Information Systems Security and the Structuring of Organisations

Maria Karyda[1], Spyros Kokolakis[2] and Evangelos Kiountouzis[1]

[1]Athens University of Economics and Business, Athens, Greece, {mka,eak}@aueb.gr

[2]University of the Aegean, Karlovassi, Samos, Greece, sak@aegean.gr

Abstract

This study explores the consequences of the introduction of a security plan into organisations by means of a case study of a non-governmental organisation for the treatment of individuals with drug addiction. The paper mainly focuses on the implications of the application of a security plan to the social system in the organisation. The framework for analysis used for the case study is based on the fundamental tenets of A. Giddens' structuration theory. Structuration theory can be used as an analysis tool for studying the interplay between social structures and human agency and also provides the framework for taking into account aspects of organisational change. This study contributes to the stream of research on the implications of implementing security plans and policies in the organisational context, which is still in a very early stage.

1 Introduction

Within the past decade organisations have realized the need to protect their Information Systems (IS) and thus allocate significant resources to this endeavor. However, protecting an IS in the context of an organisation is far from a trivial task and needs to be addressed in a disciplined manner. In the IS security management agenda, a common practice is to design and apply an IS security plan, which address the organisational security needs and requirements.

An IS security plan includes a security policy, which comprises principles and guidelines for the protection of the IS, and a set of designated security controls. The security plan also prescribes specific protective measures and outlines a strategy and a program for implementing the plan. The aim of applying an IS security plan is to reduce the risk an IS faces, thus to transform an IS into a security-enhanced IS. Considering the axiom that there are no hundred percent secure systems, it is generally accepted that this transformation will not result in a zero-risk IS but in a lower-risk IS. This transformation entails significant changes affecting the components as well as the operation of the IS. In most cases, and especially when the IS supports significant organisational functions, many changes need to be made for the security plan to be applied. These changes need to be made not only to the IS, but also to its organisational environment. Technical issues have been systematically examined in the IS security literature, however organisational issues remain largely unexplored, despite the fact that many researchers have stressed their importance [Dhillon, 2001]. Previous work in this field has largely overlooked the impact of developing and implementing an IS security plan on organisations, and not any accounts have been given on the implications and changes that emerge within the organisational environment and are related with the application of the security plan.

This paper explores the implications from the application of an IS security plan to the organisational context, as well as the organisational changes related to it. We aim to reveal the way IS security plans and the organisational context are formulated as a result of their interaction. To do so we have studied the process of the application of an IS security plan to a non-governmental organisation for the treatment of individuals with problems of addiction. The case study presented describes the introduction of the IS security plan into this organisation, which we will call CTDI, and the changes that occurred during and after the implementation of this plan. The security plan was formulated on the basis of a generic security review that was proposed to CTDI by a group of external consultants in which the authors participated. This review was evaluated by working groups, which were formed within CTDI. The formulation process resulted to the full adoption of the security plan after a period of several months: all activities in the CTDI related to the IS conformed to the security policy and the selected security controls (technical, organisational and procedural) were implemented. This case is in contrast to the great body of IS security literature, where accounts of organisations not using their security policies, or unable to overcome major obstacles in the process of implementing security plans and policies are very frequent. We believe that by exploring the case of introducing the security plan to CTDI and its adoption, we can reach to some useful conclusions that may help IS security research and practice illuminate the cases of failures in security plans and policies' adoption.

The purpose of this paper is thus to explore the interplay between the organisational form and human agency in relation to information systems within CTDI and the process of securing these systems. More specifically, we aim to address the following questions: (a) how does the introduction of a security plan affect the organisational form and human agency, and (b) what are the implications, both intended and unintended, for the organisational structure, rules and norms from this introduction?

The theoretical framework we use in this paper for analyzing the case study and presenting our conclusions draws on structuration theory and is presented in section 2, following an overview of the issues on security plan and policies adoption that emerge from the IS security literature. Section 3 presents our methodological approach and provides background information on the case study. The analysis of the case based on the structuration framework is presented in section 4, and our overall conclusions and indications for future research are included in the last section.

2 Literature Review and Theoretical Framework

2.1 IS Security Planning

Information systems security management aims to minimize risks that information systems face in their operation. IS security management comprise a planning phase, which normally follows an evaluation of the level of risk for the IS, an implementation phase during which security plans are put to action and are tested under real conditions and an assessment or audit phase that can also serve as the evaluation phase for the future security planning [Dhillon 1997, Bjőrck 2001]. A basic instrument IS security management applies is the formulation and use of a security plan, which typically includes a security policy and a list of actions and security controls to be implemented.

IS security policies contain the security objectives and the required methods and means to achieve them, thus their development is a task that is critical for the ability of the organisation to protect its information infrastructure. An IS security policy combines technical as well as organisational and processual measures that address security requirements for the protection of information systems (Peltier, 1999). The application of a security policy is one of the most common and major means used by organisations for the protection of IS. Their application is considered as fundamental and indispensable security management practice [Dhillon 1997, Hőne and Eloff 2002]. However, it is very common that the use of security policies fails to accomplish the purposes that were originally designed to achieve [Wood, 2000]. IS security research is also trying to address the issue of the effective adoption of IS security policies by exploring the conditions and requirements for 'policy enforcement in the workplace' [David, 2002] or placing emphasis on encouraging personal accountability for achieving policy enforcement [Wylder, 2003]. Other researchers investigate the formulation of security policies through the application of a participational approach, such as an adaptation of the ETHICS socio-technical methodology [Gaunt, 1998], or by applying the principles of contextualist research [Karyda et al 2003]. This paper explores a dimension of the formulation and adoption of security polices that has been neglected by IS security research by now: the impact on the social structuring of the organisations that apply security policies.

2.2 Structuration Theory overview

Structuration theory is a sociological model proposed by Giddens (1979, 1984) in an attempt to resolve the debate between social theories that underlined the role of human agency and those emphasizing the role of the structure of social systems. Giddens put forth a unifying view over the agency/structure debate, by discarding the discretion between agency and structure and claiming that these, instead, do not exist independent from one another, but they rather form different sides of the same phenomenon. This idea, called the 'duality of structure' is central to structuration theory and is based on the claim that structure exists "*...only as memory traces, the organic basis of human knowledgeability, and is instantiated in action*"[Giddens, 1984:377]. In this way, human interaction draws on social structures and at the same time produce, reproduce or alter, these structures.

Social systems are not structures, but present some structural properties, which describe similar social practices over time and space [Giddens, 1984]. Structure can therefore be described using these properties, namely *signification*, *domination*, and *legitimation*. Structures of signification refer to the practices by which actors derive interpretive schemes that enable their communication. Structures of domination describe the power of actors to act, drawing on facilities such as the ability to allocate material and human resources. Finally, individuals sanction their actions by referring to norms and rules, thus maintaining or transforming social structures of legitimation.

Structural properties are linked to social interaction by the concept of *modality*. The three primary modalities, namely *interpretive schemes, resources* and *norms* are key concepts for understanding the interaction between human action and social structure. Human interaction draws on interpretive schemes for communication of meaning, whereas actions are carried out on the basis of individual power that is dependent domination. Human actions are constrained by norms, which are based on individual notions of the allocation of resources to human agents, forming structures of what is sanctioned and in their turn result in legitimizing or discarding these norms. In this way social structures are produced, reproduced or altered by human action over time, and at the same time human action is enabled or constrained by these social structures. Thus, structuration is the process whereby the duality of structure evolves and is reproduced over time. The separation of structure and interaction into these dimensions, however, is merely an analytical device; structuration theory considers them as inextricably linked. Figure 1 illustrates the dimensions of the duality of structure as described in Giddens (1984).

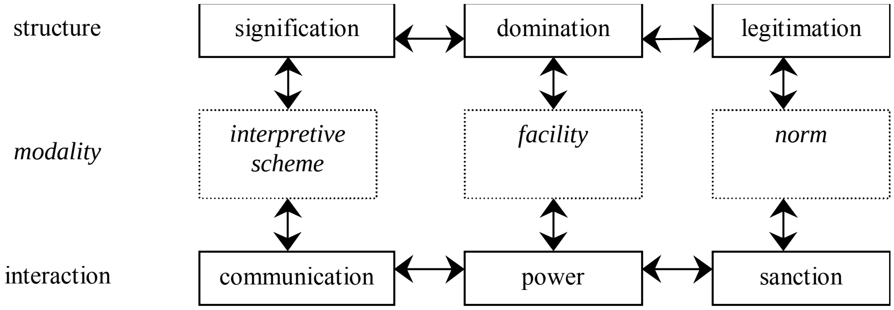

Figure 1 Dimensions of the duality of structure (Giddens, 1984)

Another basic topic in structuration theory is the element of time, since the ‘structural properties of social systems exist only as forms of social conduct are reproduced chronically across time and space [Giddens, 1984].

2.3 Structuration Theory in the Information Systems field

Structuration theory is widely used in the information systems field, mainly as a tool for understanding and interpreting organisational change related to the introduction or use of information technology in organisations [Rose 1999, Rose and Scheepers 2001]. Researchers in the IS field have applied structuration theory in a variety of ways, and drawing on different methodological assumptions, ranging from interpretivist to positivist assumptions [Pozzebon and Pinsonneault 2001].

Barley (1986) applies structuration theory in studying the introduction of computer tomography scanners into two different hospitals in USA. By applying structuration theory in studying these cases Barley reached the conclusion that the introduction of technology interfered with the routines at the level of social action, thus leading to a change in structure that differed in the two cases. Walsham (1993) uses structuration theory as a supporting theoretical device to his contextualist approach; structuration theory provides a means for analysing the linkage between the context and the processes in three separate cases concerning the introduction, development and implementation of computer-based information systems in three different organisations. Orlikowski and Robey (1991) apply the basic concepts of structuration theory for understanding the relationship between information technology and organisations. Orlikowski (1992) further explores the concept of the duality of structure in relation to technology, and proposes a ‘structurational model of technology’, where technology is integrated to structuration theory as a determinant factor that influences the interaction between agents and institutional structure. Lyytinen and Ngwenyama (1992) also consider Computer Supported Co-operative Work applications to be structures. However, Walsham (1993) criticizes this approach, emphasizing on the differences between social structures, as used in structuration theory, and technology that constitutes physical structure. Instead, he proposes that technology be placed at the modality level; in this perspective technology mediates agent interaction and thus social structure.

Adaptive Structuration Theory (AST) is another approach to extend structuration theory to address the role of technology in the shaping of social processes [DeSanctis and Poole, 1994]. AST has been largely employed by researchers in the IS field in various domains, but especially in studying group decision support systems and computer mediated communication. IS research papers that draw their theoretical basis on AST usually adopt a positivist epistemology and quantitative research methods such as statistical analysis and hypothesis testing. Overall, AST research has been criticized [Jones and Karsten, 2003] as pursuing a different research agenda from the objectives of structuration theory.

Structuration theory is considered as a significant aid for interpreting various aspects of the development and use of information systems and is therefore widely used, despite the difficulties of applying it to empirical studies, due to its abstract and general form. Although structuration theory has been having a great impact on organisational and IS studies, it has still not been employed in the IS security field. A reason for this could be that in the major body of the IS security literature a positivist epistemology is followed and researchers favor the application of quantitative research methods. The focus of most of the research in IS security is concerned with the technological part of it, leaving the social part of IS security unexplored.

Despite the fact that most of the research in IS security falls within the functionalist paradigm, however, there has been recently a trend towards exploring alternative research methods and adopting a different epistemological stance. Hence, researchers pursuing to explore the social and informal aspects of IS security are turning to sociological and organisational theoretical models and frameworks. In this paper we use structuration theory as an analytical tool [Jones, 1997] for exploring the interplay between the introduction of a security plan and its adoption in the case of CTDI.

2.4 Theoretical Framework

The framework for analysis of this paper draws on structuration theory, using its key elements as a framework for analyzing the case of the introduction and adoption of a security plan into CTDI. The basic concepts used in our analysis are listed in Table 1.

Key Concepts	Description
Structural dimensions	• Structures of signification refer to rules that regulate the formulation of meaning systems. By drawing on interpretive schemes actors reproduce signification structures. • Structures of domination are ‘asymmetries of resources’ upon which individuals draw their power. Facilities reflect the capabilities of actors to act intentionally. • Legitimation structures constitute a set of shared values and ideals on what is important and the way things should be done. They refer to the norms and rules based on which the actors sanction social interaction. Norms include rights and duties expected of actors in their social conduct.
Social interaction	• Human agency is constrained and at the same time enabled by structural properties. • Practices (routines) develop when social practice becomes reasonably stable over time and space.

Table 1 Framework for analysis of the case study

3 Research Methodology and Case Study Background

3.1 Research approach

Our research approach in exploring the case of the security plan introduction into the CTDI adopts an interpretive perspective, as opposed to the traditional ‘positivist’ approach that is most frequently used in the domain of information systems security. IS literature is populated with a significant number of interpretive case studies which are mostly employed for exploring, classifying and hypothesizing. Case studies “*...examine a phenomenon in its* *natural setting, employing multiple methods of data collection to gather information from one or a few entities.*"[Benbasat et al.,1987]. Case studies in research have also been considered as a useful and appropriate tool for answering 'how' or 'why' questions [Yin, 1994] both by a positivist and an interpretive stance [Walsham, 1995]. Walsham (1993:14) argues that the most appropriate method for conducting empirical research within the interpretive tradition is the in-depth case study. The reasons for choosing an interpretive stance towards the issue of formulating a security policy were that, in the first place, the topic of our research involved a great variety of stakeholders with different interests and, in the second place, we wanted to explore the dynamics of the development and use of a security policy, including the interaction between the various stakeholders and the evolution of organisational norms and practices over the time. Moreover, since the 'value of a case study is primary revelatory' [Yin, 1994] we aim to illuminate the mechanisms and processes related to the adoption of security policies.

With regard to data collection, multiple sources have been used: The primary sources of the data were semi-structured interviews and secondary sources have been internal reports, documents, archives and other printed material concerning the information system and the structuring of the organisation, relevant resources on security management and security policy formulation and other public available material. Overall more than 30 in-depth interviews were conducted with various groups within the CTDI.

3.2 Case Study Overview

This section describes, in the form of a case study, the authors' consultation into a non-governmental organisation for the treatment of addicted individuals, which we will call CTDI. The consulting team, in which the authors participated, was assigned the project of evaluating the risk of the organisation's information systems and proposing the designated security policy based on the findings of the risk assessment analysis. CTDI accepted the proposed security plan and launched an internal programme for its adoption. During the following two years working groups had been formed in CTDI with the objective to evaluate and formulated the security plan so as to be put into action by CTDI's members. The goal of these groups was to integrate the procedures and controls that were included in the proposed security plan and supervise and monitor the implementation of the security controls. By the time the authors returned, after a couple of years, unofficially to CTDI, the security plan was almost at its entity, adopted by the organisation and the designated security controls were followed by its members.

3.3 The Case of CTDI

The Center for the Treatment of Dependent Individuals (CTDI) is a non-governmental organisation established in 1987 that comprises more than 40 independent units concerned with prevention and treatment of drug abuse. For the purpose of its operation, CTDI keeps and processes, both manually and electronically, data mainly concerning drug addiction. CTDI is bound by the national Data Protection Legislation to provide adequate protection for this information, and to have a security policy in place, for the regulation of the use and access to this information. So, CTDI invited an external group of security experts to prepare an IS security plan and a security policy. The security plan included a generic security policy and a set of security controls that should be applied for the protection of all informational assets against the threats and vulnerabilities that were recorded by the risk assessment analysis. The plan also included suggestions for the organisational structure that would be required to carry out the proposed security management processes and support the application of security controls. For the risk assessment of CTDI's information systems the CCTA Risk

Analysis and Management Method (CRAMM) was employed. CRAMM does not provide for the analysis of social and organisational factors and the working team could only rest on their experience to handle such issues.

CTDI is organised in the form of a matrix, with working groups that are formed by the participation of members from the independent units that run the different treatment "Programmes" CTDI has for individuals with drug addiction. These groups refer to the Board of Directors, which comprises all the directors of the various Programmes. Since the beginning of its operation CTDI has also had a Committee for establishing a code of practice and for managing ethical and other issues, which arise in the everyday activities of the members of the CTDI and their interaction with external people and bodies. A major difficulty CTDI faced before establishing the security policy was requests for data concerning personal information of individuals with drug addiction who had participated in CTDI's Programmes. These requests often originated from public or governmental bodies and they came in contrast with the code of ethics and practice CTDI had established for its members. Resisting the pressure from those requests was a difficult task for CTDI, due to the fact that although its management is entirely independent, and the Board of Directors that directs it is elected by its members, most of its funding comes from the Ministry of Health.

When the generic Security Plan was delivered to the organisation, the Board of Directors declared their commitment to implement it. For implementing the security plan CTDI formed working groups, on the basis of its matrix organisation. These groups evaluated the proposed plan and 'tailored' it to the context of CTDI. In this way new work practices were established and the code of ethics and practice was adapted. It should be noted, however, that the previously existing code was in the same direction with the security policy, so no major changes were required. Besides the new processes that were designed and the technical controls that were implemented, new norms and rules were also considered for the application of the security policy. The Board of Directors accepted and supported the recommendations made by the working groups and also created new organisational roles for the management of security, as was proposed in the generic security plan. When researchers from the group of external consultants returned to explore how the implementation of the security plan had progressed, the security policy was at the early stages of its adoption and new work practices had already began to establish.

4 Structurational Analysis of the Case Study

This section presents the findings of the structurational analysis of the case of the introduction of a security plan in CTDI. The analysis uses key concepts in structuration theory, as described in section 2, as sensitizing and analyzing devices to explore the processes unfolding in relation with the formulation and application of CTDI's security policy. Table 2 includes our research findings in the CTDI presented according to the dimensions of the duality of structure and Table 3 presents our observations concerning the formation of social interaction in CTDI during and after the process of the implementation of the security plan.

Our major conclusions from this analysis is that the members of CTDI were able to handle both external and internal requests regarding the use of personal information of individuals with problems of addiction in a coherent manner and could base their actions on the directions of the formal security policy which was adopted. Moreover, the security policy strengthened the concept of following the internal code of ethics, while new work practices with regard to the handling of sensitive personal information were developed. Although a formal code of practice preexisted, the introduction of the security policy promoted and helped create a security culture and broader security awareness.

Key concepts	**Description**		
Structure	*signification* • Information resources are attributed security characteristics (namely integrity, confidentiality and availability) and thus need be treated according to the security policy. • Work practices are reformulated (where needed) on the basis of the security policy and the controls that were implemented.	*domination* • New roles were created (Security Officer and Security Managers for each Programme). • Access to information (especially to sensitive data concerning drug-addicted individuals participating in CTDI's Programmes) should follow the need-to-know principle.	*legitimation* • The Board of Directors of CTDI committed to the security plan and supported the adoption of the security policy. • The security policy encompasses all legal and regulatory requirements (e.g. the European Directives and the national legislation on personal data protection).
Modality	*interpretive scheme* • The security policy document and all other related documents are available to all CTDI members for reference. • Internal seminars and workshops related to the new security policy and its adoption help create a 'security culture'. • Information handling issues need to be reconsidered in the context of the new security policy	*facility* • CTDI members with security responsibilities gained knowledge on IS security and protection issues. • The Board of Directors allocates human resources and funding for the protection of IS.	*norm* • The security policy is formulated in accordance with the previously existing code of ethics for the members of CTDI. • Information management practices adhere to the security policy. • Security related liability and responsibility issues emerge
Interaction	*communication* • Security awareness and a common language and understanding on security issues is developed due to the participation of CTDI members in working groups for the formulation of the security policy.	*power* • IT personnel broadened their responsibilities and were able to back up their claims and financial requirements with relation to the IS and its protection.	*sanction* • The members of CTDI are keen to adopt the security policy, due to their participation in working groups for its formulation. • Denial to provide personal information concerning addicted individuals to external organisations can now be based on the security policy.

Table 2 Dimensions of Structure in the case of CTDI

Key Concepts	Description
Social interaction	• All CTDI members follow the formal rules and procedures that are included in the Security Policy. • Actions and the conduct of CTDI members towards non-members of the organisation conform to the Security Policy. • The members of CTDI are able to perform some activities with regard to other organisations by using the newly established procedures that were introduced through the Security Plan.

Table 3 Linking ST elements and case study findings

5 Conclusions

The conclusions we have drawn from the analysis of the CTDI case is that the introduction of the security plan affected the structuring of this organisation, resulting in different norms and rules, which provide the basis for the shaping of social interaction. Moreover, conclusions from our analysis have strengthened the position that elements of the organisational context, and especially social interaction, play an important role for the application of a security plan. We believe that there is need to further explore implications of the application of IS security plans from an organisational perspective, besides the technical perspective that is dominant in the relevant literature.

We also think that structuration theory provides a powerful framework within which we can achieve a better understanding of how the introduction and adoption of a security policy has interacted with the organisation. In this paper, we have shown how the duality of structure principle of structuration theory may be used to explore the cyclic process, whereby IS security policy formulation and implementation shape attitudes and behaviour and, hence social structures, which, in turn, shape attitudes and behaviour in various ways. This framework helped us derive useful observations and conclusions that we think IS security practitioners and researchers should take into account when involved or studying the process of IS security plans and policies implementation and adoption. Under this perspective, we think that structuration theory could by further used for investigating social and organisational aspects of IS security management, as well for exploring the relationship between IS security management and organisational change.

References

Barley S. (1986), Technology as an occasion for structuring: evidence from observation of CT scanners and the social order of radiology departments, *Administrative Science Quarterly,* 31 (1), 78-108

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

Bjőrck F. (2001), *Security Scandinavian Style. Interpreting the Practice of Managing Information Systems in Organisations*. PhD Thesis, Stockholm University and Royal Institute of Technology,

David J. (2002), Policy enforcement in the workplace, *Computers and Security*, 21(6), 506-513

DeSanctis, G. and Poole M.S (1994), Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory, *Organization Science*, 5(2), 121 - 147

Dhillon G. (2001), Challenges in Managing Information Security in the New Millennium, in Dhillon G. (ed.) *Information Security Management: Global Challenges in the New Millennium*, Idea Group Publishing, 1-8

Dhillon G. (1997), *Managing Information System Security*, Macmillan Press Ltd

Gaunt N. (1998), Installing an appropriate information security policy, *International Journal of Medical Informatics,* 49, 131-134

Giddens A. (1984), *The Constitution of Society*, Cambridge, Polity Press

Giddens, A. (1979), *Central Problems in Social Theory*, Macmillan Press

Hőne K. and Eloff J. (2002), Information security policy - what do international information security standards say?, *Computers and Security*, Volume 21(5), 402-409

Jones M. and Karsten H. (2003), Review: Structuration Theory and Information Systems Research, Research Papers in Management Studies, Judge Institute of Management, University of Cambridge, available online at http://www.jims.acm.ac.uk/ accessed 10.01.2004

Jones, M. (1997), Structuration Theory, in *Rethinking Management Information Systems*, Currie, W. and Galliers B. (eds.), Oxford University Press, 103-135

Karyda M., Kokolakis S. and Kiountouzis E. (2003), Content, Context, Process Analysis of IS Security Policy Formation, in the *Proceedings of the 18th IFIP International Conference on Information Security*, Kluwer Academic Publishers

Lyytinen K. and Ngwenyama O. (1992), What does computer support for cooperative work mean? A structurational analysis of computer supported cooperative work, *Accounting, Management and Information Technologies,* 2 (1), 19-37

Orlikowski W. (1992), The duality of technology: rethinking the concept of technology in organisations, *Organisation Science*, 3 (3), 398-427

Orlikowski, W.J. and D. Robey (1991), Information Technology and the Structuring of Organisations, *Information Systems Research*, 2(2) 143-169

Peltier T. (1999), *Information security policies and procedures: a practitioner's reference*, CRC Press

Pozzebon, M. and Pinsonneault, A. (2001), Structuration Theory in the IS Field: An Assessment of Research Strategies*, Proceeding of the 9th European Conference on Information Systems* (ECIS '01), Bled, Slovenia, June 27-29

Rose, J. (1999), Structurational Theory of IS – Theory Development and Case Study Illustrations, *Proceedings of the European Conference on Information Systems* (ECIS '99), Copenhagen, Denmark, June 23-25

Rose, J. and Scheepers, R. (2001), Structuration Theory and Information System Development – Frameworks for Practice, *Proceedings of the 9th European Conference on Information Systems* (ECIS '01), Bled, Slovenia, June 27-29

Walsham G. (1995), Interpretive case studies in IS research: nature and method, *European Journal of Information Systems*, 4, 74-81

Walsham, G. (1993), *Interpreting Information Systems in Organisations*, J. Wiley & Sons Ltd., England

Wood C. (2000), An Unappreciated Reason Why Security Policies Fail, *Computer Fraud and Security*, 10, 13-14

Wylder J. (2003), Improving Security from the Ground Up, *Information Systems Security*, January/February 2003, 29-38

Yin R. (1994), *Case Study Research: Design and Methods*, Sage Publications