PIN among others. However, we were the first to introduce smart cards in the Greek banking industry and the IT manager insisted that we should take precautions in order to avoid any 'breaches' of our reputation. Having considered all the available options we agreed to introduce a PIN".

As previously described, the efficient communication of security messages was also a result of a certain, knowledgeable perception of risks among the IT group employees. Using this experience, then the questioning was posed in a more appropriate manner. The researcher then asked *"At what stages of goal setting is communication vital"*? *"How the perception of risks affects the manner by which goals are being set"*? This form of questioning led to the conclusion that an efficient communication of risk messages was necessary at the stages of selecting the identified risks and maintaining control of the goal activities planned since the group activities have to be in co-ordination with the overall activities of the bank.

4.8 Analysis and Synthesis of the Findings

4.8.1 The Interrelationship of Trust, Culture and Risk Communication

An issue that has to be considered when analysing the results of a case under study is that interpretivism is not used to report facts but rather to report the interpretations of other people's interpretations (Walsham, 1995). To this end, in order to avoid situations where inefficient interpretations of data can be made, the method of data triangulation was also used. The different dimensions of the socio-organizational aspects within the suggested performance pyramid model, assist in the presentation of the empirical findings and the analysis of the data obtained. In doing so, in the previous sections of the chapter, the contextual richness was provided, with the in-depth descriptions regarding the interrelationship and effect of trust, culture and risk communication in the context of goal setting, respectively for each case.

To determine the relevance of the empirical evidence to theory, reference to the theoretical concepts within the performance pyramid model was continuously made. Further explanation of the analysis techniques is provided in Appendix E2.

The case of Alpha-Bank provided interesting results with regards to trust, culture and risk communication within the performance pyramid model. The results show that trust is an important issue within Alpha-Bank and it is the basis upon which the organization has build its reputation. In particular, the people within the IT department of Alpha-Bank believed that they can depend on each other and to the top-

management for support in order to overcome any project difficulties. Similarly, the IT employees have co-operated in a large number of projects successfully implemented which further results into high confidence levels among them.

Likewise, it was argued that high levels of trust within the IT group provided the conditions under which a strong culture within the group occurs though *positive attitudes*, *higher levels of co-operation* and *co-ordination of activities*, as well as *employees'* satisfaction towards the top-management that their efforts will be appreciated. However, in strong cultures there are widely shared and strongly held norms and values that is believed to lead to performance benefits such as enhanced co-ordination and control within the organization, increased employee effort, and improved goal alignment between the organization and its members (Sorensen, 2002). Since those benefits are characteristics of strong cultures then high levels of trust through the same characteristics provides the conditions under which a strong group culture occurs.

Trust within the Alpha-Bank IT group, played also an important role in the communication of security risk messages within the group. In particular, the issue of internet banking was characterised as highly sensitive and the development and implementation of security projects needed a good communication level between project participants which was finally achieved due to the high degree of inter-dependence within the IT group. Specifically, it was found that trust between group members provides the conditions under which an efficient communication of security risk messages occurs through *positive attitudes, employees' satisfaction to top-management decisions, and employees' motivation*. Trust of the motives, attitudes and beliefs of the 'other side' makes it easier to listen to, let alone to accept and respond respectfully to what one's opposite party is trying to communicate.

The communication of security risk messages within the IT group was also characterised as efficient due a certain, knowledgeable perception of risks among the IT employees, the efficient circulation of information between different groups and the small size of the bank, which was also reflected on the IT group's flexibility in decision making.

The culture within Alpha-Bank was characterised as very strong and consistent with a set of values and beliefs and oriented towards the investment of human resources. All the interviewees stated that the culture strength within the group, in terms of co-ordination and control of activities, had an important input in how the messages were transmitted, received and embedded in the context of internet banking security. By using the method of triangulation and cross case patterns (Miles and Huberman, 1994) it was found that a strong culture provides the conditions under which an efficient communication of risks occurs through *enhanced co-ordination and control within the group, increased employee effort, and employee's motivation to contribute to the group*.

Similarly, the communication of security risks within the IT group was characterised as efficient due to the high levels of trust among employees and of the strongly shared values and beliefs consistent with the overall Alpha-Bank's culture. It was found that there were not any particular problems in communication since the small size of the bank allowed flexibility in decision making. Although, the efficient communication of security risk messages was also attributed to the same, knowledgeable perception of risks among the employees which was a result of good educational skills and on the efficiency of co-ordination and control of group activities.

4.8.2 The Effect of Trust, Culture, Risk Communication in Goal Setting

Goal setting was a consistent part of Alpha-Bank's overall strategy and a process upon which the bank further develops its vision. Goal setting within Alpha-Bank was very important and this was reflected in the participation of all the banking units in goal setting and most of all, in the participation of the majority of its employees. The participation of employees in decision making was considered very important with an ultimate effect on the level of trust within and between different banking units.

However, trust played an important role in goal setting in terms that one party can depend on the willingness of another party to co-operate efficiently in order to produce positive work outcomes. In addition, depending on the knowledgeable and trust of people within the group saves time and effort in goal setting activities.

The culture within Alpha-Bank was also the reason of having an efficient goal setting process. All the interviewees stated that the cohesive strong group culture within the IT department plays an important role on the level of security goal setting and that employees are motivated to perform at a high standard, as they feel free to participate in the group's overall activities. The overall strong culture of Alpha-Bank provided a more efficient co-ordination and control of goal setting activities between employees, which ultimately provided clarity in goal achievement.

Risk communication played also an important role on the level of security goal setting as the interviewees stated that at the *goal execution phase* communication was a vital aspect of goal achievement and that a possible breach in communication may have negative consequences in the projects' development and implementation.

4.9 Conclusions

This chapter began by describing the background of the Alpha-Bank case in the context of its history, business, infrastructure, management and organization on a global scale, as well as its recent developments. Then, it described and analysed the process of goal setting within its 'real life'. Goal setting was a vital process of the bank's overall strategy and it was believed to be the basis upon which the bank further develops its vision. Section 4.3.2, analysed goal setting in the context of risk management with a focus on internet banking security and the findings showed that goal setting is mainly divided into three phases: goal initiation phase, execution phase, and compilation of an evaluation report. Therefore, the main research question of whether IT managers and groups set security goals with regard to the management of the integrity, confidentiality and authenticity of data through the internet banking was answered. The process of goal setting with regard to internet banking security was based on the use of checklist in order to ensure the a careful implementation of security goals is continuously taken place. By this way, the IT group ensures that information data retains its integrity, confidentiality and authenticity through the internet banking channel.

Then, the investigation proceeded to the analysis of the interrelationship of socio-organizational issues such as trust, culture and risk communication within the performance pyramid model and their possible effect on the level of security goal setting. The results show that there is indeed an interrelationship between trust, culture and risk communication with a subsequent effect at the level of security goal setting. More specifically, that trust provides the conditions under which a strong culture and an efficient communication of risks occur mainly through the employees' positive attitude, higher levels of co-operation, an efficient co-ordination and control of activities, as well as employees' satisfaction towards the top-management that their efforts will be appreciated.

It was also found that the culture strength within the IT group in terms of co-ordination and control of activities had an effect on how the messages were transmitted, received and embedded in the context of internet banking security. That is, the communication of security risk messages was characterised as efficient due to the benefits that strong cultures offer such as clarity in goal achievement and goal alignment.

The case of Alpha-Bank was prior used to refine the interview techniques as well as the questions and to validate the rationale and assumptions made in chapter 2, in the context of the performance pyramid model. The empirical findings drawn from the case of Alpha-Bank will provide the necessary ground for analysis, comparison and discussion of the results obtained from cases with different organizational structures such as Delta and Omega-Bank, discussed in Chapter 5 and analysed in Chapter 6.

Chapter 5: Delta and Omega- Banks: Some Preliminary Findings

5.1 Introduction

This chapter describes and discusses the cases of Delta-Bank and Omega-Bank used further for the purpose of this investigation. The description and analysis of the Alpha-Bank case, in the previous chapter, has shown that there is indeed an interrelationship between trust, culture and risk communication with a subsequent effect on the level of goal setting. However, these results are based on an organization with a small structure size whereas the values and beliefs of the organization are strongly held and widely held among its members. Thus, the investigation intends further to validate if the results obtained from the case of Alpha-Bank apply to cases with different organizational structures such as Delta- and Omega-Bank.

To this end, this chapter is mainly divided into two sections. The first section discusses the case of Delta-Bank with a medium-size structure while the second section focuses on the case of Omega-Bank with a large-size structure. Similarly, the chapter provides a brief background of the Delta and Omega-Bank cases in the context of their history, business and management as well as recent developments in their organizational structure. The process of goal setting in the context of risk management within both organizations is discussed as well as the issues of trust, culture and risk communication within the performance pyramid model context.

The use of interpretive epistemology in this investigation proved to be vital in the collection and analysis of data in the context of the performance pyramid model. Prior to conducting the investigation each prospective interviewee was told of the purpose of the research, the research procedures as well as the benefits of participation to the organizations and particularly to the IT groups.

5.2 Case Study Two- DeltaBank

5.2.1 Background to the Organization

Delta-Bank is a semi-public in nature bank established in 1907 and it is one of the largest commercial banks in Greece. The bank's vision was:

"to create a large, modern and flexible financial group that will completely satisfy the needs of individuals and companies".

At the end of fiscal year 2001, the bank had total assets of more than Euro 20.5 billion and profits after tax amounted to Euro 282.8 million. Delta-Bank at 2001 figures, employed 6,912 people with a network of 370 branches, 572 ATMs, 56 AEMs, 14 exchange bureaux and 70 Kiosks, of which 7 can also operate as Kiosks-exchange bureaux, since beyond automatic transaction machines they also feature employee posts. Similarly, the bank operates in Germany through a subsidiary bank with a network of six branches while the bank began operations in Cyprus with five branches. Delta-Bank has also subsidiaries in Bulgaria (with a network of six branches), Romania, Georgia, Albania, and Armenia.

The bank, in order to meet the demands of its customers and companies, has developed intense activity in financing sectors such as insurance, investment, venture capital, factoring, leasing, mutual funds, and securities and provides a wide range and substantial number of financial products and services.

In June 2000, Delta-Bank entered into a strategic alliance agreement with 'CA' an international banking group with the aim of exchanging 'know-how' and exploiting the comparative advantages of the two groups. After the merger three joint ventures have been established, Delta Asset Management S.A., Delta Life S.A. and Credicom.

Delta Asset Management S.A. is involved in the management of institutional investors' assets. The Delta Group participates with a share of 80% in the new company and 'CA' Asset Management participates with a share of 20%. Delta Life S.A. is a joint venture between Delta Group and Predica in the field of bancassurance. Delta and Predica participate with an equal share of 50% in Delta Life S.A.. Predica is

one of the leading companies in the field with 16 years of experience and has transferred its 'know-how' both regarding the design of products as well as the information technology systems to be used. Credicom is a joint venture between Delta and Sofinco. The company is active in the field of consumer credit in co-operation with commercial firms and provides consumer credit through points of sale.

5.2.2 Electronic Banking

Delta-Bank, in order to improve the services and products it provides to its customers, launched the Internet Banking product in 2001 and offers a wide variety of services and products online. The bank's web site is especially designed so that the information provided is target market specific. It is user-friendly and provides easy access to information on the Group's products and services. The bank's specialised services are easily accessible and are split into 5 categories: *accounts, portfolio of shares, exchanges, payments to thirds parties, and other services.*

In the *accounts* section customers have the possibility to view their accounts, obtain information about their account i.e. financial transactions, obtain a copy or save transactions into a text format, and analyse and control their personal accounts. The category of *portfolio of shares* gives information about the customers' portfolio management, control of orders for buying/selling shares, and information about trading shares. *Exchanges* allow the customers to transfer funds between accounts, pay debit/credit card instalments, order check books, and report any card loss.

Moreover, Delta-Bank provides a whole new range of *other services* through its web-site such as information obtained for IBAN (International Bank Account Number), make payments to IKA (Social Security), TEBE (Freelance Professionals' Social Security) payments, and VAT via Taxisnet.

The internet banking security level at Delta-Bank is based on the SSL-128bit security protocol while the Web site has been especially designed to work with Microsoft Internet Explorer. Usually when customers want to apply for an online account the bank sends a letter including the password and username. The customer in turn has to

access his/her account in the first time and change the password in order to secure that the access to the account is limited exclusively to them.

5.2.3 Technology and Operations

Delta is investing considerable funds in upgrading its systems and their infrastructure as well as its telecommunications network by applying a Network Management System (NMS) and infrastructure capable of supporting VOIP technology. The developed infrastructure is able to support networks within the organization (intranet) as well as communication with the external environment (internet, extranet).

Delta-Bank has also restructured its IT security systems by instituting a security policy which is realised not merely via IT applications, but also by procedures covering the entire operation of the company. At the end of 2002, the bank had also established the operation of the Disaster Recovery Center.

Furthermore, in 2001 the bank replaced its OS2 operating system with the new WINDOWS 2000 platform. The uniform platform of the operating environment and the software of the applications in the bank's branches, in conjunction with the upgrading of the branches' technological infrastructure, provide new opportunities for a better and qualitatively upgraded response of the bank to the requirements of its customers.

In 2001, the bank upgraded its mainframe systems by the installation of the new SIGLO platform across the branch network. The system services the provision of loans to the bank's clientele of retail customers. Similarly in the context of applying new, operationally and technologically upgraded systems the bank installed a decentralised SWIFT message management system, and undertook the trial operation of automatic SWIFT message production and dispatch from branches without the intervention of the central services. It is also preparing the application of IBAN numbers to every customer account in accordance with international standards, and the transfer of funds via modern systems, such as the DIAS TRANSFER. The bank also participated in the interbank DIAS DEBIT system for submitting corporate VAT

statements via the Internet and in the DIASPOS system for making tax payments via POS installed in tax offices.

5.2.4 Risk Management

In order to respond to market conditions, in year 2001, Delta-Bank completed the infrastructure of its systems for the identification, monitoring and management of market risk on a daily basis. In particular Delta-Bank applied internal models for estimating Value at Risk using the historical simulation method and systematic efforts were also made to apply other methods such as Monte Carlo. In addition, 'perfect portfolio' methods were adopted in order to determine the appropriate structure of the bank's position, and risk limits were calculated within the context of desired return and risk.

These new methods and approaches constitute the main axes on which risk management at the Group level will be based. The bank has already proceeded with the necessary preparation in order to monitor on a daily basis, returns and risks across the entire range of commercial portfolios of its subsidiaries. During 2001 it was also decided to create Group Treasury and Group Risk Management in order to improve the effectiveness of the implemented policies applied at Group level concerning treasury management and avoiding excessive exposure to risk.

5.3 Social and Organizational Issues in Delta-Bank

5.3.1 Goal Setting and Security Within Delta-Bank

The case of Alpha-Bank assisted in refining the questioning techniques and clarifying issues that were not clear from the literature review so that the risks involved in collecting and analysing inefficient data could be reduced. Thus, from the Alpha-Bank case the researcher was able to modify the questions in a manner that the most relevant information could be obtained.

The case of Delta-Bank has shown that goal setting was an integral and consistent part of the bank's business strategy. All of the interview respondents stated that goals are

set on a regular basis within each banking unit respectively, and that goals represent the identity of the bank's business plan. The goals in Delta-Bank are always business oriented and even within the technology banking units the main goal is cost reduction and automation of processes. In particular, the manager of the IT and operations group said:

"What IT people don't understand sometimes is the fact that we work for the benefit of the bank's business requirements by reducing the operating costs and by offering to our customers fast and reliable services online. Therefore, when we choose a specific software we do so, not only on the basis of high product specification standards but mainly on the basis of cost reduction and user friendly requirements".

Goals in Delta-Bank are considered in terms of projects and they come either from the top management or from the different units of the bank (Appendix D1 shows the organization units of Delta-Bank). Goals are not introduced as simply an idea but rather as a consequence of the business needs, which is further based on current competitive market forces. Every goal within Delta is translated into a project and according to the banking unit in which goals are being set the nature of goals has a different scope. The nature of goals within the IT unit is always technical although behind every technology project there is a business need. Internet banking for instance was initially introduced in order for Delta-Bank to retain its customer base and expand its business horizons. The marketing plans deputy manager said:

"Internet banking was a tool originally used for marketing purposes. If other banks offered internet banking, and you really wanted to keep up with competition, you had to do the same. That was our initial goal although through time internet banking turned out to be a very efficient tool to provide financial products and services to our customers online given the fact that internet banking usage is still on the increase".

Nevertheless, the procedures according to which different banking units set goals have to subscribe to the organization's overall goal activities plan. Specifically, there is a manual based on which each banking unit proceeds to goal setting activities. This manual actually describes the -*what, how, and when*- questions with regard to goals. Since goals in Delta-Bank are considered in the form of projects then the questions

become: 1) *What* is the ultimate purpose of the project, i.e., the project's nature, 2) *How* will be achieved, i.e., by what means, 3) *When* will it be achieved? i.e., specific timetable. After these questions have been defined and considering that a given project has been accepted for funding, then the manager of each banking unit respectively has to proceed to the project initiation phase.

Goal setting within Delta-Bank with regard to the security of information systems is distinguished into the project initiation phase, execution phase, evaluation phase and monitoring phase. The process is similar to that in Alpha-Bank with the main exception that the monitoring phase is considered as an additional phase rather than part of the execution phase. These goal setting steps are depicted in Figure 9 below.

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

Figure 9 Security Goal Setting in the Context of Risk Management (Delta-Bank)

Likewise, at the goal execution phase the first step is the identification of risks. The goal at this stage is to identify all the possible risks that may exist with regards to the security of information systems. In the case of internet banking, the Delta IT and operations group uses a checklist which prioritises the possible security threats from internet banking usage. During the interviews with the IT group, the IT manager was asked if it was possible to provide such a checklist but for security reasons the checklist remained confidential. However, the IT manager mentioned that internet banking risks are prioritised according to their possible impact and that the nature of

those risks is usually concerned with internet banking security policies including ISPs contracts and general outsourcing, physical risks, networks, monitoring, and controls. The second step is the estimation of risks identified. The IT and operations group has to estimate the risks' likelihood, impact, and timing in order to determine uncertainty levels and in so doing, to prioritise risks and goal setting activities. This step is different though from the case of Alpha-Bank, where the IT group selects between identified risks and then proceeds to the final selection of security risks.

At the third phase, the Delta- IT and operations group proceeds to the evaluation activities in which the group actually evaluates the levels of risk acceptability. If the risks identified have an acceptable level of risk exposure (i.e., they can be controlled) they are undertaken and new goal activities are being set; otherwise, if the risk exposure is too high, alternative means are generated. The group uses different evaluation methods, some of which include simulation techniques (e.g., Monte Carlo) or decision trees. At the end, the IT and operations unit produces an evaluation report which incorporates each relevant risk factor, the measures associated with it and the goal activities planned.

Finally, the last phase of security goal setting is the monitoring of risk activities. In this phase the IT and operations group monitors the status of the identified and selected risks and collects information, which can be used as lessons learned for future activities. At this stage, similar to Alpha-Bank, the group decides whether or not the previously taken measures compensate for the risk choices made or to formulate additional measures for existing risk factors.

In the process of goal setting, the IT manager plays an important role. It is the one who co-ordinates the group's activities and makes the team believe that the goals are feasible. When the IT manager was asked on his role in the group's goal activities, he replied that the difficulty from the technology side is to convince the business people that a particular IT project proposal offers benefits which the organization cannot afford to ignore. This is the so-called Business-Technology Gap. In particular, he said:

"The bank is a financial institution aiming to increase profits year after year and in so doing, the main criteria for business managers are based on tangible 'measured' benefits. However,

in the context of information technology, the benefits are quite often intangible, such as faster response times, more reliable on-line services, etc. which makes it more difficult to establish your reasons for the necessity of an investment. This a reason that goal setting often works not for those that invest in ideal technology but rather for those who invest on technology that cuts costs".

That above quote actually means, that business managers set business goals based on measures such as ROI (Return on Investment), cost-benefit analysis or ROM (Return on Management), while in information technology the absence of such measures makes it more difficult to specify the needs for IT investments. However, when the IT manager was interviewed, he mentioned that the IT group is considering of new ways of measures of estimating the value of IT investments and in particular of measuring the performance of a technology group. An example of such measures is included in Appendix D2.

5.3.2 Security Risk Events in the Context of Internet Banking

As more information was obtained from both the literature review and the practical experiences on goal setting, other issues became vital for the research. The investigation then focused on possible security risk events in the context of internet banking, i.e., what was the impact of such events on goal setting as well as on socio-organizational issues such as trust, culture and risk communication within the groups.

Internet banking in Delta-Bank was actually introduced in year 2001 as a fully comprehensive online banking channel to provide a wide range of financial services and products to its customers. Before 2001, the bank used to maintain a Web-site only for information-oriented purposes about its products and services, available only through its main branch network. Given the recent development of its internet banking infrastructure, the Delta IT and operations group is in the process of establishing its internet banking security policies and continuously reforming its marketing strategy for the promotion of its products and services available through the internet banking channel.

However, the IT and operations group manager as well as the other interview participants were being asked what kind of security risk events may had occurred, within Delta-Bank, in the context of internet banking. The discussion was focused on two main events concerning the server security and vulnerability assessments in the context of security policies.

In the first main security event, the IT and operations group was considering the upgrade of its system fault tolerance level. The main reason was that, since 2001, the bank had twice experienced failure in the hard drives. Fault tolerance is a security feature which is invulnerable to any kind of hardware failures, including hard drives, network interface cards, or controllers, which actually means that one or more components are tolerant to failure. In particular, if a component goes faulty there would be another available to take its place. However, the main decision had to be made on the type of fault tolerance needed to be installed providing the best solution at the minimum cost. The decision was to apply the clustering technique although there were communication problems between project teams as will be discussed in later sections.

The second main security risk event was the issue of vulnerability assessment. Vulnerability assessment allows companies to focus information security spending on areas where it is most needed. This is appropriate when security spending is a top priority but the proper amount to spend has yet to be determined. However that was an important issue discussed in the context of security policy. A security policy is a documented high-level plan for organization-wide computer in the context of security. A security policy among others covers a high-level description of the technical and legal environment, risk analysis, guidelines of system administrators, definition of acceptable use by users, or guidelines for reacting to a site compromise, e.g., whether to shut down and rebuild a system in case of intrusion.

However, there was a difficulty in communication between the technology side and the business people mainly owing to the different stakeholders' interests. In particular, the problem was that establishing such an assessment would require additional financial resources from the bank and the business units were also competing for a great share of funds. To this end, the business units suggested that vulnerability

assessment was a 'luxury assessment tool', which could be postponed at a later stage since the number of internet banking users was currently low.

5.3.3 Trust and Goal Setting Within Delta-Bank

As discussed in chapter 4, the personal interview technique was utilised to collect the data. The interviewees were provided with a questionnaire list in order to understand the issues under investigation, allow them to prepare and obtain some general form of data for the research. As the interviews commenced, the participants gave answers based on the questionnaires in a broad style, and then gradually the research became more focused in order to shed light on the practical side of the issues under investigation. The review of the literature assisted in identifying the main issues that the research would be concentrating upon, part of which is the social phenomenon of trust.

Trust in Delta-Bank was considered an important issue in the relationship between employees with an effect on their work outcome. Delta-Bank is the organization with the medium-size structure among the three, established in 1907 although it is one of the largest commercial banks in Greece. The bank's long-term establishment has transformed the organization into a strictly business-oriented environment, whereas the values and beliefs held were based on a hierarchical system. In consequence, the issue of trust between the people was not exclusively depending on a long-term relationship but rather on professional criteria. This was established from the interviews with the bank employees who all defined trust in terms of how likely is someone to deliver within the organization rather than the willingness to co-operate. This was an effect of the large size of the organization, which did not allow the possibility between people of establishing close social relationships with each other.

The issue of trust within Delta-Bank and particularly within the IT and operations group was associated with delivery. That means the groups put trust on each other in terms of their capability in successfully dealing with a problem. As the alternative networks deputy manager said:

"Most of the bank employees the last couple of years attend educational seminars on issues of high concern to the banking unit in which they belong. I expect that these people keep updated with the latest market trends and they are capable of producing an important knowledgeable input in projects".

Thus, the issue of trust within Delta-Bank was based on the employees' working experience through the years. In particular, the members of the IT group developed a certain level of confidence between them through the successful implementation of various projects and from the same, efficient perception of the internet banking security.

Although, the level of trust within specific banking units such as the IT and operations group was not equally shared with other units of the bank due to the different nature of business. In saying so, the employees developed a certain level of trust only between people within the same group as they were working together on a daily basis and co-operated in a number of projects.

In Delta-Bank, there was a certain level of dissatisfaction from some of the IT employees to the top-management because not all of them participated in the process of goal setting and especially in the context of security and internet banking. One of the IT employees particularly said:

"I think the policies and procedures of the bank are too strict and they do not give a chance for the new staff members to contribute to the team as a whole".

When the IT manager was interviewed he also mentioned that many members of the IT group do not participate in the process of security goal setting. He added that the main reason was to retain confidence in highly sensitive issues, such as particular aspects of internet banking security. This was a policy held at Delta-Bank although the last few years the bank itself is rethinking to make goal setting an open procedure where every single member of the bank can make a contribution. However participation to security issues was also restricted to other units of the bank that were also engaged in IT projects, for reasons of confidentiality.

Moreover, different stakeholder interests within Delta-Bank had negative consequences on the level of trust between the technology group and different units of the bank. In the security risk event of vulnerability assessment there was a conflict between the business units of Delta-Bank and the IT and operations unit because it was believed that the greatest share of funding would go on the technology side. Specifically the IT manager said:

"Last year the bank established the Disaster Recovery Centre to improve its risk management strategy and having procedures such as vulnerability assessment would have a significant input on security goal setting. However the business people have interest on 'financial figures' based on ROI or ROM except for figures that have different "beneficiaries".

Similarly, there were times upon which different banking units developed an intense competition between them in order to achieve the greatest share of funds available for investments. The organization deputy manager said:

"There are times when due to competition the undertaking of some projects is delayed. The reason is that different banking units have different investment interests and in effect the consequences might be negative in the context of goal setting as some important goals remain back on the schedule".

Likewise, the issue of vulnerability assessment in the context of internet banking security lagged behind because it was believed that the time for devoting financial resources to such an area was premature, considering that the number of internet banking users was a small percentage.

A low level of trust was exhibited within the IT and operations unit as some of the interviewees were not confident enough to give answers to questions in the first place. In particular when some of the interviewees were being asked to describe the security risk event of fault tolerance their reaction was of the type *"What did the manager say?"*, *"I am not sure if I can give you details about this"*, or *"I don't really know how did they come to this decision, do you think they let us know?"*. One reason for such a reaction was perhaps the fact that some of the IT employees did not always

participate in the group's security risk activities but instead they felt they had to deliver from the "outside". The strategic marketing manager in particular said:

"This is a financial institution which is oriented to maximization of profits at the minimum risk; it is not a privately owned company where the owner decides what to do. There are various shareholders in this organization and we have to follow the rules to maintain their confidence but most of all the integrity of the institution. Therefore, when we mention issues of high concern such as internet banking security, we've to follow procedures to make sure that, before we make our systems secure enough to external attacks, we've made our systems first, secure from possible internal attacks".

5.3.4 Trust in the Context of Culture and Risk Communication

In Delta-Bank the culture was based on hierarchical criteria which did not allow too much freedom for individual initiative and intellect, although the bank's merger with the CA credit financial institution in June 2000 had an effect on its culture. Due to the merger with CA, the Delta-Bank had to reform its policies and procedures and innovate in new areas. With this merger the bank tried to achieve a greater market share and re-organize its existing structure by exchanging 'know-how' with CA and exploiting new comparative advantages of the two groups.

However, the merger with CA had the effect of downsizing the number of employees within Delta-Bank as part of strategy reformation. The effect of downsizing had negative consequences on the remaining employees' self-esteem. The alternative networks deputy manager said:

"When the board of members decided to downsize the number of employees, there were many that lost their concentration as they did not know if they were next. The effect of downsizing was also a globalisation effect with similar consequences to other organizations. However the bank's activities were 'frozen' for quite some time".

From the interviews it was shown that some of the employees' trust in the top-management 'was in question' as their confidence levels at the time were very low.

The activities of the groups and particularly the technology investments were limited for some period of time and as it was described, there was a general feeling of crisis in the market.

To this end, during the interviews the respondents replied that when the trust level is high within the group, the people have a sense of job security and they are likely to co-operate more efficiently in a given task. They agreed that their effort is also increased and goal alignment between the members of the group is likely to improve.

Further, the communication between employees in Delta-Bank was taking place by various means including e-mails, telephone, and face-to-face meetings. The IT and operations unit was based in Athens in a close proximity to the other units of the bank and the meetings between project teams were regular.

The research questions then focused on the degree to which trust may have an impact on the communications of risks among group members. The respondents replied that a few communication problems had occurred which were justified as a possible effect of mistrust between some of the employees to the top-management. In particular the IT manager said:

"When we introduced internet banking in Delta-Bank we were about to sign a contract with one of the leading companies in software development world-wide. However the audit manager who was a new recruit in the bank, expressed his opinion that maybe we should re-consider the software companies and sign a contract with company 'KSD' who was the bank's customer. The result was an old political issue to come on the surface and some people were not confident enough with our decision. Thus after long-discussions and group meetings finally we engaged to the first company although our schedule lagged behind".

From the above quote, it seems that mistrust of the motives, attitudes, and beliefs of one party towards another may have a negative effect on the communication of risks between those parties. With regard to the security event of fault tolerance, the communication of security messages between different units was characterised as inefficient. In particular the alternative networks deputy manager said:

"Although there are different kinds of fault tolerance we decided that the clustering effect was the most efficient at the time, although it is a more expensive solution as it requires special hardware and multiple computers plus that the operating system must support clustering. However last year we upgraded our operating system OS2 with the new WINDOWS 2000 platform, which is capable of clustering. The company with which we have a contract was responsible to deliver the necessary software but in favour of our political agenda we had to buy some components from a different supplier for marketing reasons. The components proved to be faulty".

Generally speaking, from the interview responses within the IT and operations group it seemed that there were different political agendas that could influence the communication of risks between the groups to a large degree. On the security risk event of vulnerability assessment, the different stakeholders' interests resulted in the postponement of the scheme, which was considered a breach in the communication.

5.3.5 Culture and Goal setting Within Delta-Bank

The IT and operations group was housed in spacious offices located on the upper floors of the private-owned building, an indication of the high regard with which the bank holds the department. The employees were wearing sharp clothes indicating a professional appearance and used a reference to the clients as "customers". The bank has a mission statement and has produced a "code of ethics" for its staff. From the material shown during the interviews it can be said that Delta-Bank has a defined mission.

One of the values of Delta-Bank is a professional attitude towards the customers. Most of the interviews emphasised that customers are the most important 'capital' for the bank. The bank and its staff are motivated by a value that their organization be professional while increasing the wealth of their customers and improving their status in domestic and international markets.

Another value in Delta-Bank was the loyalty of its employees. Loyal employees were valued and they were getting promotion based on years of work experience and

contribution to the bank. As the organization manager said: *"Loyal people always deliver and you know you can depend on them"*. The people who exhibited an attitude consistent with the organization's main element were those people considered for promotions to higher levels of the hierarchy. Although, some of the interviewees stated that this is an old-fashioned way and does not necessarily work if an organization seeks to innovate. It was argued that people with new ideas and high knowledge want their own 'space' which would allow them freedom of individual intellect. This was not the case however within Delta-Bank.

Likewise, an assumption of Delta-Bank's organizational culture was about its core mission. The core mission was to attract a larger customer base and increase its market share. As the organization manager said: *"We want to expand our horizons into new markets and improve our 'know-how' so we can attract more customers in the future"*. This was one of the reasons of the Delta-Bank's merger with the CA financial group.

The second major assumption that defined the organizational culture of Delta-Bank and particularly of the IT and operations group was that risk assessment is an independent process from risk analysis whereas different sub-groups have different roles. The IT manager stated that risk assessment is best practised by independent individuals rather than a large number of people and that it is a process within the context of risk management.

The people interviewed during the case study at Delta- IT and operations group were being asked questions in the context of security in internet banking in order to shed light on the group's security related activities. The questions were designed in such a way that they were indirect, with subtle hints on security concerns, mainly due to the confidentiality of the issue under investigation. All of the interviewees responded by saying that internet banking security was a major concern. One of the IT employees said:

"I think anyone who buys a computer and is connected to the internet, is exposed to various risks ranging from financial loss to a breach of privacy. However the last few years financial

organizations invest heavily on the security of their systems and the security standards have consequently been improved".

In Delta-Bank, all the interviewees confirmed that security is a very important feature for the bank's system operations and the IT staff is continuously improved on security issues through educational seminars, meetings with people from universities and any other kind of information such as newspapers, internet, magazines, etc. As the IT manager said:

"Keeping pace with the latest technological innovations is vital for IT professionals. In order to upgrade the knowledge and skills of my people I arrange multiple seminars including on security issues because technology is continuously involving and the knowledge you have now may be obsolete in six months time".

In the context of the effect of a strong culture to goal setting, the people within Delta-Bank argued that the culture has an effect on the level of goal setting although they believed it is minimal. Having a consistent program with the overall bank's activities was very important at the goal execution level and the IT manager stated that a strong culture can improve goal alignment within the group. By using the method of triangulation during the interviews, the same responses were obtained from other interview participants. However, the structure-size of Delta-Bank was affected by a number of external shareholders whose interests had an impact on the IT group's activities. Although, different groups within Delta-Bank had knowledge about risk issues, the nature of their business had also different scope with an ultimate effect on the goal setting procedures.

As previously mentioned, the culture of Delta-Bank was based on professionalism. That means the bank's top-management values most the professional side of the employees rather than the activities based on a free initiative. The top-management believed that in order to have control of the overall bank's activities, the different units of the bank should strictly follow the procedures written into manuals and reports and always report back. Although that seems natural, some of the interviewees argued that the units within Delta-Bank have to report more often than necessary even on issues of minor importance, whereas in some of the cases the undertaking of

necessary activities was delayed. Consequently, there was a problem about the process of goal setting, although it was further argued that security issues were carefully considered within a reasonable time frame.

5.3.6 Culture in the Context of Risk Communication

In Delta-Bank, while the IT people had a comprehensive knowledge on security risk issues, there was a gap between the IT group and the business units of the bank. This is the so-called Business-Technology Gap. As mentioned, the main reason for this was the fact that business people base their estimations on financial figures, whereas the IT people consider issues such as high response times, improved performance and reliability of systems, reduction of costs, etc. which are really intangible benefits with a long-term effect. Thus, when the interviewees were asked how those differences affected the communication, they replied that communication was sometimes inefficient because some important technology projects were delayed before they start. In this sense, the necessities of the IT group were ignored in favour of the business units as some issues of high priority for the technology side were lagged behind the schedule. The alternative networks deputy manager said:

"Technology investments especially on the issue of security in internet banking, is a highly important issue and more money should be spend on. Unfortunately, there are times that the issue of security is ignored in favor of business projects".

In the security risk event of fault tolerance, communication between the risk management unit, the audit department and the IT group was considered problematic since the decision was initially disregarded. From the interviews, the people within the IT group seemed unsatisfied from the manner in which the issue was handled and the fact that many times the group had to 'struggle' in order to get a project approval.

In addition, the communication of messages within the IT group seemed to be inefficient over time, since some people were cautious to transfer their knowledge to other members of their group as they feared their status was under threat.

5.3.7 Risk Communication and Goal Setting Within Delta-Bank

Communication within Delta-Bank occurred mainly through e-mails, telephone, and group meetings. The advantage in Delta-Bank, as compared to the case of Alpha-Bank, was the fact that the IT unit was based in Athens in close proximity to the other units of the bank, which ultimately had an important input on the communication between them. Face-to-face communication was the main mode employed and assisted in clarifying issues in a more reliable manner. To establish that the group members were receiving the same messages from the higher authorities open panel discussions were held. During the meetings, questions that required long lengths of discussion were dealt with and any other issues of concern and confusion handled. This saved time and assisted in obtaining good results.

Educational seminars and other training courses on security issues, assisted further in the communication of risks process since the perception of risks among the IT employees was depending on the good knowledge and confidence in dealing with risk possibilities. This was reflected in the efficient co-ordination of group activities and ultimately, in the overall success of related internet banking security projects

Although, several interview respondents argued that the communication within Delta-Bank was not always too efficient due to mistrust in part of some employees to top-management. In particular, top-management decisions were changed at times when project funds had been promised and so, the clarity of goal activities within the IT group was confused. The IT manager and group were changing their focus until new projects were arriving in the group. This had an ultimate effect on the level of goal setting as a misunderstanding of the issues led to inefficient co-ordination of activities and further project postponement times. In addition, the merger of Delta-Bank with the CA credit financial institution established new levels in the hierarchy where proposals had to be passed through new people with insufficient knowledge about the IT group's activities. In effect, decision making in the context of goal setting was sluggish.

5.4 Case Study Three- OmegaBank

5.4.1 Background to the Organization

Omega-Bank is among the oldest and largest Greek banks founded in 1841 as a commercial bank, and boasts a dynamic profile internationally particularly in South-eastern Europe and the Eastern Mediterranean. The bank has been listed on the Athens Stock Exchange since 1880 and for a significant period the bank, in addition to its commercial banking services was responsible for issuing currency in Greece until the establishment in 1928 of the Bank of Greece as the Central Bank. Since October 1999 Omega-Bank is being listed on the New York Stock Exchange and its total assets in 2001 figures, amounted to Euro 52.8 billion with profits of more than Euro 698 million (current year). The Omega Group provides a full range of financial products and services to corporate customers and private individuals alike, including retail and corporate lending, investment banking services, insurance, asset management, brokerage, leasing, factoring and shipping.

The bank has 586 domestic banking units and 936 ATMs covering the entire geographical area of Greece, a figure expected to reach 1200 by 2003. It has developed and expanded alternative distribution channels for its products such as Mobile and Internet banking. Today, after recent acquisitions in the Balkans, the Group's network overseas includes 328 units in four continents.

Having reaffirmed its leading position in the Greek market, the bank is further modernising its operations, backed by investment in new technology, so as better to serve its customers and enhance its profitability. Since 2001, the Omega Group is active in 18 countries outside Greece, via its branches, representative offices and subsidiaries. The Group controls 7 banks and 8 financial service providers, which together number 359 units and employ a total of 5,558 individuals. The total number of employees at 2001 figures, was 15, 194.

5.4.2 Electronic Banking

Omega-Bank has a dynamic presence in the area of electronic banking by offering a wide range of products and services online. The bank in order to improve the services and products it provides to its customers has launched internet banking. A few of the bank's services and products offered through its web site include funds transfer between accounts, VAT payments through Taxisnet, debit-credit card payment instalments, payments of life insurance premia to Omega General Insurance Co., obtain information on mutual funds portfolio, shares trading i.e., buying/selling shares, and application for public offerings on the Athens Stock Exchange (ASE).

To ensure that data remains confidential and unaltered, the bank uses the SSL128 bit (secure sockets layer) security protocol which is based on an encryption program developed by Brokat software company, considered inviolable in Internet applications. The system encrypts data and constantly authenticates communication between the customers' PC and the central system. That means if any disturbance or interference occurs in the communication process the transaction will be interrupted immediately and the PC-central system communication must be re-established. Internet banking allows users to access the service by means of User-ID and Password codes. If wrong codes are entered, user access is invalidated, the codes are cancelled and new codes must be issued. Likewise the bank's internet identity has been given an authenticode certificate by Verisign, the leading internet certification authority. This is always displayed as a padlock icon at the bottom of the log-in page and remains there while the *User* are genuine and prepared by the Bank.

5.4.3 Technological Infrastructure

In 2001, the bank's substantial technological infrastructure advanced in line with the targets set, which are comparable with those of the largest European banks. Particular emphasis was placed on ensuring that all computer systems would switch to the Euro environment smoothly. The bank runs over 200 different computer systems and applications, all of which converted successfully and were up and running from the first day of implementation.

The component of the IRIS deposit and loan management system that handles housing and consumer loans was put into operation, while the system is being further developed and adjusted to handle business loans and maximise the benefits deriving from the bank's Customer Relationship Administration system. The bank considers this a major project whose benefits lie in: the implementation of integrated procedures; flexible management of products offered through the system; the creation of automated operations to support its procedures and exercise of internal controls; and automated service of dues on loans via linked deposit accounts.

In addition to the above, the bank's branch and international network made substantial advances in upgrading their computer systems with the installation and extension of the Globus system. Globus has been installed in 12 branches in 7 different countries, and in 2002 will be installed in a further 186 branches of 3 subsidiaries operating in Canada, the Former Yugoslav Republic of Macedonia, and Bulgaria. The major benefit of this infrastructure project is the servicing of all banking tasks by a single computer platform.

5.4.4 Risk Management

Omega-Bank attaches great importance to effective and up-to-date risk management to ensure stability and continuity in its business. The bank's activity in the Balkans and Southeast Europe implies an increased level of risk given that these countries are not members of the OECD and should, under the current regulatory framework, be approached differently. Moreover, Omega-Bank's expansion to retail banking, with continuing growth in its range of products, means that its loan portfolio is also growing both quantitatively and qualitatively. Thus, generating a need for increasingly sophisticated risk management.

The listing of Omega-Bank's stock on the New York Stock Exchange has created more exacting demands, in line with US GAAP, as regards the presentation of the bank's results. At the same time, Omega-Bank is now seen to have taken its place in a

truly global market whose benefits it will endeavour to maximise. The bank closely follows international developments regarding the revision of the framework for Banking Supervision, and has contributed to the final proposals of the Basel Committee via its membership of the Hellenic Bank Association and the Institute of International Finance.

5.5 Social and Organizational Issues in Omega-Bank

5.5.1 Goal Setting and Security Within Omega-Bank

It was imperative for this investigation that any organization used for the research should have followed goal setting procedures and particularly the organizations' IT groups. Before the interviews commence the contacted organizations replied positively that goal setting was a consistent part of their overall business strategy. In fact, during the interviews the respondents showed particular interest in this investigation as the findings promised to deliver to the banks could provide an insight into how to improve their goal setting procedures and particularly in the context of internet banking security.

Goal setting was an implicit focus of Omega-Bank business activities plan and was reflected on its development philosophy. The aim of goal setting in Omega-Bank was oriented towards profit maximization at the possible minimum cost. As previously mentioned, the Omega Group is active in 18 countries outside Greece via its branches, representative offices and subsidiaries whereas having control over goal setting activities is crucial for the bank. The bank, although the leader of financial services in the Greek banking industry, is very cautious towards new innovations and the investment of its capital. The bank's long-term history and establishment has an effect on the manner according to which decisions are taken and procedures are followed. Appendix E1 shows the organizational chart of Omega-Bank.

The goals within Omega-Bank are seen in the form of projects, which originate from the top-management levels of the hierarchy towards the different units of the bank and vice versa. Considering that a goal is actually a project the projects within Omega-Bank are being introduced at the end of each year in order to set the scene of the

planning activities for the next year. The bank keeps always track of its different banking units' activities by getting reports back from each unit manager at the end of each month. The process of goal setting within Omega-Bank is also reflected on the way by which different banking units organize their activities. For example, the IT group exhibits similar patterns of the overall goal setting process within Omega-Bank in the sense that the deputy IT managers have to report regularly to the IT manager about the group's current activities.

The issue of security within the IT group was highly sensitive and confidential and that was also reflected in the fact that tape recording during the interviews was prohibited. Instead, the only type of recording allowed was note taking. Goals however within the IT group of Omega-Bank were focused on three levels and there were: systems efficiency, automation of processes and security. The planning of security systems within Omega-Bank was a process exclusively monitored by a small number of people. In fact, the design of information systems security was based on specific security steps including passwords and access codes, which were changing on a regular basis. As the IT manager said:

"The design of information systems security has to focus on the internal systems and networks since security breaches are likely to incur from the inside, from either viruses unleashed by customers to unintentional damage cause from curious staff. Even me, as the IT manager, I don't know certain passwords and access codes for reasons of confidentiality".

Nevertheless, the process of security goal setting in Omega-Bank is similar to the cases of Alpha- and Delta-Bank respectively, with a few differences though in the initiation and evaluation phases. At the initiation phase, shown in Figure 10 below, the IT group distinguishes security into physical security goals, security of internal systems, security applications in internet banking, and alternative networks.

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

Figure 10 Security Goal Setting in the Context of Risk Management (Omega-Bank)

Although, the first four steps at the goal initiation phase are identical with those of Alpha- and Delta-Bank, the IT group at Omega-Bank is also considering security applications in internet banking and alternative networks as additional steps of security group activities. All the interview respondents stated, that this taxonomy of security gives a more clear insight into the different aspects of security. Thus, in the security applications of internet banking the IT group by the use of a checklist considers the possible risks inherent to applications such as credit cards, online loan applications, VAT payments, etc. The group then is using a different checklist to keep record of possible security threats coming from the use of the internet banking channel and takes measures if necessary against their risk likelihood. These threats are categorised according to their importance in order to maintain control of security related activities. Although the taxonomy of such risks and risk factors is changing on a regular basis, the checklist for the purposes of this investigation was not provided.

The security level of alternative networks such as ATMs, Voice (telephone) banking, mobile banking, intranet-extranet, etc., incorporates identified possible risk factors

and areas where security threats are likely to occur. The IT group makes also use of a checklist of risk related factors for each alternative network which is considered a standard process inherent in the overall security risk management program.

At the goal execution phase, the IT group within Omega-Bank follows four main steps which include risk identification goals, selection of identified risks, final risk identification and risk monitoring. The steps are similar to those in the case of Alpha-Bank, although the Omega IT group does not incorporate the extra step of controlling the goal setting activities planned.

At the evaluation phase, the first step for the IT group is to evaluate the security risk activities planned. At this stage, the group evaluates the levels of risk exposure and decides whether to set new goals. At the end, the group has to produce a report which concludes with each relevant factor, its likelihood ratio, time-schedules, and further activities of the group. Similarly, the last step includes security policies and procedures in which the IT group, based on lessons learned, investigates whether there is a need to change any particular aspect of the security policies or procedures.

5.5.2 Security Risk Events in the Context of Internet Banking

During the interviews within the Omega-Bank IT department three security risk events were mentioned. The first one was the security of wireless networks in the context of network security, the security of e-mail servers in the context of server security, and the last the establishment of the unit of disaster recovery planning and post-evaluation.

In the first security event, the IT group considered the upgrade of its wireless networks security levels, mainly due to the introduction of mobile-banking to Omega-Bank customers. Wireless networks allow connectivity to a resource that is usually in a different location. One of the most important considerations in establishing wireless networks is encryption. In broad terms, encryption ensures that the data sent between two points is in a format that no one except those who are authorised can actually

read. Although, there is a variety of methods of securing wireless networks, the IT group was considering the use of the VPN (Virtual Private Network) technology method. VPN is actually a method of creating a private entrance to a private network using the internet, a VPN server and a VPN client. A wireless workstation connects to the VPN server using the access point and then "tunnels" into the network. The VPN client takes care of the password and data transmission encryption.

The second security risk event was the security of e-mail servers in the context of server security. The bank in year 2002 had recorded a few intrusion attempts to its operating system from the outside and a virus unleashed perhaps from unintentional damage caused by curious staff. To this end, the IT group considered changing the anti-virus software program on the e-mail server since the program created more problems than it solved. Anti-virus software programs are powerful programs that can conflict with other software installed on a computer, from Office applications to drivers in the operating system itself. The solution was to upgrade the existing anti-virus software program to a new edition and restrict some of the employees' e-mail usage.

The final security risk event in Omega-Bank was the establishment of the unit of Disaster Recovery Planning and post-evaluation. That was part of the IT group's overall strategic scheme, although different stakeholders' interests had an impact on the unit's activities. In particular, the Disaster Recovery Planning (DRP) unit focuses on security spending on areas of post-evaluation implementation and in possible disaster incidents involving the use of the networks, operating system, or any other means of communication. However, the spending amounts required for the unit's purposes conflict with the available financial resources spend on other business projects and therefore the competition between units becomes significant with an effect on the DRP unit's activities.

5.5.3 Trust and Goal Setting Within Omega-Bank

Omega-Bank is the largest organization among the three case studies with an IT department consisting of 410 employees. Omega-Bank is one of the oldest established

financial organizations in Greece and thus its philosophy is based on traditional banking means. By doing so, the bank invests heavily on its capital acquisition through a rapid expansion in international financial markets whereas the use of alternative technology means such as the internet banking channel is seen for strategic and marketing purposes. Although the bank is the leader of financial services in the Greek banking industry, its investments in technology are based on a rather cautious approach reflecting the bank's traditional values and beliefs.

During the first visits in Omega-Bank, it was evident that trust was based on a hierarchical system and that the members within the IT group were following specific procedures and always reported back to the top-management. For example, one of the interviewees within the organization unit had been asked the provision of the organization's chart diagram. The interviewee had to make two internal phone-calls to ask permission for providing such a diagram whereas the respondent on the other line of the telephone had also to make one more phone-call until a decision had to be made. Finally, it was decided that the organization's chart could be provided although the researcher found out afterwards that this chart diagram was available on the bank's web-site, free to download from any web-visitor. Thus, it seemed that the people within the organization unit were not confident enough to take the initiative, which reveals the effect of the hierarchical system on member activities.

All the interviewees were being asked to define the meaning of trust in the context of goal setting within their group and organization. The responses received show that the people within the IT group define trust on how a group or a third party is likely to deliver. The IT group members defined trust in the context of professionalism which means having the capability to produce efficient work outcomes. The employees within Omega-Bank developed a certain level of trust between different banking units with which they have successfully co-operated in a number of projects in the past. In particular the strategic plans manager said:

"We were about to introduce mobile-banking to our customers but with a main focus to attract the young generations, if you consider that two out of three young people have a mobile-phone and 'tomorrow' they could be our customers. Mobile banking though requires high wireless network security standards, as it seems more vulnerable to attacks than other

banking means. However, I was confident enough that the IT group will find the right solutions especially because any new application it has been dealt with in the past, was successfully implemented".

Evidence from the interviews, shows that in the process of security goal setting a large number of IT employees was restricted to participate. Like in the case of Delta-Bank, the top-management believed that the issue of security is highly confidential and only a small number of loyal people have to be involved in the process. Loyalty in Omega-Bank, was considered in terms of the number of years an employee works for the bank and has exhibited patterns that he is capable of delivering. However, the restriction to participate in security goal setting created some feelings of mistrust from some of the bank's employees to the top-management.

Although, during the interviews some of the respondents seemed very cautious to give answers to the questions, they mentioned that the low salaries within the bank, as compared to rivalry banks, was also an issue that caused some highly skilful employees to leave the organization. In effect, this had an impact on the activities of the IT group since some highly educated employees left the group in the middle of project development and implementation, whereas the IT manager had to recruit people with experience in projects. The IT manager also commented on this by saying:

"There have been a couple of times that some well experienced employees with knowledge in security issues left the group to join other companies because they were too money-oriented. Although I don't believe in such attitude, the outcome did have an effect on the project team up to a certain degree, because it takes time for the new project entrants to cope with the culture of the team. I assume money sometimes is a motivation of trust".

As mentioned, the different units within Omega-Bank had different business scopes, which created some degree of mistrust between them. In the context of the establishment of the Disaster Recovery Planning (DRP) centre, the interest of some business units diverged from that of the IT unit. The amounts invested on the DRP unit activities were higher than originally estimated and as a result, at the bank meetings, the business people were arguing on the methods of funding the DRP unit

activities. To this end, the business people tried to establish control over the IT and DRP unit project proposals, which resulted in project postponement times or even rejection.

When the IT deputy manager was asked to comment on this issue, he replied that the different stakeholders' interests, particularly on the activities of the DRP unit, had some effect on the level of goal setting. Specifically, the stage of risk monitoring is very critical for the status of the risks identified in the context of internet banking security since lessons can be learned for future activities and decide whether to take additional measures for existing risk factors. The activities of the DRP unit have an important input at the stage of risk monitoring since they provide valuable information on risk factors by enhancing the process of identifying risk factors with regards to internet banking security. In addition, DRP activities contribute to the evaluation phase as they also focus on post-evaluation implementation on security related projects. To this end, control of the DRP unit's activities by different stakeholders within the organization has a negative effect on goal setting as the unit's activities are impoverished.

5.5.4 Trust in the Context of Culture and Risk Communication

A strong culture was defined as a system of shared values and norms that define appropriate attitudes and behaviours for organizational members. This hypothesis however is based on the belief that organizations benefit from having highly motivated employees dedicated to common goals (Deal and Kennedy, 1982; Kotter and Heskett, 1992). To this end, the culture within Omega-Bank was ambiguous since the mistrust between different banking units had an ultimate effect on the co-operation between them, at least to some extent. In strong cultures, the employees are likely to co-operate and co-ordinate their activities more efficiently (Sorensen, 2002) although the differences between the units within Omega-Bank slowed down the activities of the Disaster and Recovery Planning centre. The co-operation between the units was not characterised as very efficient but instead competitive.

Mistrust may have also existed within the IT group since the majority of the employees did not participate in the process of goal setting, especially on issues of high concern such as internet banking security. This however had an ultimate effect on the group's co-ordination and control of activities as some of the employees felt less motivated since they believed that goal setting is a group effort (O' Really and Chatman, 1996). Many of the interview respondents also mentioned that information within Omega-Bank is withheld and it is a privilege of a small number of employees.

To confirm that the opinions obtained were not those of few people, and that a biased view was not being obtained, the method of triangulation, with reference to bank reports and archival documents, was used. The reports entailed information on the different group activities within Omega-Bank and the degree to which their activities were related to the activities of the IT and DRP units. The reports were internal and the researcher was allowed to read them only at his presence in the bank.

The effect of trust in the context of risk communication was also reflected in the fact that e-mail usage was prohibited within Omega-Bank by a large number of employees. That means many employees were not allowed to send and receive e-mails from an account held within the Omega-Bank, owing to the security restrictions imposed by top management. Because the bank had experienced some virus attacks perhaps from unintentional or even intentional damage from curious staff, the management within the IT unit, in association with the board of members, decided to categorise e-mail accounts according to the employees' nature of status. The interview respondents stated with no hesitation that the e-mail account did affect the communication between the groups as the communication took place in a rather sluggish manner. In particular one of the IT employees said:

"When communication takes place through e-mails, you can go back and check the text again and again if you want to clarify its meaning. In phone conversations you just can not do this and so you may be confused with the outcome of a decision".

All the interviewees within Omega-Bank commented that the restriction imposed on use of the internet left many people dissatisfied with the top-management's decision, since important information can also be obtained and used for educational purposes.

5.5.5 Culture and Goal Setting Within Omega-Bank

The culture within Omega-Bank is described by the use of Schein's cultural typology, who divides the organizational culture into three dimensions, that of artifacts, values, and assumptions (Appendix A1). The IT department was housed in modern spacious offices located in an independent building inside the city of Athens. As professional as the offices appeared, what was also noticeable was the sharp dress and demeanor of the IT staff. While this could be attributed to the location of the department, it is also reflective of the sharp tone of the group. The situation was similar, though, in the other units of the bank, such as the organization department, and the strategic plans department who also participated in the interviews.

Omega-Bank had a neutral reference to the customers as clients. The use of the term client was used in either formal or informal conversations. All of the public material, brochures and reports, use the term client. Omega-Bank explains its functions and strategic vision into its Web-site, although its culture is assumed as "solid", it is gone to great lengths internally to produce clarity and consensus in its functions. A characteristic of such commitment is the fact that Omega-Bank over the last few year recruits people with advanced educational degrees, such as Masters or PhDs, and specialised experience in technology.

One of the values of the organization is to provide flexible solutions to the financial needs of its customers, as it is from them that the bank derives its achievements and strengths. Recurring within the structured and informal conversations within the IT department is the value that the customers are a very important element and the bank should continue its commitment and determination to improve its customer relationships. The introduction of internet banking was also considered as a marketing tool to provide information and quality of products and services available to its customers. Similarly, the strategic plans manager said that the bank's efforts are to enhance the wealth of its shareholders by an efficient management of operations and the continued broadening of the bank's sources of income.

Another value is in staff relationships. Loyalty and professionalism among staff is valued, especially by senior staff. In fact, most interviewees stressed that loyalty was

a criterion upon which employees are promoted, depending also on the number of years they have worked, in the bank. Professionalism was the main belief in work relationships since it was argued that the structure size of the bank did not allow enough space for social relationships among the staff, and so the employees developed personal contacts only with those with which they have worked in the same projects.

A firm assumption in the Omega-Bank organizational culture is about the core mission. Although the core mission was not widely stated, the interview respondents repeatedly said that part of the way Omega-Bank operates is the assumption that to sustain and strengthen its performance it must endeavour to forge even more efficient management of the overall needs of the bank's customers. To this end, the bank accelerated the reorganization of its branch network: by the end of 2001, no less than 170 new-generation branches were in operation, producing results that promise much for the immediate future, in terms of both quality of service and level of sales. The interviewees commonly agreed that the bank aims on its dynamic repositioning in the local and international markets.

The second main assumption, similar to the case of Delta-Bank, that defines the organizational culture of Omega-Bank is that Risk Assessment is an individual process. Most of the interview respondents answered that risk assessment was best done on an individual basis although three employees stated that Risk Assessment should be done at a group level. The researcher then asked those three employees why Risk Assessment is best done on a group level rather than an individual one and the most simple reply obtained was: *"because when risk assessment is done on a group level we have the chance to participate, learn and improve our experience"*. Thus, it seems that some of the employees within Omega-Bank disliked the fact that participation to various activities, including Risk Assessment, was to the advantage of few people.

When the organization manager was asked to comment on whether Risk Assessment should be done at a group level he replied: *"We have a veteran staff that makes effective decisions on an individualized basis"*. Although, he underscored that the large number of experienced staff allowed them to make subjective overrides of the

point of scales that make for more effective decision making. The measurement of results of Omega-Bank, part of which include the development of retail banking operations, mortgage lending, acquisitions, etc., seem to confirm that they are making effective decisions.

During the interviews though the respondents mentioned that the hierarchical system within Omega-Bank did not allow enough room for innovations, individual initiative, and freedom of individual intellect. The sense of organizational control of the employees' activities was also observed during the process of interviews. The respondents were reserved in giving answers to the questions, at least to some extent, although they argued the effects of the hierarchical system within Omega-Bank may have had an effect on the groups' overall activities, including goal setting.

In particular, there was a general belief that the policies and procedures should run the bank not necessarily the people. This however was limiting people's creativity as they felt their individual intellect was limited by bureaucratic procedures with a consequence of some of the employees abandoning their efforts. For example, some of the interviewees had been asked the question: *Do you think sometimes your creativity pushes you to work overtime?* The answer was: *if I am paid.* Although, in strong cultures the values and norms of the organization are widely shared and strongly held (Sorensen, 2002), it seems that this was not absolutely the case in Omega-Bank, at least to a certain degree.

5.5.6 Culture in the Context of Risk Communication

In the security risk event of e-mail servers, the Omega-Bank in year 2002 had experienced some intrusion attempts to its operating system from the outside and a virus unleashed from damage caused perhaps from curious staff. The IT group decided to change the anti-virus software program on the e-mail server with a latest version, since the program created more problems than it solved. Part of the decision was to restrict e-mail usage to a large number of bank employees while allowing e-mail usage according to the employees' status. Although, many employees were not satisfied with the decision, they additionally argued that information and

communication flow within the bank was less accurate. The restrictions on e-mail usage by the employees in Omega-Bank, was seen as part of the policies and procedures of the organization.

The differences between the banking units in Omega-Bank had an effect on decision making at the level of goal setting, as the communication of messages was considered quite often as inefficient. As previously mentioned, the units' different business scope led to competition between them with an ultimate effect on the communication. The IT group activities quite often lagged behind in favour of the business units who acquired a larger share of the funding available for project spending. Although, the interview respondents mentioned that technology is an important aspect of the bank's business strategy, the business units had a great share over investments. Thus, a communication break down occurred quite often between the IT group and the business units within Omega-Bank.

In the context of risk perception, the IT staff seemed to be aware of the security threats in internet banking and the interview respondents mentioned that the IT groups members attend regularly seminars on security related issues. The IT group is continuously exchanging its 'know-how' with companies with which it co-operates for the development of software solutions. It has to be mentioned that software development in Omega-Bank is based in-house, although the IT unit co-operates with other companies mainly for the assembling of software components. During the first visits in Omega-Bank, it was obvious that the IT employees shared the same, knowledgeable perception of internet banking security which resulted in good communication skills among them. One of the IT employees when asked on the issue of internet banking security, he replied:

"Internet banking offers full potential to exploit market opportunities, if we consider the existence of banks exclusively on the Web. At the moment, most of the customers hesitate to go online, owing to the security risk events or of the danger they hear almost everyday on the news. I believe many steps have been put forward and internet banking is more secure now than it was two years ago. It is just a matter of time to gain the customers' confidence and I think we're on the right road if we consider the fact that the internet banking users of Omega-Bank are on the increase".

5.5.7 Risk Communication and Goal Setting Within Omega-Bank

From the findings so far, communication of security risk messages is an important aspect of goal setting within the context of risk management. The activities defined within the goal setting action plan need to be co-ordinated with other organizational activities. In the case of Omega-Bank, there was a certain level of difficulty in the communication between the different banking units, since the units had to compete for financial resources. As explained, the extent of such differences in the context of communication was rather minimal, with the overall co-ordination and control of the groups' activities characterised as efficient. Another reason for that, was that the perception of the IT employees on security issues was based on the same, knowledgeable criteria.

In the risk event of wireless networks security, the application of the VPN technology proved to be difficult due to difficulties in communication. VPN technology can be technically difficult for user account administration and technical assistance for set up. VPN can be implemented in various ways. The use of firewalls for VPN access is assumed to be ideal as it consolidates and minimizes points of entry to a network. Another way to implement VPN connectivity is by using a software solution such as that offered in Windows NT, Windows XP, or Windows 2000 Server. Like a firewall, this requires two network interfaces. The IT manager after a group meeting decided that the best possible solution was to use the VPN client features that comes along with Windows 2000. The audit manager though had ordered software components in order to install a VPN server software on the existing server, since it has an outside connection to the internet and a static IP. The audit manager said:

"I though that installing a VPN server software is more secure solution although a bit more expensive. I thought that the IT group having considered all the available options made a final decision to use different VPN software. I don't really know how, but the last moment they had changed their initial decision while I have given already the order".

The result was an initial confusion and a delay at the project initiation phase because the IT group had to reorder other software components that were temporary in short supply. The IT manager on this issue said:

"After we decided within the group what solution we'll implement I sent an e-mail to the audit manager with an attachment of the report. The next day I received back another e-mail from him, saying that he ordered the particular software components for the VPN server. I don't know why sometimes we make things difficult when it is the IT department to have the last word on such projects".

From the responses obtained during the interviews, the communication of messages within Omega-Bank was quite often difficult owing to the large size of the organization. That means there was a circulation of messages among different parties within different units of the bank and the involvement of such parties in decision making was, in some cases, unnecessary. Political agendas identified in the culture of Omega-Bank had an effect on the communication of messages between people within the organization. The interests of different stakeholders were diverged from those the IT group activities in some cases, as the IT group had to sign contracts with third party software providers who were the bank's customers. In doing so, some of the product specification requirements were not always met from those suppliers and therefore the activities of the IT group were postponed until a specific part was obtained from elsewhere.

5.6 Summary

This chapter described and discussed some preliminary findings of the Delta-Bank and Omega-Bank cases, used for the purposes of this investigation. The first section discussed the case of Delta-Bank with a medium organizational size structure while the second section focused on the case of Omega-Bank with the larger organizational structure. Likewise, the chapter gave a brief background of the Delta- and Omega-Bank cases in the context of their history, business and management, and the recent developments in their infrastructures.

The investigation focused thereafter in the interrelationship of trust, culture and risk communication in the context of the performance pyramid model and their effect on the level of security goal setting with regards to internet banking activities. The findings of the Delta- and Omega-Bank cases exhibit different patterns of social,

organizational behaviour and group activities than that of the Alpha-Bank case. The main reason appears to be the different organizational structures of the case studies, with an ultimate effect on the process of goal setting within the internet banking security context.

The qualitative data approach used in this investigation provided useful insights on the socio-organizational issues of the performance pyramid model, as it focuses on human thought and action in socio-organization contexts. It is noticeable that interpretive studies seek to understand the actual, relativistic meaning of phenomena in terms of the meaning people assign to them and that was the strategy employed in this investigation. The next chapter will draw on the case studies findings in order to analyse and discuss how the performance pyramid model can be operationalised and thus, can be used in practice. This should also allow the investigation to reflect upon the results and provide a useful insight into different socio-organizational perspectives of information systems security.

Chapter 6: Analysis of the Case Studies

6.1 Introduction

This chapter draws on the findings of the case studies described in the previous chapter. The case of Alpha-Bank has exhibited socio-organizational patterns that are in identical form to those depicted in the performance pyramid model. Specifically, social and organizational aspects such as trust, culture, risk communication, and goal setting play an important role in the context of information systems security management with regards to internet banking. The main interpretation of the phenomena under study in the case of Alpha-Bank is the fact that the bank's organizational size structure exhibits 'family-oriented' business patterns which is reflected on the strongly held and widely shared values and beliefs.

The cases of Delta-Bank and Omega-Bank respectively were described and discussed in chapter five. Although, the findings of both banks were purely descriptive they were central to the generation of insight. At first sight, the findings of the Delta- and Omega-Bank exhibited different patterns of social and organizational behaviour with an ultimate effect on the management of internet banking security. The analysis of the case research findings, will shed light on the interpretation of the phenomena by reflecting upon the results and thus providing particular aspects unique to each case within the performance pyramid model context. The analysis of the case studies is based on the performance pyramid model facilitated by the use of the case analysis (Yin, 1984) and cross-case patterns (Miles and Huberman, 1994) methods.

The chapter presents and discusses the determinants of trust, culture, and risk communication, as they were reported in the case studies by the interviewees, necessary to operationalize the model. The determinants of commitment at group level are also discussed and taxonomized into project, psychological, social and structural determinants. Commitment to goals is a critical aspect of goal setting because *"it is*

virtually axiomatic that if there is no commitment to goals, then goal setting will not work" (Locke et al., 1988, p.23).

6.2 Reasons for Choosing the Particular Case Studies

Depending on the nature of research case studies could be used either for exploratory, explanatory, or descriptive purposes (Yin, 1994). In this investigation, the case studies were used to utilise knowledge obtained from the literature review on socio-organizational aspects of information systems security management. To this end, by examining the procedures based on which different IT departments set security goals for the management of the integrity, confidentiality, and authenticity of information through the internet banking channel.

A case study approach has been followed within the IT departments of three financial institutions in Greece due to the investigator's availability of access and the introduction of the internet banking product by Greek banks in recent years. Thus, the investigation of the phenomena under study, in the Greek market sector, may reveal interesting results in the sense of providing new data for banks willing to introduce internet banking. However, as Greece belongs to the individualism paradigm, the results obtained may not necessarily hold for countries with collectivist societies.

Moreover, the institutions range from small- Alpha-Bank- to medium- Delta-Bank- to large- Omega-Bank- size structures, in terms of their financial assets base. A reason for choosing the specific case studies, is to investigate whether the performance pyramid model can be applied to IT groups with different structure size. In other words, if there are any differences, similarities of the phenomena under study within the information security management context. To this end, the IT group in Alpha-Bank consisted of approximately 60 employees, at Delta-Bank 150 employees while at Omega-Bank 410 employees respectively.

In the context of technological innovations, Alpha-Bank was the first bank to introduce internet banking to its customer-partners, which made it an interesting candidate to investigate. Likewise the Delta- and Omega-Banks have also introduced internet

banking to their customer base, while offering a wide variety of financial products and services on-line.

Generally speaking, the financial services industry is a leading global user of information systems and information technology. All major banks in the world use global communication networks such as SWIFT (Society of Worldwide Interbank Financial Telecommunications) for international payments. The banking industry is undergoing a period of rapidly intensified competition and fundamental changes due to regulatory changes and technological advances. Thus this 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).

In the Greek banking sector, financial institutions have realised that International and European information networks as well as technological improvements, allow flexible, specialised institutions with an international presence to provide a wide range of specialised products and services at lower costs (Koskosas, 1999). In effect, Greek banks invest in the supply of intelligent technological equipment and the full exploitation of it, which makes it also an interesting candidate to investigate within the scope of information systems security.

6.3 Analysis and Synthesis of the Case Studies

Benbasat et al. (1987) suggest that when multiple case studies are being employed, the contextual and data richness of the study should be provided. This has been achieved in chapters 4 and 5, where chains of evidence were presented by using quotes, which also illustrate that the responses were actually received and are not the researcher's interpretations. The contextual richness was provided with the in-depth descriptions of trust, culture, risk communication and goal setting in an information security management context. Likewise, the method of triangulation was used in previous chapters to present the data findings and to ensure that the correct interpretations of the data richness were obtained. This proved to be beneficial since the information provided by one source was limited and therefore any possible gap was overcome.

In the following sub-sections, different issues and their interrelationship with each other are examined. In order to allow the reader to understand the iterative process in obtaining the data, the means of obtaining the data are also explained. In doing so, the researcher's interpretations of the research are provided.

6.3.1 The Issue of Goal Setting in the Context of Risk Management

As stated in Chapter 2, the theory of goal setting falls within the broad domain of cognitive psychology and its literature is extensive. A goal can be viewed as an internal psychological representation of desired states, which can be defined as outcomes, events, or processes (Mitchell, et al., 2000). A goal encompasses terms such as intention, aim, task, deadline, purpose and objective. It is part of the human condition, in the sense that almost all human activities are consciously or unconsciously directed by goals. The initial assumption in this investigation was that *information security risks may arise due to failure to obtain some or all the goals that are relevant to the integrity, confidentiality, and authenticity of information through the internet banking channel.* To this end, the first main research question was, if IT groups follow goal setting procedures in the context of risk management with regards to internet banking security.

It was imperative for this investigation however that any organization used for the research should have followed goal setting procedures and particularly the organizations' IT groups. Before the investigation commence, the contacted organizations replied positively that goal setting was a consistent part of their overall business strategy. In fact, goal setting was a very important issue and it was seen as an integral part of the overall risk management process.

To collect the data, the personal interview technique was utilised. A questionnaire list was send to the interview participants in order for them to obtain a general insight of the issues under concern and allow them to prepare. The possible bias that the interpretive researcher may be associated with, have been overcomed by data triangulation. In doing so, information was obtained through internal organizational reports, published material, documents, or the organization's web-site. The time needed for interviews was

not easily available due to the highly sensitive nature of security as well as the dynamic activities of the IT groups, and so the researcher attempted to exploit any possible advantage including questionnaires. The questionnaire list however provided also the necessary information needed for the appropriate selection of the interview participants.

The case study of Alpha-Bank assisted in refining the research techniques, and clarifying issues that were not clear from the literature findings. In this way, the investigation ensured that a better clarification and development of issues was obtained through relevant information.

All the interviewees within Delta and Omega-Bank stated that goals are being set on a regular basis within each banking unit respectively, and that goals represent the identity of the banks' business activities plan. The goals within both organizations, like in the case of Alpha-Bank, are always business oriented and within the technology units the main goals are cost reduction, automation of processes, systems efficiency, and security. Likewise, goals within all of the three organizations, come in the form of projects which either originate from the top-management towards the different banking units or from those units towards the top-management, in the form of project proposals.

As the focus of the investigation became more intense the questions then focused on how goal setting is processed. Goal setting activities, in the context of security risk management, were distinguished into three main phases: the *goal setting initiation phase*, the *goal execution phase*, and the *evaluation phase*. However, the IT group within Delta-Bank distinguished the monitoring phase into a different 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, as it is shown in Figure 4.2, has also an additional step of controlling the goal activities planned, while Delta-Bank and Omega-Bank do not. At Alpha-Bank though this stage is considered as reactive since the IT group seeks feedback to ensure that the security goal setting plan until that stage, will actually accomplish its objectives. From the interviews, Delta- and Omega-Bank considered that such feedback is achieved at the evaluation phase while at Alpha-Bank the IT group members argued that although feedback is achieved at the evaluation phase, some of the goal activities planned may be '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.

In the context of internet banking security, all of the three case studies make use of a checklist which prioritises internet banking risks in terms of their likelihood ratio and possible impact. In doing so, the IT groups can take measures if necessary in order to maintain control of security related activities to internet banking. Although, it was stated that the taxonomy of such risks and risk factors in internet banking change on a regular basis, the provision of such a checklist was not provided due to confidentiality reasons. However, in the case of Alpha-Bank, an example of such checklist was obtained for the purposes of this investigation. This checklist is included in Appendix C3, which consists of five main clusters of internet banking risk categories.

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

However, goal setting within all of the three case studies was a significant and consistent part of the overall organizations' business activities plan and development. The procedures according to which the IT groups within the three organizations respectively set goals, in the context of security risk management, exhibit similar

patterns although with a few minor differences in the implementation process, in terms of stage prioritisation. In the context of internet banking security, all of the interview respondents within the organizations suggested that the use of the checklist proved to be beneficial as it provides clarity of the internet banking risks and of the security goal activities that have to be planned. In this way, the IT managers and groups ensure that the information data available through the internet banking channel will retain its integrity, confidentiality and availability. Thus, the main research questions of whether IT managers and groups set security goals with regard to the management of information through the internet banking channel is answered.

6.3.2 The Interrelationship of Trust, Culture and Risk Communication

As mentioned, the analysis of the results takes place within the context of the performance pyramid model. The socio-organizational aspects of the suggested model can be viewed as categories or different dimensions, which can be used to define similarities and differences within organizations and groups. In this way, the data can prove more reliable in relation to the socio-organizational assumptions made earlier in this dissertation. The analysis though is not complete by discussing only the empirical findings from each case study but also following a comparison between theory and practice.

The issue of trust has attracted particular attention through the years due to the numerous benefits it offers to organizations (Kramer, 1999). Theorists of trust support the view that trust may work as an independent variable (cause), dependent variable (effect), or interaction variable (moderator) (Rousseau et al., 1998). This investigation supports the view that trust has a moderate effect as it provides the conditions under which a strong culture and an effective communication of security risks are likely to occur. Trust though was defined as confidence and positive expectations of one party within an IT group that another party is willing to co-operate in setting goals effectively, in the context of security risk management with regards to internet banking.

In the case of Delta-Bank, trust was seen as an important issue in the relationship between employees although with a minor effect on their work behaviour. The issue of

trust within the organization and particularly within the IT and operations group was associated with delivery. That means the group members placed trust on each other in terms of their capability in successfully dealing with a problem. From the interviews though evidence shows that trust within Delta-Bank and between different banking units was not equally shared mainly because the nature of business scope was different and therefore, the employees developed a certain level of trust only between people within their group.

Dirks and Ferrin (2001), argue that trust has significant effects on attitudes, perceptions and other cognitive constructs such as employees' satisfaction with decisions, supervisor, relationship, and job. In Delta-Bank, there was a certain level of dissatisfaction between some of the IT employees towards the top-management because they did not participate in the process of security goal setting with regard to internet banking. Moreover the different stakeholders' interests within the organization had negative consequences on the level of trust between the technology group and different units because it was believed that the greatest share of funding would be spend on technology projects. To this end, there were times upon which different banking units within the bank developed an intense competition between them in order to gain the greatest share of funds available for project spending. This confirms Dirks and Ferrin's (2001) findings that under high levels of trust, individuals will be more likely to attend to co-operative motives, while under low levels of trust individuals will be more likely to attend to the competitive motives.

Mishra and Spreitzer (1998) state that downsizing (lay-offs) can have devastating effects on survivors because they lose sense of empowerment and control, as they are wondering if they will be next. The merger of Delta-Bank with the CA financial credit group had the effect of downsizing the number of employees within the organization, which ultimately affected the employees' confidence levels. To this end, during the interviews the respondents replied that when the trust level is high within the group, the culture becomes stronger as the individuals have a sense of job security and are likely to co-operate more efficiently with another party in a given task. They also supported that their efforts are increased and that goal alignment is likely to improve, as the co-ordination and control of group activities is more efficient. Thus, in the case of Delta-Bank, the evidence shows that trust could provide the conditions under which a group

strong culture is likely to occur through higher levels of co-operation and co-ordination of activities, and satisfaction of employees towards the management. Although, trust in Delta-Bank, was believed to have a weaker effect on culture because the organization's cultural stereotype was based purely on professionalism criteria.

The case of Omega-Bank exhibited similar patterns to the Delta-Bank case. Omega-Bank is the larger organization among the three case studies, with an IT department consisted of 410 employees. The responses received from the interviewees within Omega-Bank show that the people within the IT group define trust in terms of how a group or a third party is likely to deliver. The IT group members defined trust in the context of professionalism which actually means, having the capability to produce efficient work outcomes.

Evidence shows that in the process of security goal setting a large number of IT employees did not participate. The main reason was that the top-management believed that the issue of security is highly confidential and only a small number of loyal people have to be involved in the process. This however may have had an impact on the group's co-ordination and control of activities as some employees may have felt less motivated, since they believed goal setting is a group effort. To this end, some of the interviewees believed that information within the organization was possibly withheld, which shows similar results to those found by Dirks and Ferrin (2001), which are that lower levels of trust are associated with suspiciousness of information.

Similarly, trust was believed to affect the organization's culture owing to the low salaries paid to the employees compared to other financial organizations. Dirks and Ferrin (2001) argued that the extent to which individuals trust their manager, they are likely to devote their attention and effort, to role performance, norm conformance, and rule compliance because of their confidence that they will receive appropriate rewards. Since trust in Omega-Bank was seen in terms of professionalism, some of the IT employees were dissatisfied, as they believed that they should have money rewards for excellence in performance. Instead, the low salaries paid to employees, as compared to other organizations, created feelings of dissatisfaction with an effect, some highly skilful IT employees to abandon the organization. Thus, money incentives was seen as a

motivation for trust, where the departure of some employees affected the IT group's activities at times of project development and implementation.

Based on the interviews however it seems that trust provides the conditions under which a strong culture occurs through participation in group activities, employees' satisfaction towards the management, and higher levels of co-operation and co-ordination of activities. Although, the evidence shows that trust within Omega-Bank had a weaker effect on culture because, like in the case of Delta-Bank, the organization's large size structure makes it more difficult for different banking units to become flexible and trust depends purely on professionalism rather than on willingness to co-operate. In such organizations the values are less widely shared and the beliefs less strongly held mainly due to different political agendas. In addition, the procedures according to which the organizations co-ordinate their activities are based on manuals and bureaucratic procedures which do not allow individual initiative.

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

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

overall communication of security risk messages within the IT group, it was argued that trust through employees' satisfaction to the management, increased efforts, and co-operation in group activities, provides the conditions under which an efficient communication of risks occurs.

In the case of Omega-Bank, the restriction of e-mail usage by a large number of employees created a 'climate' of dissatisfaction among the employees, as they argued that the information flow within the bank was less accurate. Similarly, the different stakeholders' interests and the different political agendas had also an effect on the level of risk communication within Omega-Bank.

From the interviews, it was argued that the communication of messages within Omega-Bank was quite often difficult due to the large size of the organization. That means there was a circulation of messages among different parties within different units of the bank and the involvement of such parties on decisions was, in some cases, unnecessary. However, all the interviewees stated that trust provides the conditions under which an efficient communication of risks occurs through employees' satisfaction towards the management, increased efforts, and higher levels of co-operation.

The issue of culture has particularly attracted the attention of researchers in recent years. One of the reasons, is the belief that organizational cultures provide a sense of control, in terms of unifying the way employees process information and behave within the organization, which increases the predictability of organizational behaviour (Trice and Beyer, 1993). However, most of the literature on organizational cultures focuses on the hypothesis that strong cultures, enhance organization performance (Deal and Kennedy, 1982; Burt et al., 1994). In this investigation, a strong culture was defined as a system of shared values and norms that define appropriate attitudes and behaviours for organizational members (O' Reilly and Chatman, 1996).

It is also believed that having widely shared and strongly held norms and values leads to performance benefits such as enhanced co-ordination and control, increased employee effort, and improved goal alignment between the organization and its employees. During the interviews within Delta- and Omega-Bank, the respondents argued that

based on the performance pyramid model, the issue of culture could be prior to the issue of trust, as it shown in Figure 11 below.

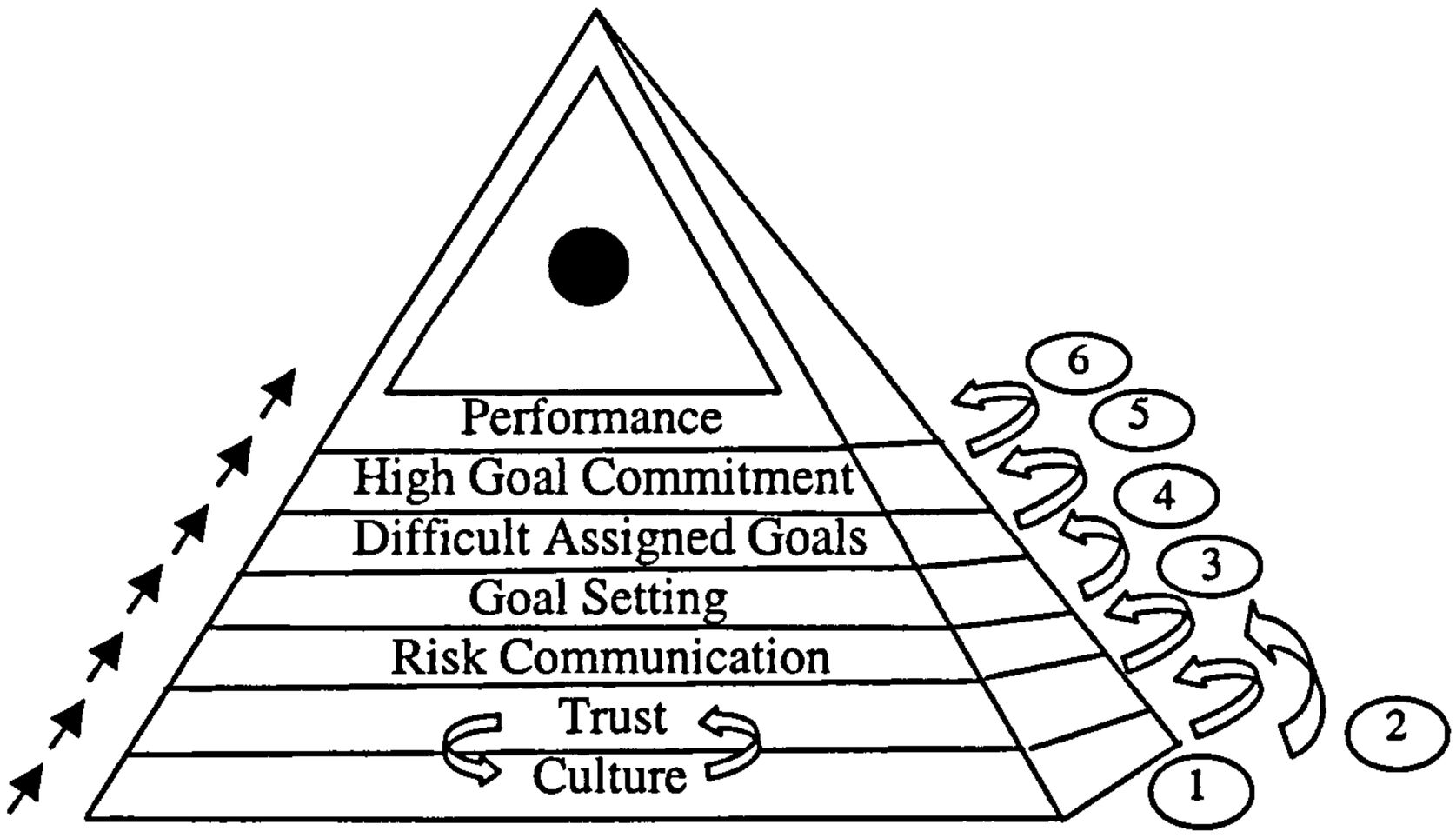


Figure 11 The Performance Pyramid Model (*Analysis Phase* 1)

The main reason of having the level of culture before trust is that an organization's culture plays a role on whether trust is high or low between the employees and different groups. For example, in the case of Delta- and Omega-Bank, some of the IT employees in the group did not participate in the process of goal setting with regards to the security of internet banking. Although, the issue of internet banking security was considered as highly confidential, the number of employees that did not participate in the security activities developed feelings of mistrust to the top-management. Thus, it can be seen that since the top-management's decision was part of the manuals and procedures followed within the organizations, it was also a characteristic of their culture in terms of how the organizations co-ordinated and controlled their activities.

However, in the interviews having discussed the definition of trust and strong culture, it was further argued that trust could be assumed as a social phenomenon observed within a society, whereas the society is always a consistent part of culture. To this end, the interviewees agreed that if an organization seeks to strengthen its culture, it could do so by increasing the levels of trust among its employees. From this perspective, trust is another dimension of culture because through trust the employees are likely to increase their efforts, and co-operate more efficiently as they know their efforts will be

rewarded. Since enhanced co-ordination and control, increased employee effort, and improved goal alignment, are characteristics of a strong culture, then high levels of trust through employees participation in group activities, satisfaction, and higher levels of co-operation provides the conditions under which a strong culture occurs. Thus, as the interview respondents stated, the level of trust should remain at first level of the performance pyramid model as shown in Figure 12 below.

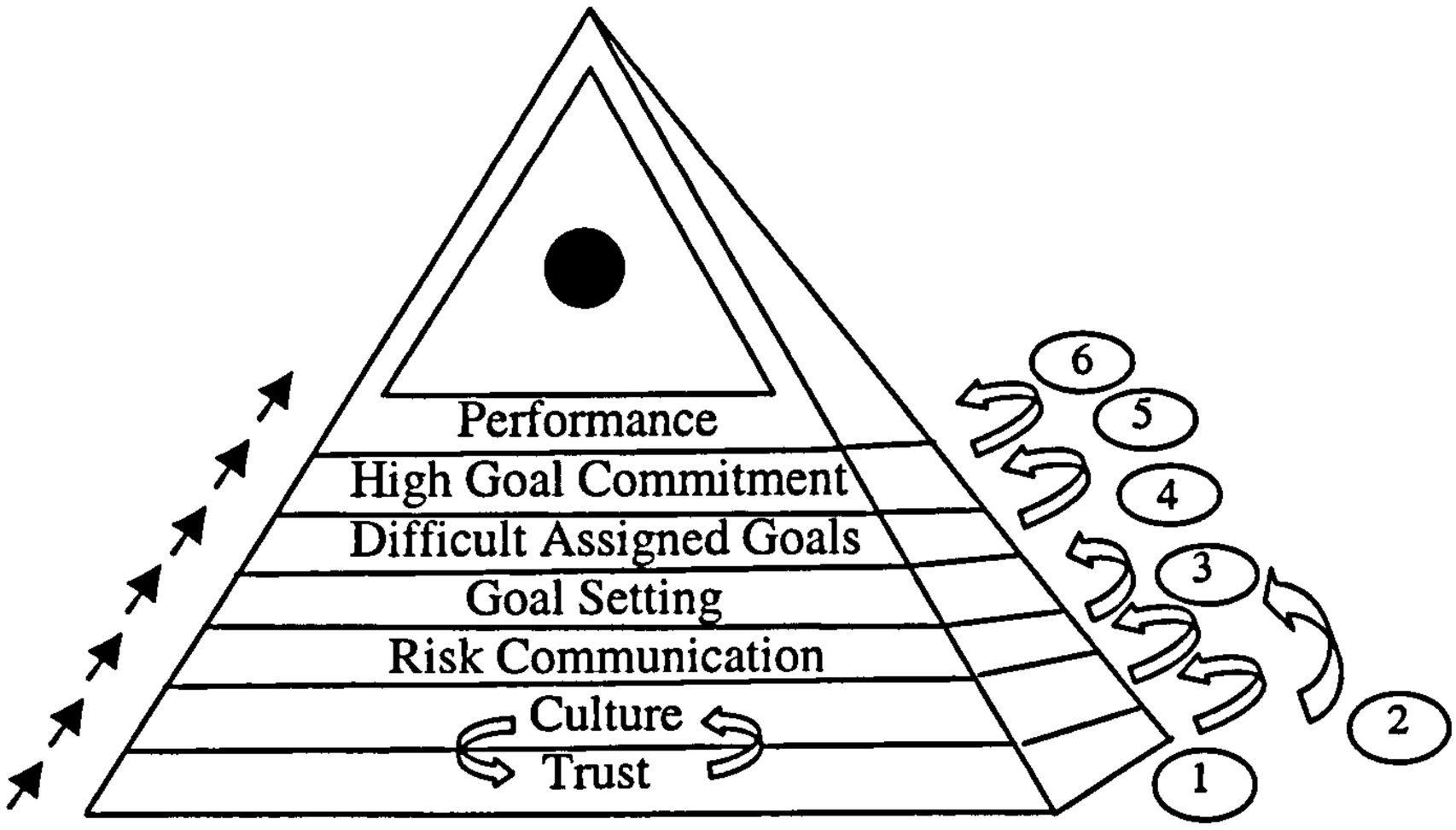


Figure 12 The Performance Pyramid Model (*Analysis Phase* 2)

In the context of risk communication, evidence shows that in Delta-Bank while the members of the IT group had a comprehensive knowledge of security risk issues, there was a gap between the IT group and the business units of the bank. This is the so-called Business-Technology Gap. The main reason was the fact that business people base their estimations on financial figures such as ROI, ROM, cost-benefit analysis, etc., which provide tangible benefits, while the IT people consider highly technical issues such as faster response times, improved performance and reliability of systems, which provide intangible benefits with a long-term effect. As previously mentioned, the non-participation of some IT employees in security goal setting had an effect on the communication of security risk messages since these employees felt less motivated to contribute to the group. In addition, the communication of messages within the IT group seemed to be inefficient over time since some people were cautious to transfer their knowledge to other members of the group, as they might felt their status was under threat.

In the case of Omega-Bank, the restrictions posed on e-mail usage by a number of employees led to some difficulties in communication between them as they argued that the information flow within the bank was less accurate. Similarly, the differences in business scope between different banking units had also an effect on the communication between these units, as some of the IT projects lagged behind in favour of the business units. However, all the interviewees stated that culture provides the conditions under which an efficient communication of risks occurs through participation to group activities, educational seminars, and enhanced co-ordination and control of group activities.

6.3.3 The Effect of Trust, Culture, and Risk Communication in Goal Setting

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

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

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

In the context of the effect of a strong culture to goal setting, the interviewees within Delta-Bank argued that culture has an effect on the level of goal setting. Having an IT program consistent with the bank's overall activities was very important on the goal execution level and it was agreed that a strong culture improves goal alignment between the employees and among different banking units. However, due to the structure size of Delta-Bank a number of stakeholders with different political agendas influenced the IT group activities. Considering that the stakeholders are part of the organization's culture, their different interests had an effect on the way the IT group co-ordinated and controlled its activities, quite often in the context of security issues.

In the case of Omega-Bank, the interview respondents said that the hierarchical system within the bank did not allow enough room for innovations, individual initiative, and freedom of individual intellect, which ultimately had an effect on the contribution of employees to goal setting. In addition, the non-participation of some IT employees in security goal setting with regards to internet banking was believed to affect the level of goal setting since the co-ordination and control of the IT group's activities could otherwise be improved. As argued, goal setting is a group effort rather than a process run by a specific number of employees.

However, from the interviews within both Delta-Bank and Omega-Bank, it was found that culture had a relatively weak effect on the overall goal setting activities, because the organizations, and particularly the IT groups, co-ordinate their activities based on manuals and procedures which provide the necessary control over the groups' activities.

The perception of internet banking security risks within the Delta- and Omega-Bank IT groups was based on the same, knowledgeable criteria mainly due to educational and training courses the IT members had to attend. When the interviewees were being asked questions in the context of internet banking security, they exhibited full knowledge and

awareness of the issue under concern and the mentioned that having equally shared information on security issues has a positive effect on the communication between members within the group. The confident, knowledgeable perception of security risks within the Delta and Omega-Bank IT departments was reflected on the overall success in internet banking projects and in the effective project co-operation with third party companies.

During the interviews though within both organizations, there was an argument that the communication of security risk messages was not always efficient due to different political agendas and competition between the banking units. Thus, the difficulties identified in the communication process had an ultimate effect at the level of goal setting particularly on specialised issues such as internet banking. Evidence shows that communication was a vital aspect of security goal setting since the activities defined in the context of risk management had to be co-ordinated with the overall organizations' activities, particularly when conflicts arise.

6.4 Socio-organizational Determinants

6.4.1 The Determinants of Trust

The scope of this investigation was also to identify the determinants of trust in the context of the performance pyramid model. The main reason is that in order to operationalize the performance pyramid model would be necessary to identify the determinants of the socio-organizational aspects of information security management that form the performance pyramid model.

To this end, the investigation proceeded further to the identification of the determinants of trust within all of the three organizations. The findings are based on the interviewees' work related experience, social relationships between people within groups, knowledge, and personal value attributes.

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 12 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 12 The Determinants of Trust at Macro-level

6.4.2 The Determinants of Culture

The investigation next focused on the determinants of culture within the three organizations. Specifically, the interviewees were being asked to describe the determinants based on which a culture can be strong. The most important determinant mentioned from all the interviewees was education and training seminars. The IT manager in particular said that educated people understand better the responsibilities they have within the group and consequently the co-ordination and control of group activities is likely to be more efficient. In addition, they mentioned that educated people are more likely to co-operate within the team and have the necessary 'tools' to express their opinion in decision making as well as to transfer their knowledge to other members of the group.

Similarly, training seminars on issues of high concern such as internet banking security is also an important factor in co-ordinating the groups' activities more efficiently and

providing goal alignment within the group, which ultimately has an effect on culture strength. Participation in the organization's activities was also another important determinant, also identified in the issue of trust, since in strong cultures employees feel free to participate in group activities (O' Reilly and Chatman, 1996). That means allowing employees to participate in group activities, makes them feel important and they increase their effort in order to contribute to the group.

The interviewees within the three organizations stated that another important determinant of a strong culture is clarity in goal achievement. The IT manager or project leader is a key aspect in providing clarity of the goals that have to be achieved within the group, by explaining efficiently to the group members what are the goals and how are they going to achieve them. Clarity of goal achievement was argued to provide better co-ordination and control of group activities since employees face less uncertainty about the proper course of action when faced with difficult situations (Cremer, 1993).

The interviewees within Delta-Bank, in particular, stated that mergers is also another determinant of strong cultures. All the interviewees within Delta-Bank commonly agreed that a merger may have negative consequences for the smaller organization whose identity may be absorbed by the larger one. The interviewees within Delta- and Omega-Bank mentioned that salaries (financial incentives) play an important role, since satisfied employees are likely to co-operate more efficiently within the group. Competitive/political rivalry between different banking units within the organizations, was also another determinant previously discussed. Ultimately, the issue of trust is also an important determinant of a strong culture. These determinants are also depicted in Table 13 below

Determinants of Strong Cultures
▪ Education/training seminars
▪ Group participation in group activities/decision making
▪ Clarity in goal achievement
▪ Competitive/political rivalry
▪ Mergers
▪ Financial incentives
▪ Trust

Table 13 The Determinants of Strong Cultures

6.4.3 The Determinants of Risk Communication

The next phase of this investigation was to identify the determinants of risk communication at a macro-level. The interview respondents within the three organizations mentioned that regular group meetings facilitate the communication of information flow between members. Participation in group activities and decision making was also an important determinant for an efficient communication of risks since the members of the group can contribute to the group and make a better effort to communicate their knowledge, as they feel important being part of the group.

Education and training seminars was also considered an important determinant of risk communication since the participants develop useful skills and advance their knowledge on highly specialised issues such as internet banking security. In addition, it was argued that educated people are likely to communicate more efficiently with the other members of the group.

Another important determinant of risk communication was believed to be the evaluation phase on security risk projects since evaluation and particularly post-evaluation provides useful feedback which is used as lessons learned for future activities. The experience gathered from the evaluation phase, was argued to improve the communication of security risk messages in the future. Ultimately, trust and strong cultures play also a significant role in the efficiency of the risk communication process. These determinants are also included in Table 14 below.

Determinants of Risk Communication
▪ Regular group meetings
▪ Participation in group activities and decision making
▪ Education/training seminars
▪ Evaluation/post-evaluation
▪ Trust
▪ Strong culture

Table 14 The Determinants of Risk Communication

6.5 The Determinants of Commitment at a Macro-level

A major finding in goal setting research is that difficult goals lead to higher performance levels than do 'easy' or 'vague' goals (Locke et al., 1981). Specifically, when individuals are assigned specific, difficult goals their performance tends to increase as compared to instructions of 'do your best' or no assigned goals. These findings though depend on the assumption of commitment to the goals at both, an individual and group level. To this end, the performance pyramid model shows that in a complex task environment, such as internet banking security, 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, the 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.

Although, the results of specific goals on performance have been supported by 90 percent of studies at both, an individual and group level (Locke and Latham, 1990), and even though the relationship of goal level, commitment and performance holds at an individual level, this relationship may not necessarily hold at a group level. For example, Seiijts and Latham (2000) found different impacts of goal setting on performance based on group size, while Wegge (2000) found moderating effects from participation in goal setting, group cohesion, and group conflict. Likewise, Koskosas

and Paul (2003a) report that group size had different impact on the process of goal setting mainly due to differences in the socio-organizational contexts.

However, the relationship of goal level, commitment, and performance is not in the scope of this investigation but rather the ultimate scope is the identification of the determinants of commitment, at a group (macro) level. To this end, the investigation focused on the determinants of group commitment to goals and in so doing, it categorised them into project, psychological, social and structural determinants as originally proposed by Staw and Ross (1987). This taxonomy is based on the findings achieved from the organizations, based on the interview respondents' work experience and critical judgement through the years.

The use of an interpretive epistemology proved to be very beneficial as it provided rich insights into group commitment. The use of other methods such as laboratory experiments, may not adequately assess self-justification because the subjects may feel emotionally committed as the individuals personally involved in projects (Brockner, 1992). They may not also be able to address the effect of social factors such as political rivalry (Keil and Mixon, 1994). In addition, considering that goal setting, in the context of security risk management, is a very dynamic process based on radical life cycles, obtaining access to observe the management of phenomena such as internet banking security would be difficult due to the high confidentiality of the issue under concern.

6.5.1 Project Determinants

According to Locke et al. (1981) commitment is the determination to try for a goal and the persistence in pursuing it over time. In this investigation, commitment is defined as a state of mind that holds people and organizations in line of behaviour (Staw, 1982) and encompasses psychological factors that force individuals to take action (Kiesler, 1971).

Commitment within all of the three organizations was considered very important for goal achievement. The importance of commitment though was particularly recognized in the case of Alpha-Bank due to the 'family-oriented' business environment, whereas

the individuals were more willing to co-operate and commit to the bank, as they felt part of the organization. In the case of Delta- and Omega-Bank, although commitment was important, it was also considered a standard criterion since the organizations valued most professionalism rather than just willingness. To this end, the employees were expected to be committed.

Considering that a goal within the three organizations is translated into a project, one of the most important project determinants is time. Time may not always be sufficient especially in cases where new projects arrive in the IT group, that compete with current ones. In this case, the IT managers at Delta- and Omega-Bank said that they occupy part-time staff, in cases of emergency. Similarly, project related experience is also an important determinant, particularly on issues of high knowledge skills such as internet banking security.

Another project determinant of group commitment is clarity of goal achievement, which is also some of the socio-organizational determinants previously discussed in the context of the performance pyramid model. A project is also likely to continue if it promises to deliver a large-payoff over time (Keil, 1994). However it was argued that if a project fails to meet initial requirements, that is it runs to a deadlock, the IT manager/project leader has to stop the project before the consequences become even worst, as additional financial and human recourses may have to be used. This was also referred to as flexibility of the IT group and particularly of the project leader in making decisions. These project determinants are included in Table 15 below.

Project Determinants
▪ Time ▪ Project related experience ▪ Clarity of goal achievement ▪ Large payoff (Keil, 1994) ▪ Flexibility

Table 15 Project Determinants

6.5.2 Psychological Determinants

During the interviews within all of the three organizations, the respondents mentioned a number of psychological determinants to group commitment. Although, a group is consisted of a number of individuals, the group is more dynamic than the individuals themselves, and the determinants of group commitment may affect the individuals respectively, and vice versa. Based on the interviews, an important psychological determinant to group commitment is money and moral rewards. Money difficulties may affect an individual's psychology and loose his focus and efforts in the group. The effect of downsizing is also an important determinant to group commitment as it was discussed earlier.

Likewise, personal/individual goals that diverge from those in the group is also a determinant of group commitment, since some people may act differently within the group due to personal interests. For instance, if an individual is not satisfied with the IT manager's decision in the assignment of a responsibility, the individual may abandon his efforts while his focus is elsewhere.

Overconfidence in goal achievement due to prior project success may lead to overestimation of the chances to achieve the goal. This may be particularly the case on IS security projects due to the highly knowledge requirements and the complexity of the issue under concern. Also the arrival of the project champion/leader during the project implementation stage may also create confusion within the group and cause even the project to be abandoned (Reich and Benbasat, 1990). It was also argued, that the project leader may slow down the group activities, for personal reasons, and thus the project implementation to be delayed. Table 16 shows the psychological determinants of commitment at group level.

Psychological Determinants
▪ Moral rewards (promotions, performance evaluations, etc.) ▪ Money rewards ▪ Downsizing ▪ Personal/individual goals that diverge from those in the group ▪ Prior history of success (Keil, 1994) ▪ Arrival of project champion during project implementation (Reich and Benbasat, 1990)

Table 16 Psychological Determinants

6.5.3 Social Determinants

Political/competitive rivalry is an important determinant of commitment discussed earlier in the chapter. Different stakeholders' interests may affect the commitment of an IT group in the context of security goal setting. For example, within all of the three organizations it was found that the IT groups had to buy software program from a software supplier who was the bank's customer. This phenomenon was particularly observed in large organizational structures such as Delta- and Omega-Bank.

Limited financial budgets (Garland, 1990) play also a significant role to group commitment, as additional resources may be needed on complex project solutions such as internet banking security. From the interviews withheld within all of the three organizations, it was commonly agreed that the issues of trust, and risk communication are also determinants of group commitment. Briefly, that trust to the IT manager plays a significant role in group commitment since the IT manager who is usually the project leader, is responsible for staff promotions, performance evaluations, guidance in job responsibility. Risk communication plays also a significant role by providing an efficient circulation of information with regard to security risks in the context of internet banking. These social determinants are also included in Table 17 below.

Social Determinants
▪ Political/competitive rivalry (Grover et al., 1988) ▪ Top-management support (Keil, 1994) ▪ Limited financial budgets ▪ Trust ▪ Risk communication

Table 17 Social Determinants

6.5.4 Structural Determinants

A strong culture, as has been defined in this investigation, enhances co-ordination and control of group activities, increases employees' efforts, improves goal alignment, and provides clarity of goal achievement. Thus, a strong culture through these characteristics is an important structural determinant of group commitment.

Top-management support during project implementation is also another important determinant of group commitment (Keil, 1994) as well as the knowledge of the project leader on issues of internet banking security. It was particularly mentioned that the IT manager or project leader has to have experience and knowledge in project implementation, as he is the ultimate key to goal achievement. The structural determinants of group commitment are incorporated in Table 18 below in relation to the project, psychological, and social determinants. It has to be mentioned though that discussion of project failures has negative connotations and thus, organizations may not feel comfortable enough to discuss such issues in detail.

Project Determinants	Psychological Determinants	Social Determinants	Structural Determinants
▪ Time ▪ Project related experience ▪ Clarity of goal achievement ▪ Large payoff (Keil, 1994) ▪ Flexibility	▪ Moral rewards (promotions, performance evaluations, etc.) ▪ Money rewards ▪ Downsizing ▪ Personal/individual goals that diverge from those in the group ▪ Prior history of success (Keil, 1994) ▪ Arrival of project champion during project implementation (Reich and Benbasat, 1990)	▪ Political/competitive rivalry (Grover et al., 1988) ▪ Top-management support (Keil, 1994) ▪ Limited financial budgets ▪ Trust ▪ Risk communication	▪ Strong culture ▪ Top-management support (Keil, 1994) ▪ Top-management's knowledge on internet banking security

Table 18 Determinants of Group Commitment

6.6 Conclusions

The aim of this chapter was to analyse the findings of the Delta- and Omega-Bank cases in the context of the performance pyramid model. The analysis of the research findings obtained from the case of Alpha-Bank exhibited socio-organizational patterns identical to those depicted in the performance pyramid model. That is, there is a strong interrelationship between trust, culture and risk communication, whereas in turn, these elements have a strong effect on the level of security goal setting with regards to internet banking. The main reason, was that the small size of the organization exhibited patterns of a 'family-oriented' business environment whereas the values and beliefs were widely shared and strongly held among the members of the organization.

More specifically, in the case of Alpha-Bank evidence shows that trust provides the conditions under which a strong culture and an efficient risk communication occur through *employees' satisfaction to top-management, positive attitudes, increased efforts, and higher levels of co-operation between members*. Likewise, a strong group

culture provides the conditions under which an efficient risk communication occurs through *participation in group activities, enhanced co-ordination and control, motivation, clarity of goals, and goal alignment.*

Next, the performance pyramid model was applied to different cases, that of Delta- and Omega-Bank, with a larger organizational structure in order to investigate any possible similarities/differences in the findings obtained from Alpha-Bank. To this end, the cases of Delta- and Omega-Bank exhibited different patterns of socio-organizational behaviour although the process of goal setting in the context of risk management was based on the same philosophy among the three case studies. In particular, evidence shows that there is indeed an interrelationship of trust, culture and risk communication although the degree of importance was less consistent with the original findings. In fact, these elements had also a weak effect on the level of security goal setting in internet banking since the values and beliefs of the organizations are based purely on professional criteria. In saying so, people within Delta- and Omega-Bank valued most professionalism between third parties and groups, and that policies and procedures should run the bank, not necessarily individual initiative. It was valued though that the process of goal setting with regard to internet banking security could be even more efficient if trust, culture and risk communication were more strongly held and widely shared among individuals and different groups.

In other words, the process of goal setting in the context of information systems security management, with a focus on internet banking, could become even more efficient if the issues of trust, culture and risk communication are considered and determined more carefully than just acknowledging their value. To this end, failure to recognize and improve socio-organizational values such as trust, culture and risk communication may lead to an inefficient process of IS security goal setting whereas security risks in relation to the integrity, confidentiality, and availability of information through the internet banking channel, may arise.

Similarly, most of the interviewees within the three organizations argued that trust, culture, and risk communication are not necessarily dependent variables. That means, these values may exist independently of each other, although it was argued that trust facilitates the establishment of a strong culture and an efficient communication of risks.

Finally, the chapter presented and discussed the determinants of trust, culture and risk communication required in order to operationalise the performance pyramid model. Then, the determinants of commitment at a macro-level were analysed and discussed and they were taxonomised into project, psychological, social, and structural determinants based on the taxonomy originally proposed by Staw and Ross (1987).

Chapter 7: Summary and Conclusions

7.1 Overview of the Research

This thesis started with an overview of current information systems security research issues in the context of internet banking in chapter 1. The use of new distribution channels such as the internet, increases the importance of security in information systems due to the security threats the organizations are likely to be exposed. A number of major studies recently contacted in Europe, among these being the Andersen 2001 survey, the Ernst and Young 2001 survey, and the DTI study 2002, indicate a general upward trend in the number of security incidents in organizations.

Although, a number of valuable security approaches have been developed, over the years, that help in managing IS security and in limiting the chances of an IS security breach, they fall short of interpreting the social aspects of IS, i.e. socio-technical and social organizational roles of IS security. To this end, the investigation in this dissertation adopts a socio-organizational approach to information systems security with a focus on internet banking. The main assumption of the research is that security risks may arise *due to failure to obtain some or all the goals that are relevant to the management of the integrity, confidentiality and authenticity of information through the internet banking channel.* Thus, Chapter 1 states the aim of the research which is *to investigate if IT groups set security goals in relation to the integrity, confidentiality, and availability of information through the internet banking channel.*

Based on a literature review, however, this research identified a set of socio-organizational aspects that may have an important role on the level of goal setting within the context of information systems security management. In doing so, the purpose of this research in broad terms was: (a) to validate if there is an interrelationship between the identified socio-organizational aspects and their possible effect on the level of goal setting; and (b) to present a model which can be used to

analyse future research studies and shed light into the socio-organizational dimensions of information systems security. Ultimately, Chapter 1 provided an introduction of the research methodology and an overview of the dissertation outline.

Chapter 2 reviewed the social sciences literature for a suitable theory of knowledge that could be applied in the area of information systems security. The chapter provided an overview of the concept of risk and introduced the theoretical concepts that form the basis of the socio-organizational model suggested in this dissertation. Understanding the theoretical concepts that lie beneath the chosen approach allowed the establishment of the rationale and assumptions for this particular investigation.

In reviewing the literature on goal setting, it was also found that commitment to goals is a very important aspect of goal achievement. Specifically, when individuals are assigned specific, difficult goals their performance tends to increase as compared to instructions of 'do your best' or no assigned goals. These findings though depend on the assumption of commitment to the goals at both an individual and group level.

In the same fashion, the rationale and assumptions established, after the review of the literature on socio-organizational aspects of goal setting within the information systems security context, were illustrated into the suggested performance pyramid model. The first part of the model shows that there is an interrelationship and effect of trust, culture, and risk communication on the level of goal setting with regard to internet banking security. The second part shows that if people are assigned specific, challenging goals (given goal acceptance), people's commitment to the goals will increase. Similarly, the goal level, commitment and performance have a complex relationship including both direct and moderator effects. That means, if the goal level is held constant there are direct effects of commitment on performance. The model however was used as the unit for analysis in this investigation in the context of information systems security.

Chapter 3 described and discussed the methodological as well as philosophical assumptions underlying the research approach chosen for the nature of this particular investigation. The justification of an interpretive epistemology was provided and the chosen qualitative research approach within the case study strategy was discussed. Then, the research design and process were presented. The research design of this

investigation employed multiple data collection methods as it is important in case research studies (Benbasat et al., 1987). The use of multiple collection methods makes triangulation possible and this provides stronger substantiation of theory (Eisenhardt, 1989). In all cases data was collected through a variety of methods including interviews, documents, and observation. It has to be mentioned though that the investigation focused within the IT departments of three financial organizations as it is those groups exclusively involved with information systems security issues.

In Chapter 4, the performance pyramid model was applied to the case of Alpha-Bank with a small IT group structure in order to test the validity of the rationale and assumptions made in this research. The chapter gave a brief background of the case of Alpha-Bank in the context of its history, business, infrastructure, management and organization on a global scale as well as its recent developments. The case of Alpha-Bank was also prior used to refine the interview techniques and provide the necessary ground for analysis, comparison and discussion of the results obtained from cases with different organizational structures such as Delta- and Omega-Bank.

In the case of Alpha-Bank evidence shows that trust provides the conditions under which a strong culture and an efficient risk communication occur through *employees' satisfaction to top-management, positive attitudes, increased efforts, and higher levels of co-operation between employees*. Likewise, a strong group culture provides the conditions under which an efficient risk communication occurs through *participation in group activities, enhanced co-ordination and control, motivation, clarity of goals, and goal alignment*. Moreover, evidence shows that these socio-organizational aspects play an important role on the level of goal setting with regard to internet banking security. However, the main reason that such socio-organizational aspects have a strong effect is, that the small structure of the Alpha-Bank IT group exhibited patterns of a 'family-oriented' business environment whereas the values and beliefs were widely shared and strongly held among the members of the organization.

Chapter 5 described and discussed the cases of Delta-Bank and Omega-Bank in the context of their history, business and management, as well as recent developments in their organizational structures. The investigation focused thereafter in the interrelationship of trust, culture and risk communication in the context of the

performance pyramid model and their effect on the level of security goal setting with regard to internet banking activities. Based on some preliminary findings, the cases of Delta- and Omega-Bank exhibited different patterns of social, organizational behaviour and in-group activities than that of the Alpha-Bank case. The main reason appears to be the different organizational structures of the case studies, with an ultimate effect on the process of goal setting in the context of internet banking security.

Chapter 6 analysed the findings of the Delta- and Omega-Bank cases in relation to the case of Alpha-Bank. The analysis of the case studies took place within the context of the performance pyramid model and it was facilitated by the use of the case analysis (Yin, 1984) and cross-case patterns (Miles and Huberman, 1994) methods. To this end, the cases of Delta- and Omega-Bank exhibited different patterns of socio-organizational behaviour although the process of goal setting in the context of risk management was based on the same philosophy along the three case studies. In particular, evidence shows that there is indeed an interrelationship of trust, culture and risk communication although the degree of importance was less consistent with the findings of the Alpha-Bank case. These socio-organizational aspects had also a weak effect on the level of goal setting in the context of internet banking security because the values and beliefs of the organizations were based on professional criteria rather than more idealistic. In saying so, people within Delta- and Omega-Bank valued most professionalism between third parties and groups, and that policies and procedures should run the bank, not necessarily individual initiative. Although, the interview respondents stated that the process of goal setting could become even more efficient if trust, culture and risk communication were more strongly held and widely shared among individuals and groups.

The chapter then presented and discussed the determinants of trust, culture and risk communication necessary for the operationalisation of the performance pyramid model. Ultimately, the determinants of commitment at a macro-level were also identified and distinguished within a taxonomy form into project, psychological, social, and structural determinants based on the taxonomy originally proposed by Staw and Ross (1987).

7.2 Synthesis of the Research Findings

The major contribution of this thesis has been to develop a socio-organizational model, which can be used to analyse future research studies and shed light into the social, organizational dimensions of information systems security. This contribution has implications for issues that have been raised throughout the research, either as shortcomings of previous research work or as findings in the empirical research setting. This section summarises and presents the findings within each of the main chapters.

1. From a literature review it was found that the social organizational roles of information systems (IS) security are important and need to be investigated if information systems security is to be achieved.

2. In an attempt to address the different social organizational roles of IS security, the researcher established a multi-conceptual model for the management of information systems security. The suggested model is based on a consistent set of socio-organizational aspects namely: (a) trust; (b) culture; (c) risk communication; (d) goal setting; and (e) goal commitment.

3. In academic terms, the conceptual model can be used to analyse future research studies and shed light into the socio-organizational dimensions of information systems security. In practical terms, the conceptual model can be used by IT managers and practitioners to improve the efficiency of the process of goal setting and therefore, their overall performance in managing effectively information systems security in the internet banking context.

4. The undertaking of empirical studies revealed that IT managers and groups do set security goals with regard to the management of the integrity, confidentiality, and authenticity of information through the internet banking channel, which satisfies the first objective of this research. Goal setting activities within the three organizations were mainly distinguished into three phases: the goal setting initiation phase, the goal execution phase, and the evaluation phase although one of the organizations (Delta-Bank) adds another phase in the process, that of monitoring.

5. The security of internet banking was carefully considered within all the three organizations, as part of the risk management process, and the possible risk related opportunities and threats were identified by the use of checklists. An example of such a checklist was provided by the case of Alpha-Bank and it is included in Appendix C3.

6. It is empirically verified through the three case studies that there is indeed an interrelationship between trust, culture and risk communication and that these socio-organizational aspects have an ultimate effect on the level of goal setting. However, this interrelationship and effect is stronger in organizations with small structure size because such organizations exhibit 'family-oriented' business patterns whereas the values and beliefs are strongly held and widely shared among the organizational members. Although, this interrelationship and effect of such socio-organizational aspects apply to organizations with large structures, their impact is rather minimal because such organizations depend on manuals and procedures, which focus on strict, professional criteria rather than individual initiative and intellect. To this end, the conceptual performance pyramid model can be successfully applied to small organizations rather than large ones.

7. With regard to the background literature on the social and organizational aspects of the performance pyramid model, it was found that trust has a moderate role and in doing so, it provides the conditions under which a strong culture occurs through positive attitudes, increased efforts, participation to group activities, satisfaction of employees that their efforts are rewarded by top-management, higher levels of co-operation and efficient co-ordination of group activities. Trust also provides the conditions under which an efficient communication of risks occurs through positive attitudes, increased efforts, employees' satisfaction to top-management decisions and employees' motivation.

8. It was found also that a strong culture provides the conditions under which an efficient communication of risks occurs through an efficient co-ordination and control of group activities, increased efforts, employees' motivation to contribute in the group, clarity of goal achievement and goal alignment.

9. Although the concepts of trust, culture and risk communication are closely interrelated they are not always mutually dependent variables. That means, these aspects may exist within an organization independent of each other; for example the culture within an organization may be strong but the trust levels low, although it was found that trust facilitates the establishment of a strong culture within organizations and the efficiency of risk communication to be achieved.

10. Trust, defined in simple terms as the willingness of one party (individual) within the IT group to co-operate with another party in order to produce efficient work outcomes, plays an important role on the level of goal setting through the provision of characteristics under which a strong culture and an efficient risk communication occur. For example, when the employees are satisfied from the top-management in the sense that their efforts and work outcome are either morally or financially rewarded, they are motivated to contribute in the group.

11. The culture strength of a group plays also an important role on the level of goal setting through the provision of characteristics under which an efficient communication of risks occurs. For example, in a strong group culture there is clarity of goal achievement and goal alignment, which in turn provide better co-ordination and control of the group activities with an ultimate effect in the process of goal setting.

12. Risk communication plays also an important role on the level of goal setting, as the activities of the IT group have to be in co-ordination with the overall activities of the organization. The perception of risks was also an important factor for an efficient communication of risks and to this end, educational seminars and training courses on risks and security issues was necessary.

13. From the empirical studies the determinants of trust, culture and risk communication were also identified and presented in a tabular form in Tables 12, 13, 14, and 15 respectively. The determinants of commitment at group level were also identified and distinguished (Table 18) into project, psychological, social and structural determinants based on the taxonomy originally presented by Staw and Ross (1987).

14. The existence of different political agendas- different stakeholders' interests- was found to have a greater impact to large organizations as compared to small ones. On the contrary, the case of Alpha-Bank with the small structure had greater flexibility in decision making and consistency within group activities as compared to the cases of Delta- and Omega-Bank with large structures.

15. The ontology of this research with regard to security is that, security should not be treated as something tangible and concrete but also as a social, organizational issue and that was best described by a socio-organizational approach to security within three organizations.

16. The empirical results with regard to trust, culture, risk communication and commitment were similar to the theoretical findings obtained from the socio-organizational literature, which confirm that theories from other disciplines are also applicable to the information systems security context.

17. A major conclusion with regard to security goal setting was determined within the research and is something that has not been proven in research yet. In particular, the research has shown that the issues of trust, culture and risk communication play an important role in the process of goal setting within the information systems security context. To this end, failure to recognize and improve different social and organizational aspects such trust, culture and risk communication may lead to an inefficient process of goal setting, whereas security risks with regard to the management of the integrity, confidentiality, and authenticity of information through the internet bankng channel, may arise.

18. The conflict type that was found within the three case studies was mainly due to differences in business scopes between units rather than due to inefficient knowledge on the subject matters. These conflicts were most commonly existent in organizations with large structures than in the case of Alpha-Bank with the small structure.

19. The investigation has shown that the use of Schein's typology of organizational culture can be used and operationalised for the study of groups within organizations.

20. In this investigation, the chosen research methodology approach was described and it was concluded that research of this kind would benefit by a qualitative approach. In turn, the use of interpretivism was also beneficial, as interpretive research provides an understanding of social factors inherent in information systems security as it focuses on human thought and action in socio-organizational contexts.

In order to consider these research findings in a more systematic way, the following sections will consider in turn the theoretical, methodological and practical contributions, thus relating to the concerns raised in the synthesis of results.

7.3. Overview of the Research Contributions

Walsham's view on the possibility to derive generalised conclusions from interpretive systems case study was reviewed in Chapter 3 in the context of research methodology. According to him, interpretive case study research can contribute to the development of concepts, the generation of theory, the drawing of specific implications, and the contribution of rich insight. The following sections in this dissertation illustrate that this thesis has made contributions in each of these four areas by introducing a social organizational model in the information systems security context, describing the process of security goal setting for the internet banking context, discussing the possible interrelationship and effect of trust, culture, and risk communication on the goal setting context, and also by contributing to our understanding of goal setting procedures and information systems security more generally.

Moreover, this thesis has made an important contribution to interpretive research. This has been achieved by exploring and making practical recommendations for the process of goal setting within an interpretive research methodology. Second, it provided an interpretive grounding for social organizational approaches in information systems security. In particular, the research concluded that a social organizational approach is not independent of epistemological assumptions. Rather, this research has reinforced the argument that trust, culture and risk communication may be interrelated and also argued

that these aspects may have an effect on goal setting depending on the organization's structure. In this respect, the research contributes to socio-organizational research in information systems security as well as to interpretive research.

Clearly, the performance pyramid model developed and applied in this thesis has also some implications for the research context. It has shown that it is appropriate and valuable to information systems and internet banking security research. Consequently, it is particularly relevant for providing a rich insight to social and organizational issues of security in the context of information systems and internet banking.

7.3.1 Theoretical Contributions

The first set of important contributions in this research stems from limitations that were identified in the information systems security context. These are related in particular to the study of trust, culture, risk communication and goal setting in this context. The introduction and development of such concepts in this wide research context provided the study of the theories of trust, culture, risk communication and goal setting and how they can be used.

In particular, one important theoretical contribution of this research has been the study of the goal setting theory in the information systems security context. Studying the trends and the recent developments in goal setting research in both the social and organizational literature provided the basis for more extensive developments in these research areas. The concept of goal setting has not been used extensively in the information systems (IS) security literature and this research provided an extensive review of this issue and identified some weaknesses and limitations in its use. Specifically, it highlighted the emphasis of trust, culture and risk communication in the context of goal setting and their role in information systems security management. It has been evident that the concepts of trust, culture, and risk communication have a weak effect on the level of goal setting in the context of IS security to organizations with large IT group structures. A few of the reasons is that large structure organizations have

a wider context of stakeholder interests, intense competition between different groups for project funding, manuals and procedures that are strictly applied, bureaucratic criteria which do not allow individual initiative and intellect and inflexibility in decision making. In effect, as the process of IS security goal setting activities may be inefficient, security risks in relation to the management of the integrity, confidentiality, and authenticity of information through the internet banking channel, may arise.

The adoption of an information systems security perspective has been useful in identifying social and organizational issues that are a consequence of internet banking security management (e.g., trust, culture, risk communication) and which are missed in most information management research.

Another contribution of this research is the application of these socio-organizational roles in the context of internet banking security management, as there is a lack of social and organizational approaches in the scope of internet banking. Contribution of the theories of trust, culture, risk communication and goal setting is related with the use of the concepts in a new and different domain of the social and organizational behaviour. In the case of internet banking security, the IT managers can enhance the efficiency of the process by which security goals are being set and in so doing, to improve the performance of their IT groups in managing effectively internet banking security. However, as organizations' reputation relies on the security of providing financial products and services to their customers, these social and organizational issues should not be overlooked.

Likewise, the use of Schein's typology of organizational culture to describe the cultural characteristics of the three cases studies, is an important contribution since it shows that such typology can be used and operationalised for the study of groups within organizations. The use of such typology was parallel to ethnographic observations.

The identification of the determinants of trust, culture, risk communication and goal commitment was also another important contribution since academics and practitioners can have a useful insight into how to determine such variables in order to understand human behaviour in the context of information systems security management.

The use of performance pyramid model suggested in this dissertation was a useful tool for the exploration of issues related to information systems security not only from a managerial viewpoint but also for considering different implications in the process of security goal setting with regard to internet banking. This investigation demonstrated, by interrelating the concepts of trust, culture, risk communication and goal setting in the context of information systems security phenomena that these concepts are useful in considering multiple social and organizational viewpoints of security in internet banking activities.

7.3.2 Methodological Contributions

The most important methodological contribution of this research has been the use of the interpretive epistemology in a social and organizational context of information systems security management. The socio-organizational concepts of trust, culture, risk communication and goal setting were used to identify an interpretive approach to the management of information systems security, an area in which most approaches fall short of interpreting the social aspects of IS, e.g., socio-technical and social organizational roles of IS security.

In this research, it was argued that goal setting with regard to internet banking security is a dynamic process that changes frequently and thus having a consistent set of socio-organizational values that may provide a better understanding and control of how to set efficiently security goals is very important. The unit of analysis was the process of goal setting in the context of information systems security consistent with a set of socio-organizational aspects such as trust, culture, and risk communication, which provide a new dimension to information systems security.

Another methodological lesson for information systems security researchers relates to the adoption and use of concepts in related research areas. Information systems research has often used concepts and theories from different domains without exploring their implications in depth. Although, in this research there are issues that need further

development and understanding due to the complexity of social and organizational issues in the context of IS security management, this research has demonstrated how the selective focus on social and organizational aspects of IS security and the emphasis on the process of goal setting with regard to internet banking security has limited the scope and implications of previous research. The ontology of the research with regard to security is that, security should not be treated as something tangible and concrete but also as a social, organizational issue. To this end, the investigation of social and organizational aspects of goal setting theory in the context of IS security management has contributed to a more holistic consideration of socio-organizational issues. It allowed the research to break away from the narrow-technically oriented solutions of most IS security approaches to a variety of social, organizational and political issues that are of concern to researchers and practitioners alike.

7.3.3 Practical Contributions

The most obvious practical contribution of this research is the rich insight it provided to the context of goal setting with regard to the management of information systems and internet banking security. This is evident first in the different social and organizational aspects of goal setting in the context of security. The interrelationship of trust, culture, and risk communication provides useful insights into how trust provides the conditions under which a strong group culture and an efficient communication of security risks occur as well as how culture provides also the conditions under which risk communication can become more efficient. Likewise, the effect of these socio-organizational aspects to goal setting show their importance in the context of risk management with regard to internet banking security. In turn, the identification of the determinants of trust, culture, and risk communication can show to IT managers and practitioners how to make such variables more consistent in order to obtain an efficient process goal setting within groups.

The second part of the performance pyramid model shows that in complex task environments, i.e. goal setting, if people are assigned specific, challenging goals (given

goal acceptance), people's commitment to the goals will increase. In the same line of reasoning, the goal level, commitment, and performance have a complex relationship including both direct and moderator effects. That is, when the goal level is held constant, it appears that there are direct effects of commitment to performance. Although, this relationship is not in the scope of this investigation, the identification of the determinants to commitment at group level can be useful in order to understand possible problems faced by groups.

In addition, the study of the goal setting theory in the context of risk management can be useful for organizations and particularly for IT managers and groups, as they can compare their own procedures with the results reported in this dissertation and identify differences and/or similarities. In addition, the example of the checklist with regard to internet banking security risks, exhibited in Appendix C3, can be useful as it gives an overview of the internet banking security threats and opportunities.

7.4 Limitations of the Research Approach

The interpretive research approach has been criticised for the significant influence the researcher's interpretation might have on the findings. This influence has been acknowledged in this investigation, by using material from multiple case studies, various resources, and most of all from the practitioners' views. The main limitation in an interpretive information systems security research is that the empirical results will depend heavily on the access that organizations and particularly IT managers allow to the researcher. This access is critical for investigating social and organizational issues and for eliciting the interviewees' interpretations of information systems security. However, if the interviewees do not see the data collection process as legitimate they will be unlikely to participate in the process. Likewise, the issue of information systems security is considered highly sensitive and confidential and thus access to the IT departments is difficult. Nevertheless, the inquiry to investigate the social and organizational aspects of information systems security rather than the technical side proved to be of interest to the organizations. In fact, an important aspect of gaining

access to the organizations and particularly to the IT departments was the promise to deliver the results of the findings obtained. Thus, stating the benefits to organizations was an important criterion of gaining access.

Further, 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, the researcher in this investigation attempted to address this issue by developing a conceptual model based on social and organizational factors that may play an important role in the context of information systems security management. Although, qualitative research does not offer the pretence of replication since controlling the research will destroy the interaction of variables, the researcher conducted the investigation within a structured methodology guided by the socio-organizational concepts of the performance pyramid model, as he considered the investigation of such independent variables more appropriate and safer based on the literature review. However, having completed the research process a lesson that can be learned is that a positivist approach may have also been suitable to investigate the interrelationship and effect of different socio-organizational factors.

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

7.5 Recommendations for Further Research

The research contributed to a rich understanding of information systems security in the context of internet banking by using social organizational aspects in the context of goal setting. To this end, it offered a novel social organizational approach to information

systems security by establishing the performance pyramid model. Further research could investigate whether the relationship between goal level, commitment and performance in the context of information systems security with regards to internet banking applies at a macro level.

The case study research suggests that IS security goal setting is influenced by a number of factors in the social organizational context of trust, culture and risk communication. 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 the effects of the social organizational considerations. In addition, future research on the determinants of trust, culture, and risk communication can identify new determinants in the context of IS security.

Although, the study utilized an extensive amount of qualitative data, no quantitative measures of commitment or its determinants were used. Clearly, future research can build upon the findings of this research by examining additional cases and by trying to develop and use quantitative measures of the various constructs. Likewise, another issue interesting to investigate would be the role of feedback in goal setting and performance in the context of information systems security, e.g., whether the type of feedback (outcome or process feedback) provided affects the goal-performance relationship. In addition, to examine the relationship of goals, type(s) of feedback, and performance in security risk management projects.

Ultimately, the performance pyramid model could be applied to other information systems domains such as software development, information systems evaluation at organizational level, simulation modeling, or software programming. It could also be used at an organizational human behaviour management level.

LIST OF ABBREVIATIONS

ISs	Information Systems Security
CRAMM	CCTA Risk Analysis Management Methodology
PARA	Practical Application of Risk Analysis
ITSEC	Information Technology Security Evaluation Criteria
TCSEC	Trusted Computer Systems Evaluation Criteria
BS7799	British Standard
INFOSEC	Information Security

APPENDICES

Appendix A1: Schein (1990) Typology of Organizational Culture

Dimension	Questions To Be Answered
1. The organization's relationship to its environement	Does the organization perceive itself to be dominant, submissive, harmonizing, searching out a niche?
2. The nature of human activity	Is the "correct way for humans to behave to be dominant/proactive, harmonizing or passive/fatalistic?
3. The nature of reality and truth	How do we define what is true and what is not true; and how is truth ultimately determined both in the physical and social world? By pragmatic test, reliance on wisdom, or social consensus?
4. The nature of time	What is our basic orientation in terms of past, present, and future?
5. The nature of human nature	Are humans basically good, neutral, or evil, and is human nature perfectible or fixed?
6. The nature of human relationships	What is the correct way for people to relate to each other, to disctribute power and affection? Is life competitive or cooperative? Is the best authority system autocratic/paternalistic or collegial/participative?
7. Homogeneity vs. Diversity	Is the group best off if it is highly diverse or it is highly homogenous? Should individuals be encouraged to innovate or conform?

Source: Adapted from E.H. Schein, Organizational Culture, American Psychologist, 1990, p.114.

	PROJECT DETERMINANTS	PSYCHOLOGICAL DETERMINANTS	SOCIAL DETERMINANTS	STRUCTURAL DETERMINANTS
Level of analysis	The project	Each decision maker	Each decision maker and his/her social group	The organization and the IS function
Description	Objective features of the project, reflecting costs and benefits	Attributes of the decision maker's relationship with the project	Features of the social group surrounding each decision maker	Contextual conditions surrounding the project
Determinants	• Large payoff (Keil, 1994) • Long-term payoff structure (Ross and Staw, 1986; 1993) • Large closing costs (Ross and Staw, 1993) • Low salvage value (Ross and Staw, 1986; 1993) • Infeasibility of alternatives (Keil and Mixon, 1994) • Ambiguous performance data (Ross and Staw, 1986; 1993) • Temporary cause of setback (Keil, 1994)	• Personal responsibility for failure (Staw, 1976; Bazerman et al., 1982; Davis and Bobko, 1986; Haunschild, et al., 1994; Keil, 1994) • Information processing errors (Ross and Staw, 1986; 1993; Keil, 1994) • Framing (Davis and Bobko, 1986) • Sunk costs (Garland, 1990; Keil and Mixon, 1994) • Reinforcement traps (Ross and Staw, 1993) • Comtinuity of champion (Ross and Staw, 1993; Keil, 1994) • Emotional attachment (Keil, 1994) • Prior history of success (Keil, 1994) • Strong and repeated support in the past • Value attached to turnarounds	• Public identification with the project (Ross and Staw, 1993) • Responsibility for failure (Caldwell and O' Reilly, 1992) • Competitive/political rivalry (Rubin et al., 1980; Haunschild et al., 1994; Keil, 1994) • Successful models of persistence (Staw and Ross, 1980; Brockner et al., 1984; Ross and Staw, 1993) • Norms of consistency (Ross and Staw, 1993; Keil, 1994) • Public decision context (Haunschild et al., 1994) • Emotional attachment (Keil, 1994) • Prior resistance encountered (Fox and Staw, 1979)	• Political support for the project, including top management support (Ross and Satw, 19851, 1993; Keil, 1994) • Institutionalization, or strategic nature of the project (Ross and Staw, 1986, 1993) • Economic and technical side bets (Ross and Staw, 1993) • Slack resources (Keil, 1984)
				• Administrative inertia • Top management's knowledge of information technology • Information intensity • IS maturity

Table 2.2 Determinants of Commitment to Projects (Staw and Ross, 1987)

* Most, but not all, of the determinants listed in this table have been empirically tested
And supported in prior research on escalation. The determinants shown above the dotted line have been supported in the cited empirical research. The determinants shown below the dotted line have not received empirical support.

Appendix B: Interview Questions

A Socio-organizational Approach to Information Systems Security: The Case of Internet Banking

Date of Interview:

Name of Interviewee:

Job and Position Title:

Organization and its Nature (Private, Semi-public, Public):

Years in Organization:

Years in Industry:

Responsibilities:

Academic Declaration:

The researcher aims to investigate and deepen understanding of the possible interrelationship, interaction and impact of different social organizational concepts, part of the suggested theoretical performance pyramid model, in the context of information systems security management. The suggested model is consisted of social and organizational aspects such as trust, culture, risk communication, and goal commitment in the context of setting security goals for the management of internet banking risks. To this end, the information obtained through the interviews and through the use of any organizational material such as white reports, documents, and archival records will be used strictly for academic and research purposes and thus confidence is being assured. For any further requirements and/or comments on the research issues please do not hesitate to ask for more details prior to investigation commencement.

Appendix B1: Goal Setting Questionnaire

1. How would you describe a goal?
2. Do you have yearly goals? How are they set? Does the IT manager have any input? Does any other unit have any input?
3. How are the goals accomplished? How is the decision of security systems made? How was the process originally constructed? What input from top-management? What input from other units?
4. Do you have any specific goal setting procedure/s in risk management?

- If yes, do you have separate groups for internet banking security and information systems (IS) risks? How are they integrated?
- If no, who is responsible for internet banking security? Information Systems (IS) security?
- How are the goals accomplished?

5. What is the nature of goals at an organizational level?
6. What is the nature of goals at an IT group level?
7. Is clarity in goal achievement important?
8. Do you have top-management's support in goal achievement?
9. What criteria are used to measure results? What data indicators do you consider most important?
10. Do employees participate in goal setting?

- If yes, how often? To what extend?
- If no, why not? Do you think that participation should be encouraged?

11. Does goal setting improves group performance in managing security risk activities and how?
12. Have you changed your risk assessment instrument/process in the last year, or more?
13. Do you have feedback in goal setting?

- If yes, does feedback is valuable?
- If no, how the risk management process should be improved?

14. Do you have conflicting goals within the organization? Group?
15. Do you prefer goals to be group-assigned, or group-participated?

- If group-assigned, do you copy better with difficult assigned goals?
- If group-participated, do you copy better with more difficult goals?

Appendix B2: Trust Questionnaire

1. What does this organization mean by "trust"?
2. What is the meaning or intent of trust within your group?
3. Do you believe that trust is an individual characteristic or a behavioural expectation among parties (individuals) within the organization?
4. Would you take the risk to co-operate with another party (in your group) in a given task?
5. Do you believe that you can depend on the group or on other individuals within the group to succeed in any work related task?
6. Do your efforts are recognised by your colleagues? By top-management?
7. Do high levels of trust within the group have an effect on culture? How?
8. Do high levels of trust within the group have an effect on the communication of risk messages? How?
9. Do high levels of trust within the group have an effect on the level of goal setting? How?

Appendix B3: Culture Questionnaire

1. What does this organization mean by "culture"?
2. What is the meaning or intent of strong culture within your group?
3. What is the Core Mission? Do you have a Mission Statement? What are the primary tasks of your group?
4. What things make it easy or hard for you to do your job? Which terminology do you find yourself using to describe your purposes?
5. Do you attend training seminars with regards to internet banking security? Do the new group members attend to training programs before they start?
6. How is an employee rewarded for exceptional "success"? What are the routine procedures for promotion? Are there extraordinary means of promotion? Are there other, symbolic means of honoring employees?
7. If you used a "family metaphor" to describe your group, how would you describe it, i.e., traditional, partnership, single parent or orphan? Are staff more "professional" or more "collegial"? Is team work encouraged?
8. How are sanctions of group members applied? What is the formal process? Is there an informal process?
9. How are critical events handled?
10. In general, what is the "correct way" for humans to behave, dominant/pro-active or harmonizing or passive?
11. Is life co-operative or competitive? Are groups best organized on the basis of individualism or "collectivism"? What is the best way to exert human authority, i.e., autocratic/paternalistic or collegial/participative?

12. How co-ordination of activities within the group takes place?

13. Given the definition of strong cultures- Does a strong culture have an effect on the communication of security risk messages? How?

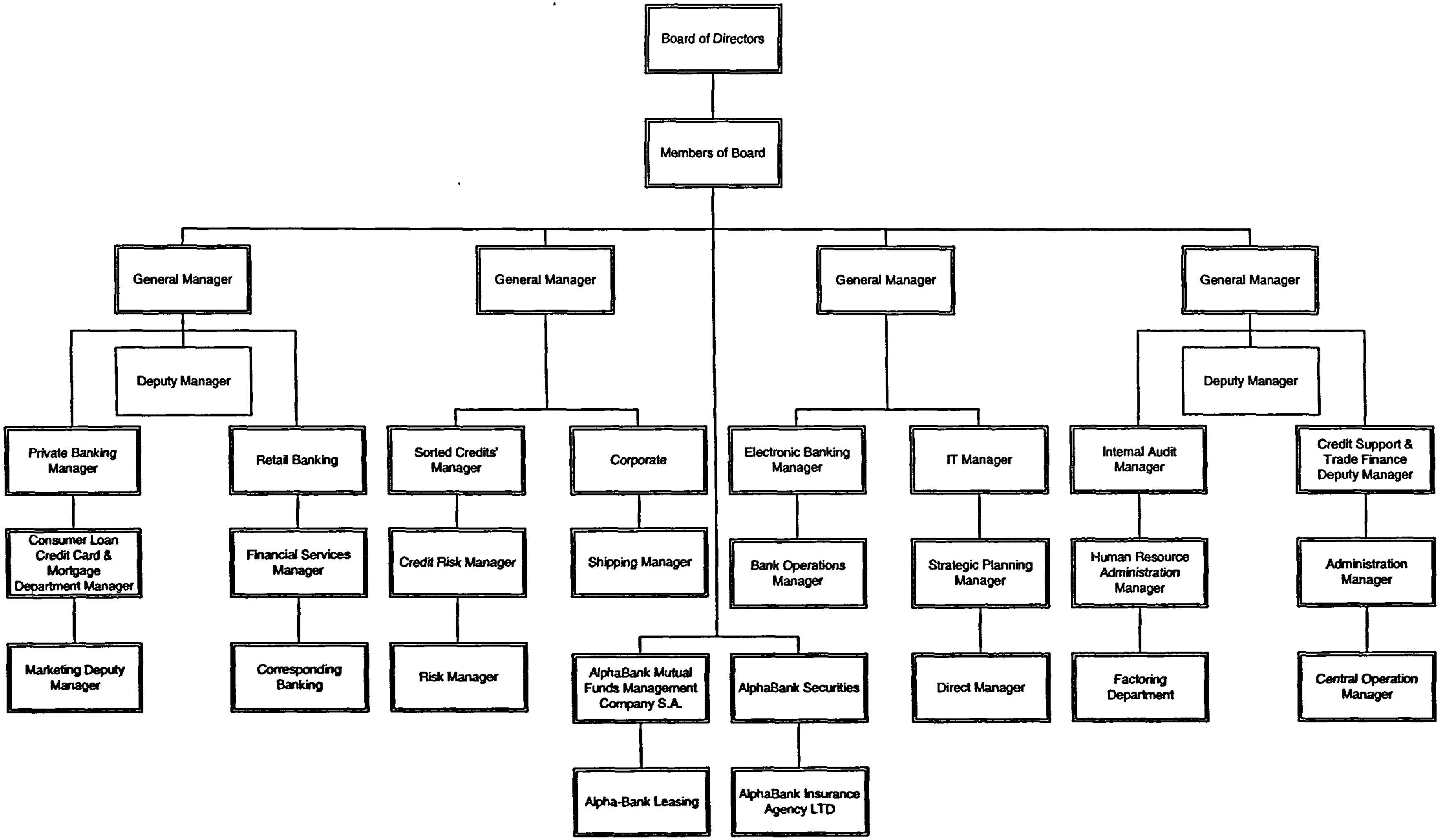
14. Does a strong culture have an effect on the level of goal setting? How?

Appendix B4: Risk Communication Questionnaire

1. What does this group mean by "communication"?
2. What is the purpose or intent of the communication?
3. Who should be involved in the communication process and at what stages?
4. What kind of communication plans, techniques, mechanisms are now in use for communication of security risk messages, e.g., notices, announcements, forums, e-mails, reports?
5. What is risk? What is the meaning of security in the context of internet banking? Do you believe that security should be approached by a different angle other than technical?
6. What kinds of risks should be of first priority to your group? To the organization?
7. What impediments, barriers, or facilitators do currently influence security risk communication?
8. What funding is available or is needed for risk communication activities?
9. Can/should topic-specific workshops be offered in groups prior to the need for project specific decision-making?
10. Does an efficient communication of risk messages have an effect on the level of security goal setting? How?

Appendix B5: Goal Commitment Questionnaire

1. What does this group mean by "commitment"?
2. Do you believe that commitment is essential to goal achievement?
3. Do you have multiple goal levels?
4. Are you likely to be more committed when the goals are challenging, or easy?
5. Do you have sense of goal achievement?
6. Do you feel competitive within your group?
7. Is there a motivation within your group to try for a goal?
8. Are you prepared to work overtime, if needed, to successfully implement a project?
9. What are the determinants of group commitment?


Board of Directors
Members of Board
General Manager
General Manager
General Manager
General Manager
Deputy Manager
Deputy Manager
Private Banking Manager
Retail Banking
Sorted Credits' Manager
Corporate
Electronic Banking Manager
IT Manager
Internal Audit Manager
Credit Support & Trade Finance Deputy Manager
Consumer Loan Credit Card & Mortgage Department Manager
Financial Services Manager
Credit Risk Manager
Shipping Manager
Bank Operations Manager
Strategic Planning Manager
Human Resource Administration Manager
Administration Manager
Marketing Deputy Manager
Corresponding Banking
Risk Manager
AlphaBank Mutual Funds Management Company S.A.
AlphaBank Securities
Direct Manager
Factoring Department
Central Operation Manager
Alpha-Bank Leasing
AlphaBank Insurance Agency LTD

Appendix C2: Alpha-Bank 2001 Information Technology Goals Report (Abstract)

1. Central Systems Architecture

The architecture establishment and full operation of the two new central UNIX engines (S80 & M80) as well as the establishment of the system saving data Shark in a common line, so as to achieve the support of the Globus operations (Development of applications-Operational Acceptability- Production).

Expected Benefits:

- The improvement of time analysis/development of applications
- The existence of a complete replicate of Production for direct control of possible problems and the empowerment of backup procedures
- The existence of a senario for the operational transportation of Production- within a few hours- from the main engine to the secondary in case of problems in the first one
- The possibility of establishing and activating the mechanism Archiving of Globus so that search in past data on transactions is established without to aggravate the Production system.

2. Technological Platform Globus

The establishment in Production of the edition G11 of Globus in substitution of the G9. The stage substitution of GUI with the Desktop to customers.

Expected benefits:

- The solution of Globus basic architecture problems (multithreading-multiprocessing) and the operational improvement in Batch and in On-line.
- The solution of many operational problems (bugs) which were mentioned by users concerning the bank's editions as well as G10 and products where the IT department is thinking to develop such as (MGs, Trade Finance, etc.)
- The improvement in stability and the strategic development of logistics of Globus (e.g., OFS, IBI, for eGLOBUS)

The consideration for the substitution of UniVerse from Jbase.

Expected benefits:

- The complete transition of the whole Globus operating section into technological data basis platform where its development is made by Temenos

- The last two core changes are capable presuppositions for the establishment and operation of eGlobus. In addition the triptych- IBM Hardware- Jbase- G11, edition of Globus- is compatible with Temenos for the new era of Globus.

3. New Products Development in Globus

The development of new products into Globus which briefly are: MGs, Debit Card, LDs, Visa Acquiring, Cash Advance, eGlobus.

Expected benefits:

- The promotion in Production of new banking products and the empowerment of the bank's competitive status
- The erasure of various peripheral products and the empowerment of Globus central system
- The empowerment of the group's programmers knowledge which develops and supports the specific platform Globus.

4. Project Euro- Second Phase

The completion time of all necessary changes in platforms such as Globus, FEP, ATMs, Peripheral Applications, so the bank can operate according to law regulations for the substitution of Drachma to Euro currency.

5. E-banking of Peripheral Applications

The adaptation of all parameters of the electronic infrastructure (WAN, LAN, Internet connections, communication of peripheral applications with Globus, Client infrastructure, Server infrastructure and management) for the operation of peripheral applications (eON, SWIFT, Abacus, e-mail).

Expected benefits:

- The completion of transition of important Unit proceedings from manual procedures to new procedures of electronic form and management
- The limitation of hardware and software mixture in peripheral applications
- The gathering of mutli-peripheral applications under one platform and the their management base on new procedures.

6. e-Banking

The consideration for the structure of a new Internet platform (software/hardware) in which other applications can be transferred (as an operation) and to develop new applications. The three product categories the IT department considered are:

Internet banking (Web-Teller)
Payment System (Web-Shop, Web-Trader)
e-Commerce (e.g. Merchant Hosting)

Expected benefits:

- The strategic bank's status in the area of e-Banking
- The improvement of the technical operation of applications and the addition of new applications which can introduce new products
- The establishment of a 24-hours environment of Production for the Internet
- The completion of connection between Internet and the bank's Central system

7. Technology and Operational Costs

The suitable use of technology (and especially of tele-communications) directed in limiting the operating costs for the bank.

Expected benefits:

- The control of the banks expenses and the reasons which cause them (e.g. extra-ordinary use of mobile phones)
- The registration of options (technical and political) available focused on the direction of limiting costs without the parallel reduction of services offered
- The option and development of the 'desired solution' (e.g. VPNs, Video-Conferencing, etc.).

Alpha-Bank: Appendix C3 Internet Banking Security Checklist

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

Appendix D1: Delta-Bank- BASIC ORGANIZATIONAL STRUCTURE-

PRODUCTIVE STRUCTURE

CORPORATE- CONSUMER BANKING GROUP

CUSTOMER DIVISION (CORPORATE BANKING)
CUSTOMER DIVISION (CONSUMER BANKING)
CUSTOMER DIVISION (PRIVATE BANKING)
NETWORK OPERATIONS DIVISION

INSTITUTIONAL BANKING GROUP

CORPORATE DIVISION
PROJECTS & CONSTRUCTION COMPANIES DIVISION
PUBLIC SECTOR DIVISION
SHIPPING DIVISION
FINANCIAL INSTITUTIONS DIVISION

I.T. AND OPERATIONS BANKING GROUP

INFORMATION TECHNOLOGY DIVISION
ORGANIZATION DIVISION
ACCOUNTING DIVISION
EXECUTIVE OPERATIONS DIVISION

STRATEGIC MARKETING AND ALTERNATIVE NETWORKS BANKING

STRATEGIC MARKETING DIVISION
ALTERNATIVE NETWORKS DIVISION

CENTRAL EXECUTIVE/ SUPPORTING STRUCTURE

HUMAN RESOURCES DIVISION
AUDIT DIVISION
CREDIT POLICY DIVISION
SECRETARIAT DIVISION
PUBLIC RELATIONS DIVISION
LOANS IN ARREARS DIVISION
PLANNING AND ECONOMIC ANALYSIS DIVISION
RISK MANAGEMENT DIVISION
DOMESTIC SUBSIDIARIES DIVISION
INTERNATIONAL DIVISION
PROPERTY DIVISION
SUPPORT DIVISION
TECHNICAL ADVISERS DIVISION
LEGAL DIVISION
TRAINING DIVISION
TREASURY DIVISION

REGIONAL DIVISIONS

ATHENS REGION
ATTICA REGION
PIRAEUS AND ISLANDS REGION
CRETE AND DODEKANISOS REGION
PELOPONNISOS REGION
WESTERN GREECE REGION
NORTHWESTERN GREECE REGION
NORTHWESTERN GREECE REGION
THESSALONIKI REGION
CENTRAL GREECE REGION

Appendix D2: Performance Measures Indices (Delta-Bank)

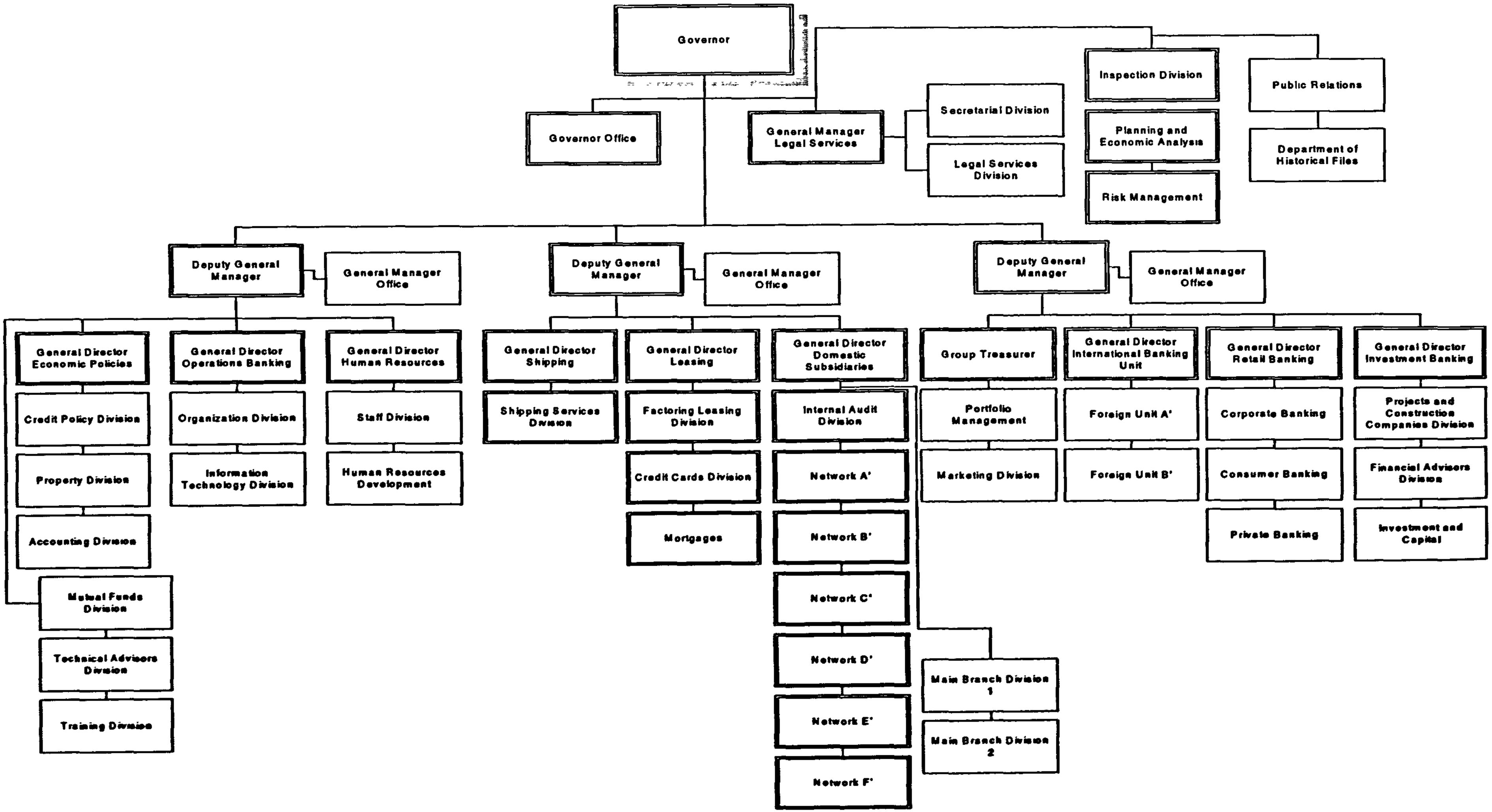
The following are some index measures currently considered in the context of Delta-Bank IT performance criteria. These measures are not applied yet.

Measure 1:

The strategic design unit of Delta-Bank has established a system based on some indices according to which it would be possible to measure the performance of IT. One such index is the telecommunications costs in relation to banking transactions. Banking transactions is possible to measure: e.g., the number of deposits, withdrawings, loans. Telecommunications costs are also possible to measure: e.g., one telecommunication line between Athens and Thessaloniki has a specific cost. In the same line of reasoning, the total cost of the telecommunications to support the bank's infrastructure can also be estimated. This total cost is then subdivided and an index is being developed which can be used to measure whether the IT improves the total cost of telecommunications. The IT group therefore with continuous monitoring of the telecommunication lines can estimate whether the lines need to be upgraded or if necessary to changes the line arrangements to a certain point. If some of the lines are not being used to satisfied degree, the IT group cancels them and finds other line patterns. Thus with such an index it would be possible to measure the IT performance in reducing the telecommunications costs. Based on that index it would also be possible to define the bonus that corresponds to the unit and set a standard for the next year.

Measure 2:

Another index is the business functions as a result of applications e.g., new services in internet banking such as the employees payment scheme so that the companies can have access and control their employees' payment schedules without having to send an accountant to the bank each month. The applications record a code based on the business requirements that originate from the board of directors and the other units of the bank. According to the number of applications or the services offered, an index is also being established.



Appendix E1: Omega Organizational Chart

Appendix E2: DESCRIPTION OF THE DATA ANALYSIS TECIINIQUES

This appendix shows the technique used for the analysis of data, within all of the three case studies, in more detail. This will provide to the reader a deeper understanding of how the analysis of data was taken place and an individual feel of the iterative process involved in obtaining the data.

DETAIL OF THE PROCESS OF CODING

After the interviews were recorder, the next step was to transcribe them. The outcome of the transcriptions was in the form of 'raw' interview data (word-document) achieved from each of the case studies. Based on the socio-organizational aspects of the performance pyramid model each time that a particular concept was mentioned or explained it was marked off. For example, during the interviews when asking about risk communication, the question was of the type:

"Does a strong group culture affects the process of goal setting with regard to security"?

The response obtained was of the type:

"Strong culture defined as what and in what sense to affect the process of goal setting"?

At this point, the first step was to give the definition of strong culture. Once the definition was given, the respondent mentioned the phrase political agendas. Then, the term political agendas was marked, and a note was made on the beginning of a set of sheets separated by each organization's name. Based on the process of coding suggested by Rubin and Rubin (1995), the page number that the term political agendas appeared on was also stated on the another page of the set of interviews.

DESCRIPTION OF THE PROCESS OF THEORETICAL IMPLICATIONS

As the interview process proceeded, the researcher focused even in more detail to questions within the context of each socio-organizational aspect of the performance pyramid model. For example, when questions about political agendas started, the researcher then focused on the nature of political agendas within each organization.

Questions: *"Could you explain into more detail about the nature of political agendas"*?

Response: *"I am not sure if I go into more detail to the degree that you may want to, but for example, there are quite often an argument about the activities of the IT and operations and group. For example, if the IT manager proposed a new project that was important and necessary for the efficient operation of other internet banking applications, another department will intervene and require specific details of the proposed benefits of the project. This was the case when different departments had also at the same time project proposals and were thinking competitively on the basis that the technology projects will get more funding over them. However, this had also a negative outcome on the IT group's activities as some projects had to be delayed until a decision was made from the board of directors. Although, this phenomenon does not take place to a great extend since enough funding is always available. It happens though in cases where project funding requirements reach millions of Euros".*

This result was important for the data analysis, as it became clearer that political agendas were existent within organizations and although they were of business nature rather than personal, they did have an effect on groups' activities. An observation was also made of the degree to which different political agendas had an effect on the culture of the groups and ultimately, on the goal activities planned. For example, it was observed that such political agendas had a stronger effect in organizations with large structures than in organizations with small structures such as Alpha-Bank. Thus, the implications of

political agendas within the organizations' culture were recorded and noted. All these responses assisted in the analysis of data.

During the interviews within organizations there were times upon which some issues had to be left until the next time due to limited time on the part of the interviewees. To this end, the next time of interview appointment with the same individual, the researcher attempted to revive the initial stage of interview and remind the individual of the issues under discussion by saying:

"From our last meeting, the issue of security related activities within the IT group, was left unfinished. Can we please finish this issue by describing to me into a more detail how the group decides on the security activities to be followed"?

Therefore, what can be concluded from the descriptions is that the process of data analysis involved reading into more detail the text document, obtained from the interviews, and the words in it. In this way, the process of coding and any possible theoretical implications of the socio-organizational concepts within the performance pyramid model were noted from practice. To this end, the researcher ensured that the process provided some meaning and purpose to the collated data.

References

Adams, J. (1995) *Risk*, First published in 1995 by UCL Press.

AFIPS (1979) *Security: Checklist for Computer Center Self-Audits*, AFIPS, USA.

Andersen, I.T. (2001) *Sicherheit in Europa*, Studie 2001, Status Quo, Trends, Perspektiven.

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

Anderson, A.M. et al. (1993) The Risk Data Repository: A Novel Approach to Security Risk Modeling. *Proceedings of the Ninth IFIP International Symposium on Computer Security*, IFIP Sec 1993, Deerhurst, Ontario, Canada, pp.179-188.

Angell, I. (1990). Systems Thinking About Information Systems and Strategies. *Journal of Information Technology*, 5, 168-174.

Angell, I.O. and Smithson, S. (1991) *Information Systems Management: Opportunities and Risk,* Published by McMillan Education LTD, First Edition.

Angell, I.O. (1994) The Impact of Globalisation on Today's Business and Why Information System Security is Strategic, *Proceedings of the 1994 Annual Congress of the European Security Form*, Cologne, Germany.

Angell, I.O. (1996) Economic Crime: beyond good and evil. *Journal of Financial Regulation and Compliance*, 4(1).

Ansell, J. and Wharton, F. (1992) *Risk: Analysis, Assessment and Management*, Chichester, John Wiley and Sons Ltd.

Avison, D.E. Lau, F., Myers, M.D. and Nielsen, P.A. (1999) Action Research,

Communications of the ACM, **42**(1), pp. 94-97.

Backhouse, J. and Dhillon, G. (1993) A Conceptual Framework for Secure Information Systems, *The Tenth World Conference on Computer Security, Audit, and Control*, COMPSEC, London, Elsevier Advanced Technology.

Backhouse, J. and Dhillon, G (1994) Responsibility Analysis: A Basis for Understanding Complex Managerial Situations, *International System Dynamics Conference*, University of Stirling, Scotland.

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.

Baskerville, R. (1988) *Designing Information Systems Security*, John Wiley and Sons, New York,Information Systems Series.

Baskerville, R. (1991) Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, *European Journal of Information Systems*, **1**(2), pp.121-130.

Baskerville, R. (1993) Information Systems Security Design Methods: implications for information systems development, *ACM Computing Surveys* **25**(4), pp.375-414.

Baskerville, R. (1994) Research Directions in Information Systems Security, *International Journal of Information Management*, **14**(5), pp. 375-387.

Beck, U. (1992) *Risk Society: Towards a New Modernity*, Sage Publications, London.

Bell, D. and La Padula (1976) *Secure Computer Systems: Unified Exposition and Multics Interpretation*. MITRE Corp. Bedford, UK.

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.

Beynon-Davies, P. (1997) Ethnographic and Information Systems Development: Ethnography of, for and within IS Development, *Information and Software Technology*, **39**(8), pp. 531-540.

Bhattacharya, R., Devinney, T., and Pillutla, M. (1998) A Formal Model of Trust Based on Outcomes, *Academy of Management Review*, **23**(3), pp. 459-472.

Birch, D. and McEvoy, N. (1992) Risk Analysis for Information Systems, *Journal of Information Technology*, **7**, pp. 44-53.

Birch, D. and Young, M.A. (1997) Financial Services and the Internet: What Does Cyberspace Mean for the Financial Services Industry, *Internet Research*, **7**(2), pp.120-128.

Bleicher, K (1989) To the Management of Inter-Company Co-operation: From the Joint Venture to the Strategic Alliance, In: Buehner, R. (OD.): *Guidance organization and technology management*, Berlin.

Boland, R. (1985) Phenomenology: A preferred approach to research in information systems, In: E. Mumford, R. Hirschheim, G. Fitzerald and A.T. Wood-Harper (Eds), *Research Methods in Information Systems*, Amsterdam, North-Holland, pp. 193-201.

Boockholdt, J.L. (1987) Security and Integrity Controls for Microcomputers: A Summary Analysis, *Information and Management*, **13**, pp.33-41.

Bowen, M.G. (1987) The Escalation Phenomenon Reconsidered: Decision Dilemmas or Decision Errors, *Academy of Management Review*, **12**(1), pp. 52-66.

Bradford, D.L. and Cohen, A.R. (1984) *Managing for Excellence: The Guide to Developing High Performance in Contemporary Organizations*, New York,

John Wiley.

Brockner, J. (1992) The Escalation of Commitment to a Failing Course of Action: Toward Theoretical Progress, *Academy of Management Review*, **17**(1), pp. 39-61.

Burnham, B. (1996) *The Internet's Impact on Retail Banking*, Booz-Allen Hamilton Third Quarter, (http://www.strategy-business.com/briefs/96301).

Burrell, G. and Morgan, G. (1979*) Sociological Paradigms and Organizational Analysis*, Heinman, London.

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

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

Chokhani, S. (1992) Trusted Products Evaluation Process, *Communications of ACM*, **35**(7), pp. 66-76.

Chua, W.F. (1986) Radical Developments in Accounting Thought, *The Accounting Review*, **6**(1), pp. 601-632.

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

Conford, T. and Smithson, S. (1996) *Project Research in Information Systems*, London, MacMillan, Press Ltd.

Crede, A. (1995) Electronic Commerce and the Banking Indusrty: The Requirement and Opportunities for New Payment Systems Using the Internet, *Journal of Computer-Mediated Communication*, **1**(3), pp. 220-243.

Creswell, J. (1998) *Qualitative inquiry and research design*, Sage Publications, Inc., Thousand Oaks, California, USA.

Computer Security Consultants (1988) *Using Decision Analysis to Estimate Computer Security Risk*, Computer Security Consultants, Ridgefield.

Courtney, R. (1977) Security Risk Analysis in Electroni Data Processing. *Proceedings of the AFIPS Conference*, National Computer Conference (R.R. Korfhage), Vol. 46, AFIPS Press, pp.97-104.

Cremer, J. (1993) Corporate Culture and Shared Knowledge, *Industrial and Corporate Change*, **2**(3), pp. 351-386.

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.

Currall, S. and Judge, T. (1995) Measuring Trust Between Organizational Boundary Role Persons, *Organizational Behaviour and Human Decision Processes*, **6**(4), pp.151-170.

Das, T.K., and Teng, Bing-Sheng. (1998) Between Trust and Control: Developing Confidence in Partner Co-operation in Alliances, *Academy of Management Review*, **23**(3), pp. 491-512.

Davis, M. and Bobko, P. (1986) Contextual effects on escalation processes in public sector decision making, *Organizational Behaviour and Human Decision Processes*, **37**(1), pp. 121-138.

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

De Dreu, C., Giebels, E. and Van de Vliert, E. (1998) Social Motives and Trust in Integrative Negotiation: The disruptive effects of punitive capability, *Journal of*

Psychology, 8(3), pp. 408-423.

Denison, D.R. (1990) *Corporate Culture and Organizational Effectiveness*, New York, Wiley.

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

Denzin, N. and Lincoln, Y. (1994) *Handbook of Qualitative Research*, Thousand Oaks, CA: Sage Publications

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.

DeVito, J.A. (1988) *Human Communication*, 4th edition, New York: Harper & Row, Inc.

Deutsch, M. (1962) *Co-operation and Trust: Some Theoretical Notes*, Nebraska Symposium on Motivation, Lincoln: Nebraska University Press, pp.275-320.

Dhillon, G. (1995) *Interpreting the Managing of Information Systems Security*, Unpublished Ph.D Thesis, London School of Economics and Political Science, University of London, UK.

Dhillon, G. and Torkzadeh, G. (2001) Value-Focused Assessment of Information Systems Security in Organizations, *Twenty-Second International Conference on Information Systems*, New Orleans, USA, December 2001.

Dhillon, G. (2001) Challenges in Managing Information Security in the New Millennium, In *Information Security Management: Global Challenges in the New Millennium*, G. Dhillon (ed.), Idea Group Publishing, Hershey, PA.

Dhillon, G. and Backhouse, J. (2001) Current Directions in IS Security Research:

Towards Socio-organizational Perspectives, *Information Systems Journal*, **11**(2), pp.127-153.

Dirks, K.T. (1999) The Effects of Interpersonal Trust on Work Group Performance, *Journal of Applied Psychology*, **84**(3), pp. 445-455.

Dirks, K.T. and Ferrin, D.L. (2001) The Role of Trust in Organizational Settings, *Organization Science*, **12**(4), pp. 450-467.

Dobson, J. (1991) A Methodology for Analysing Human and Computer-Related Issues in Secure Systems, In*: IFIP International Conference in Computer Security and Information Integrity*, Amsterdam, pp.151-170.

Donaldson, L. (1985) *In Defence of Organizational Theory: A Reply to the Critics*, Cambridge University Press, Cambridge.

Doney, P.M., Cannon, J.P., and Mullen, M. (1998) Understanding National Culture on the Development of Trust, *Academy of Management Review*,**23**(3), July, pp. 601-620.

Doonan, P. (2001) Freud, Fishing and Risk Management, *Risk Management* **48**(12), pp.48-52.

D.T.I. (2002) *Information Security Breaches Survey 2002*, Technical Report, April Department of Trade and Industry, London.

Dyer, W.G., Wilkins, A.L. and Eisenhardt, K.M. (1991) Better Stories, Not Better Constructs, to Generate Better Theory: A Rejoinder to Eisenhardt: Better Stories and Better Constructs: The Case for Rigor and Comparative Logic, *The Academy of Management Review*, **16**(3), pp. 613-627.

Earle, T.C. and Cvetkovich, G.T. (1995) *Social Trust: Towards a Cosmopolitan Society*, Praeger, Westport, CT.

Earley, P.C., Connolly, T., and Ekegren, G. (1989) Goals, Strategy Development and Task Performance: Some Limits on the Efficacy of Goal Setting, *Journal of Applied Psychology*, **74**(1), pp.24-33.

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

Erez, M. and Earley, C. (1987) Comparative Analysis of Goal Setting, *Journal of Applied Psychology*, **72**(2), pp. 658-665.

Ernst and Young (2001) *Information Security Survey*, Ernst and Young, London.

Ewusi-Mensah, K. and Przasnyski, Z.H. (1991) On Information Systems Project Abandonment: An Exploratory Study of Organizational Practices. *MIS Quarterly*, **15**(1), pp. 67-88.

Ewusi-Mensah, K. and Przasnyski, Z.H. (1994) Factors Contributing to the Abandonment of Information Systems Development Projects. *Journal of Information Technology*, **9**(10), pp. 185-201.

Ewusi-Mensah, K. and Przasnyski, Z.H. (1995) Learning from Abandoned Information Systems Development Projects, *Journal of Information Technology*, **10**(1), pp. 3-14.

Fisher, R. (1984) *Information Systems Security*, Prentice-Hall, Englewood Cliffs, NJ.

Fitzgerald, J. (1978) EDP Risk Analysis for Contingency Planning, *EDP Audit Control and Security Newsletter*, **6**, pp.1-8.

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.

Frechette, S.K.S. (1991) *Risk and Rationality*, Philosophical Foundations for Populist Reforms, University of California Press, Berkeley, Ch.3, pp.29.

Gable, G. (1994) Integrating Case Study and Survey Research Methods: An Example in Information Systems, *European Journal of Information Systems*, **2**(3), pp. 112-126.

Gadamer, H.G. (1975) *Truth and method*, 2nd revision, (J. Weinsheimer and D.G. Marshall), Crossroad, New York.

Gallegos, F., Dana, R.R., and Borthick, A.F. (1987) *Audit and Control of Information Systems*, Cincinnati, OH: South- Western Publishing Co.

Galliers, R.D. (1987) Information Systems Planning in the United Kingdom and Australia: A Comparison of Current Practice, In: *Oxford Surveys in Information Technology*, Vol.4, P.I. Zorkoczy (ed.), pp.223-255.

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

Garland, H. (1990) Throwing Good Money After Bad: The Effects of Sunk Costs on the Decision to Escalate Commitment to an Ongoing Project, *Journal of Applied Psychology*, **75**(6), pp. 728-731.

Gellatly, I.R. and Meyer, J.P. (1992) The Effects of Goal Difficulty on Psychological Arousal, Cognition and Task Performance, *Journal of Applied Psychology*, **7**(7), pp.694-704.

Gore, A. (1999) Putting People First in the Information Age, In: *Masters of the Wired World*, A. Lee, eds., Financial Times Pitman Publishing, London, pp.31-36.

Groth, E. (1991) Communicating with Consumers About Food Safety and Risk Issues, *Food Technology*, **45**(5), pp. 248-253.

Habermas, J. (1972) *Knowledge and Human Interest,* Boston, Beacon Press.

Habermas, J. (1987) *The Theory of Communicative Action- the Critique of*

Functionalist Reason, Vol. 2, Beacon Press, Boston, MA, USA.

Hagen, J.M. and Choe, S. (1998) Trust in Japanese Interfirm Relations: Institutional Sanctions Matter, *Academy of Management Review*, **23**(3), July, pp. 589-600.

Harrison, J.R. and Caroll, G.R. (1991) Keeping the Faith: A Model of Cultural Transmission in Formal Organizations, *Administrative Science Quarterly*, **36**(6), pp.552-582.

Heide, J.B., and John, G. (1992) Do Norms Matter in Marketing Relationships*? Journal of Marketing*, 56(2), pp.32-44.

Herriot, R. E., and Firestone, W. A. (1983). Multisite Qualitative Policy Research: Optimizing Description and Generalizability, *Educational Researcher*, **12**(3), pp. 14-19.

Hester, R.E. and Harrison, R.M. (1998) *Risk Assessment and Risk Management,* Issues in Environmental Science and Technology, 9, Royal Society of Chemistry, Cambridge.

Higgins, H.N. (1999) Corporate System security: towards an integrated management Approach, *Information Management and Computer Security*, **7**(5), pp.217-222.

Hirschheim, R. and Smithson, S. (1988) *A Critical Analysis of Information Systems Evaluation, IS Assessment: Issues and Challenges*, N. Bjorn-Andersen and G. Davis, Amsterdam, North-Holland.

Hirschheim, R. (1992) Information Systems Epistemology: An Historical Perspective, In: *Information Systems Research: Issues, Methods, and Practical Guidelines*, R. Galliers, (eds.) Blackwell Scientific Publications, Oxford, pp. 28-60.

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

Hitchings, J. (1996) A Practical Solution to the Complex Human Issues of Information Security Design, In: *Information Systems Security: Facing the Information Society of the 21st Century*. Gritzalis, D. (eds), pp. 3-12. Chapman and Hall, London.

Hofstede, G. (1994) *Cultures and Organizations: Software of the Mind*, London, Harper- Collins.

Hoffman, J., Michelman, E. et al., (1978) SECURATE- Security Evaluation and Analysis Using Fuzzy Metrics. *Proceedings of the AFIPS National Conference*, pp. 531-540.

Hui, C.H. and Triandis, H.C. (1986) Individualsim-Collectivism: A Study of Cross-cultural Reseacrhers, *Journal of Cross-Cultural Psychology*, **20**, pp. 296-309.

Hurst, N.W. (1998) *Risk Assessment: The Human Dimension*, The Royal Society of Chemistry, Cambridge.

Hutt, A.E., Bosworth, S.and Douglas, B.H. (1988) *Computer Security Handbook*, MacMillan, USA.

IBM (1972) *Secure Automated Facilities Environment Study 3*, Part 2. IBM, Armonk, NY.

Iivary, J. (1989) Levels of Abstraction as a Conceptual Framework for an Information System, In: Falkenberg, E.D. and Lindgreen, P. (eds.) *Information System Concepts: An in-depth Analysis*, North-Holland, Amsterdam, pp.323-351.

Jaeger, C.C., Renn, O., Rosa, E.A., and Webler, T. (2001*) Risk, Uncertainty and Rational Action*, First Published 2001, Earthscan Publications Ltd., London.

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.

Jones, G. and George, J. (1998) The Experience and Evolution of Trust: Implications for Cooperation and Teamwork, *Academy of Management Review*, **23**(3), pp. 531-546.

Kailay, M. and Jarratt, P. (1995) RAMeX: a Prototype Expert System for Computer Security Risk Analysis and Management, *Computer and Security*, **14**(5), pp. 449-463.

Kanfer, R. (1990) Motivation Theory and Industrial/Organizational Psychology. In: M.D. Dunnette and L.M. Hough (eds.) *Handbook of Industrial and Organizational Psychology*, (2nd edition, Vol.1), Palo Alto, CA: Consulting Psychologists Press.

Kasperson, R. E. (1992) The Social Amplification of Risk: Progress in Developing an Integrative Framework, In: *Social Theories of Risk*, S. Krimsky and D. Golding, Westport, CT, Praeger Publishers, pp. 153-179.

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.

Kiesler, C.A. (1971) *The Psychology of Commitment: Experiments Linking Behaviour to Belief*, Academic Press, New York.

Klein, K.K. and Myers, M.D. (1999) A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems, *MIS Quarterly*, **23**(1), 67-94.

Kosiur, D. (1997) Understanding Electronic Commerce, Microsoft press, Redmond, Wash.

Koskosas, I. (1998) *The Response of Greek Banks to Competition from EMU*, MA Dissertation, Middlesex University.

Koskosas, I. And Paul, R. (2003a) The Performance of Risk Management in the

Context of Goal Setting: The Case of Internet Banking, *Proceedings of the 8th Collaborative Electronic Commerce Technology and Research Conference*, Editors: Thomas Acton, June 24th, pp. 242-249.

Koskosas, I. and Paul, R. (2003b) A Socio-Organizational Approach to Information Systems Security, *International Journal of Risk Assessment and Management*, **4**(2/3), pp. 232-244.

Koskosas, I.V. and Paul, R.J. (2004) Information Security Management in the Context of Goal Setting, *Risk Management: An International Journal*, **6**(1), pp. 19-29.

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

Kramer, R. (1999) Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions. *Annual Review of Psychology*, **50**(1), pp. 569-598.

Krauss, L. (1980) *SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems*, Revised ed. Amacon, New York.

Krimsky, S. and Plough, A. (1988) *Environmental Hazards: Communicating Risks as a Social Process*, Dover, MA: Auburn House Publishing.

Krimsky, S. (1992) The Role of Theory in Risk Studies, In: *Social Theories of Risk*. S. Krimsky and D. Golding, Westport, CT, Praeger Publishers, Inc, pp.13-22.

Krueger, K.H. (1993) Internal Controls by Objectives: The Functional Control by Objectives. *Proceedings of the IFIP/Sec "93*, Computer Security: Discovering Tomorrow, Deerhurst, Ontario, Canada, pp. 151- 164.

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

Lagoutte, V. (1996) *The Direct Banking Challenge*, Unpublished Honours Thesis, Middlesex University.

Land, F. (1992) *The Information Systems Domain. Information Systems Research: issues, methods, and practical guidelines*, R. Galliers, Blackwell Scientific, London, pp.6-13.

Larson, C. and LaFasto, F. (1989) *Teamwork*, Newbury Park, CA: Sage.

Latham, G.P. and Locke, E.A. (1991) Self-regulation through goal setting. *Organizational Behaviour and Human Decision Processes*, **50**(1), pp.212-247.

Laudon, K. and Laudon, J. (1996) *Management Information Systems: Organization and Technology*, New Jersey, Prentice- Hall Inc.

Lederer, A.L. and Sethi, V. (1988) The Implementation of Information Systems Planning Methodologies, *MIS Quarterly*, **12**(3), pp.445-462.

Lee, A.S. (1991) Integrating positivist and interpretive approaches to organizational research, *Organizational Science*, **2**(4), pp. 342-365.

Lee, H. and Liebenau, J. (1996) In What Way are Information Systems Social Systems? A Critique from Sociology, *Proceedings of the First US Academy for Information Systems Conference*, Cranfield School of Management, Cranfield, Bedford.

Lewicki, R.J. & Bunker, B.B. (1995) Trust in relationships: A model of trust development and decline, In B.B. Bunker and J.Z. Rubin (Eds.), *Conflict, cooperation and justice*, San Francisco: Jossey-Bass, pp. 133-173.

Lewicki, R.J., McAllister, D.J., Bies, R.J. (1998) Trust and Distrust: New Relationships and Realities, *The Academy of Management Review*, **23**(3), pp. 438-458.

Lichtenstein, S. (1996) Factors in The Selection of a Risk Assessment Method, *Information Management and Computer Security*, 4(4), pp.20-25.

Liebenau, J. and Backhouse, J. (1990) Understanding Information, Macmillan Press, London.

Loch, K. D., Houston, H.C. Warkentin, M. E., (1992) Threats to Information systems: Today's Reality, Yesterday's Understanding, *MIS Quarterly*, 16(2). pp.173-186.

Locke, E.A. (1996) Motivation Through Conscious Goal Setting, *Applied and Preventive Psychology*, 5(1), pp. 117-124.

Locke, E.A., Saari, L.M., Shaw, K.N., Latham, G.P. (1981) Goal Setting and Task Performance: 1969-1980, *Psychological Bulletin*, 90(1), pp.125-152.

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

Locke, E.A., Frederick, E., Lee, C. and Bobko, P. (1984) Effects of Self-Efficacy, Goals, and Task Strategies on Task Performance, *Journal of Applied Psychology*, 6(9), pp. 241-251.

Locke, E.A., Latham, G.P., and Erez, M. (1988) The Determinants of Goal Commitment, *Academy of Management Review*, 13, pp. 23-39.

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

Locke, E.A., Smith, K.G., Erez, M., Chah, D.O. and Schaffer, A. (1994) The Effects of Intra-Individual Goal Conflict on Performance, *Journal of Management*, 20, pp. 67-91.

Lyytinen, K.J. and Klein, H.K. (1985) The Critical Theory of Jurgen Habermas as a Basis for a Theory of Information Systems, In: *Research Methods in Information*

Systems, E. Mumford, R. Hirschheim, G. Fitzerald, and T. Wodd-Harper (eds.), North-Holland, New York.

Lyytinen, K.J. and Hirschheim, R. (1989) Information Systems and Emancipation, Promise or Threat, In: *Systems Development for Human Progress*, H.K., Klein and K. Kumar (eds.) Elsevier Science Publishers B.V., Amsterdam, pp. 115-139.

March, J.G. (1991) Exploration and Exploitation in Organizational Learning, *Organization Science*, 2(1), pp. 71-87.

Markus, M.L. (1981) Implementation Politics: Top Management Support and User Involvement, *Systems, Objectives, Solutions* 1(4), pp. 203-215.

Markus, M.L. (1989) 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.

Markus, M.L. (1997) The Qualitative Difference in Information Systems Research and Practice, In: *Information Systems and Qualitative Research*, A. S. Lee, J. Liebenau and J. I. DeGross (eds.), Chapman and Hall, London, pp. 11-27.

Mayer, R., Davis, J. and Shoorman, F. (1995) An Integrative Model of Organizational Trust, *Academy of Management Review*, 20(3), pp. 709-734.

Meyerson, D., Weick, K.E., and Kramer, R.M. (1996) Swift Trust and Temporary Groups, In: R.M. Kramer and T.R. Tyler (eds.), *Trust in Organizations: Frontiers of Theory and Research*, Thousand Oaks, CA: Sage, pp. 166-195.

Merkhofer, M. (1987) *Decision Science and Social Risk Management*, Dordrecht, D. Reidel Publishing Company, Holland.

Merten, A. (1982) *Putting Information Assets on a Balance Sheet*. Risk Management, January.

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

Miles, R.E. and Snow, C.C. (1992) Causes of Failure in Network Organizations, *California Management Review*, **2**(1), June, pp. 93-172.

Mingers, J. (2001) Embodying Information Systems: The Contribution of Phenomenology, *Information and Organization*, **1**(2), pp. 103-128.

Mishra, A. and Spreitzer, G. (1998) Explaining How Survivors Respond to Downsizing: The Roles of Trust, Empowerment, Justice, and Work Redesign, *Academy of Management Review*, **23**(3), pp. 567-588.

Mitchell, T.R. (1997) Matching Motivational Strategies with Organizational Contexts, *Research in Organizational Behaviour*, **19**, pp.57-149.

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.

Moreno, V. JR. (2001) On the Social Implications of Organizational Engineering, *Information Technology and People*, **12**(4), pp. 359-389.

Murray, F. (1989) The Organizational Politics of Information Technology: Studies from the UK Financial Services Industry, *Technology Analysis and Strategic Management*, **1**(2), pp. 285-298.

Myers, M.D. (1997) Qualitative Research in Information Systems, *MIS Quarterly*, **21**(2), pp. 241-242.

Myers, M.D. and Avison, D. (2002) *Qualitative Research in Information Systems: A Reader*, Sage Publications, First published in 2002.

National Research Council (1989) *Improving Risk Communication*, Report of the Committee on Risk Perception and Communication, Commission on Behavioural and Social Sciences and Education, National Research Council. Washington, D.C.: National Academy Press.

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

Newman, M., and Sabherwal, R. (1996) Determinants of Commitment to Information Systems Development: A Longitudinal Investigation, *MIS Quarterly*, 20(1), pp. 23-54.

Ngwenyama, O. (1991) *The Critical Social Theory Approach to Information Systems: Problems and Challenges*, The Information Systems Research Arena of the 90s: Challenges, Perceptions and Alternative Approaches. Nissen, H. Amsterdam, North- Holland.

Ngwenyama, O.K. and Lee, A.S. (1997) Communication richness in electronic mail: Critical Social Theory and Contextuality of Meaning, *MIS Quarterly*, 2(1), pp. 145-167.

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.

Otway, H. and Wynne, B. (1989) Risk communication: Paradigm and Paradox, *Risk Analysis*, 9(2), pp. 141-145.

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

O'Riordan, T. (1991) *Innovation and Environmental Risk*, Edited by L. Roberts and

A. Weale, Belhaven Press, London, pp. 149-161.

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

Palmlund, I. (1992) Social Drama and Risk Evaluation, In: *Social Theories of Risk*, S. Krimsky and D. Golding, Westport, CT, Praeger Publishers, pp. 197-215.

Parker, D. (1981) *Computer Security Management*, Reston Publishing, Reston.

Parsons, T. (1960) Pattern variables revisited, *American Sociological Review*, 25, pp. 467- 483.

Pearce, J.A. and David, F. (1987) Corporate Mission Statements: The Bottom Line, *Academy of Management Executive*, 1(2), pp.109-116.

Perrow, C. (1986) *Complex organizations*, (3rd edition) New York: McGraw-Hill.

Powell, P. and Klein, J. (1996) Risk Management for Information Systems Development, *Journal of Information Technology*, 11, pp. 309-319.

Pritchard, R.D. (1995) *Productivity measurement and improvement: Organizational case studies*, New York: Praeger.

Reich, B.H. and Benbasat, I. (1990) An Empirical Investigation of Factors Influencing the Success of Customer-Oriented Strategic Budgeting. *Information Systems Research*, 1(3), pp. 325-347.

Rejda, G.E. (1998) *Principles of Risk Management and Insurance*, Addison-Wesley Educational Publishers Inc., Sixth Edition.

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, pp. 329-345.

Roethlisberger, F.J. (1977) *The Elusive Phenomena*, Harvard Business School, Division of Research, Boston.

Rousseau, D., Sitkin, S., Burt, R., Camerer, C. (1998) Not so Different All: A Cross-Discipline View of Trust, *Academy of Management Review*, 23(3), pp. 393-405.

Saltmarsh, T. and Browne, P. (1993) Data Processing- Risk Assessment, In: *Advances in Computer Security Management*, Vol.2, Wofsey, M. (eds), pp.93-116, John Wiley and Sons, Chichester.

Sandman, P. (1987) Risk Communication: Facing Public Outrage, *EPA Journal*, 13(9), pp. 21-22.

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

Schwandt, T.A. (2000) Three Epistemological Stances for Qualitative Inquiry: Interpretivism, Hermeneutics, and Social Constructionism, In: *Handbook of Qualitative Research*, N.Y.K. Denzin, and Y.S. Linclon, eds., Sage Publications, Thousand Oaks, CA.

Searle, J.R. (1969) *Speech Acts: An Essay in the Philosophy of Language*, Cambridge University Press, New York.

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.

Sheppard, B.H. and Sherman, D.M. (1998) The Grammars of Trust: A Model and General Implications, *The Academy of Management Review*, 23(2), pp. 422-437.

Singelis, T.M., Triandis, H.C., Bhawuk, D.S., and Gelfand, M. (1995) Horizontal and Vertical Dimensions of Individualism and Collectivism: A Theoretical and Measurement Refinement, *Cross-Cultural Research*, 29, pp. 240-275.

Siponen, M.T. (2000) A Conceptual Foundation for Organizational Information Security Awareness, *Information Management and Computer Security*, 8(1), pp.31-41.

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.

Slovic, P. (1990) The Legitimacy of Public Perceptions of Risk, *Journal of Pesticide Reform*, 10(1), pp. 13-15.

Smith, J. and Barclay, D. (1997) The Effects of Organizational Differences and Trust on the Effectiveness of Selling Partner Relationships, *Journal of Marketing*, 62(1), pp. 3-21.

Sorensen, J.B. (2002) The Strength of Corporate Culture and 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.

Strens, R. and Dobson, J. (1993) How Responsibility Modelling Leads to Security

Requirements, *Proceedings of the 16th National Computer Security Conference*, Baltimore, MD, pp.398-408.

Staw, B.M. (1981) The Escalation of Commitment to a Course of Action, *Academy of Management Review*, **6**(4), pp. 577-587.

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

Staw, B.M. and Ross, J. (1987) Understanding Escalation Situations: Antecedents, Prototypes, and Solutions. In: *Research in Organizational Behaviour*, Volume 9, B.M. Staw and L.L. Cummings (eds.) JAI Press, Greenwich, CT, pp. 39-78.

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.

Strens, R. and Dobson, J. (1993) How Responsibility Modelling Leads to Security Requirements. *Proceedings of the 16th National Computer Security Conference*, Baltimore, MD, pp. 398-408.

Tan, M. and Teo, T.S.H. (2000) Factors Influencing the Adoption of Internet Banking, *Journal of the Association for Information Systems*, **1**(5), July.

Ternullo, G. (1997) *Banking on the Internet: New Technologies*, New Opportunities and New Risks, Boston Regional Outlook, Second Quarter, (http://www.fdic.gov/index.html).

Triandis, H.C. (1995) *Individualsim and Collectivism*, Boulder, CO: Westview Press.

Trice, H.M. and Beyer, J.M. (1993) *The Cultures of Work Organizations*, Englewood Cliffs, NJ: Prentice Hall.

Tubbs, M.E., Boehne, D.M. and Dahl, J.G. (1993) Expectancy, Valence and

Motivational Force Functions in Goal Setting Research: An Empirical Test, *Journal of Applied Psychology*, 78, pp.361-373.

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

U.S. Department of Commerce (1999) *The Emerging Digital Economy II*, (http://www.ecommerce.gov/ede/).

Vlek, C. and Stallen, J. (1981) Judging Risks and Benefits in the Small and in the Large, *Organizational Behaviour and Decision Processes*, 28, pp. 235-271.

Von Solms, R. (1998) Information security management (1): why information security is so important, *Information Management and Computer Security*, 6(5), pp.224-225.

Walsham, G. (1993) *Interpreting Information Systems in Organizations*, John Wiley and Sons, Chichester, UK.

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

Webler, T., Rakel, H. and Ross, R.J.S. (1992) A Critical Theoretic Look at Technical Risk Analysis, *Industrial Crisis Quarterly*, 6(4), pp. 23-38.

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.

Weick, K.E. (1985) The Significance of Corporate Culture. In: *Organizational Cultures*, P.J. Frost, L.F. Moore, M.R. Louis, C.C. Lundberg, and J. Martin (eds.), pp. 381-389, Beverly Hills, CA: Sage.

Weill, P. and Olson, M.H. (1989) Managing Investments in IT: Mini Case Examples

and Implications, *MIS Quarterly*, **13**(1), pp. 3-17.

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.

Wildavsky, A. (1990) *Searching for Safety*, New Brunswick, NJ, Transaction Books.

Willcocks, L., and Margetts, H. (1994) Risk Assessment and Information Systems, *European Journal of Information Systems*, **3**(2), pp.127-139.

Williamson, O. (1993) Calculativeness, Trust and Economic Organization, *Journal of Law and Economics*, **36**(2), pp.453-502.

Woofford, J.C., Goodin, V.L., and Premack, S. (1992) Meta-analysis of the Antecedents of Personal Goal Level and of the Antecedents and Consequences of Goal Commitment, *Journal of Management*, **18**, pp. 595-615.

Wong, K. (1977) *Risk Analysis and Control*, National Computing Centre, Manchester.

Wright, P.M. (1989) Test the Mediating Role of Goals in the Incentive-Performance Relationship, *Journal of Applied Psychology*, **74**, pp. 699-705.

Wynne, B. (1992) Risk and Social Learning: Reification to Engagement, In: *Social Theories of Risk*, S. Krimsky and D. Golding, Westport, CT, Praeger Publications, pp. 123-151.

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