Gurpreet Dhillon

MANAGING INFORMATION SYSTEM SECURITY

Managing information system security

Information Systems Series
Series Editor: Professor I.O. Angell

Computer Security Within Organizations
Adrian R. Warman

Developing Information Systems – Concepts, Issues and Practice
Chrisanthi Avgerou and Tony Cornford

Effective Systems Design and Requirements Analysis
The ETHICS Approach
Enid Mumford

General Systems Theory – An Introduction
Lars Skyttner

Information in Action – Soft Systems Methodology
Lynda Davies and Paul Ledington

Management, Information and Power
A narrative of the involved manager
Lucas D. Introna

Managing Information System Security
Gurpreet Dhillon

Ourselves and Computers – Difference in Minds and Machines
Aart Bijl

Project Research in Information Systems – A Student's Guide
Tony Cornford and Steve Smithson

Systems Design – Ethical Tools for Ethical Change
Enid Mumford

Understanding Information – An Introduction
Jonathan Liebenau and James Backhouse

Managing Information System Security

Gurpreet Dhillon
Cranfield School of Management
Cranfield University, Bedford

palgrave
macmillan

First published 1997 by
MACMILLAN PRESS LTD
Houndmills, Basingstoke, Hampshire RG21 6XS
and London
Companies and representatives
throughout the world

ISBN 978-0-333-69260-8 ISBN 978-1-349-14454-9 (eBook)
DOI 10.1007/978-1-349-14454-9

A catalogue record for this book is available
from the British Library

This book is printed on paper suitable for recycling and made from fully managed and sustained forest sources. Logging, pulping and manufacturing processes are expected to conform to the environmental regulations of the country of origin.

Contents

Preface

What impact does an organisation's environment have on the security of information systems? How does organisational culture influence information system security? What is the implication of different expectations and obligations of management roles on the security of information systems? How do the meanings of actions and patterns of behaviour affect information system security? What is the relationship between the logical specification of systems and the management of security? This book is an attempt to answer these questions from the perspective of a business practitioner, but with conceptual and theoretical rigour.

Indeed the management of adverse events within organisations has become a pressing issue as the perceptions of risk continue to heighten. However, the basic need for developing secure information systems has remained unfulfilled. This is because the focus has been on the means of delivery of information, i.e. the technology, rather than on the various contextual factors related to information processing.

The overall aim of this book is to increase understanding of the issues and concerns in managing information system security. The study is conducted by reviewing the analysis, design and management of computer based information systems in two large organisations – a British National Health Service Hospital Trust and a Local Government Council. The management of information system security is evaluated in terms of the business environment, organisational culture, expectations and obligations of different roles, meanings of different actions and the related patterns of behaviour. Analysis of the cases shows that an inappropriate analysis, design and management of computer based information systems affects the integrity and wholeness of an organisation. As a result, the probability of occurrence of adverse events increases. In such an environment there is a strong likelihood that security measures may either be ignored or are inappropriate to the real needs of an organisation. Therefore, what is needed is coherence between the computer based information systems and the business environment in which they are embedded. In conclusion, this book shows that to resolve the problem of managing information system security, we need to understand the deep-seated pragmatic aspects of an organisation. Solutions to the problem of security can be provided by interpreting the behavioural patterns of the people involved.

This book not only presents a new definition of information system security but also advocates a particular stance in understanding and managing information system security. In developing such a stance a number of approaches have been reviewed and examined critically; I suspect that my own preferences will be in evidence. Readers are encouraged to interpret the various standpoints in this book *vis-à-vis* their own experience and practical situations. Two main case studies have been used in order to conduct the argument of this book. The names of the organisations and the roles of individuals have been changed to maintain confidentiality. The interpretations in no way represent the views of the case study organisations.

On a personal note, the book would not have been possible without the support of my family, which has been my inspiration, my goal and my light. I acknowledge them most sincerely. The ideas presented in this book are a product of extensive debates and discussions with a number of individuals. In particular I would like to register my gratitude to Dr James Backhouse (LSE), Professor Ian Angell (LSE) and Professor Bob Galliers (Warwick) for their constructive criticisms.

1 Orientation

1.1 Introduction

This book is about the management of information system security. Information system security is viewed in terms of minimising risks arising because of inconsistent and incoherent behaviour with respect to the information handling activities of organisations. Such inconsistencies in behaviour could lead to the occurrence of adverse events. These could be as privately experienced as a superior–subordinate conflict in an organisation, or could be as public as the technical failure of an information system. These set-backs could have been produced by sheer carelessness or after careful premeditation. Their consequences could be as transitory as monetary loss or as terrible as a complete disruption of business and loss of life. Whatever the nature of the inconsistencies, protection demands an understanding of the underlying causes and the related patterns of behaviour. How these behavioural patterns relate to adverse consequences within organisations is the theme of the work presented in this book.

The overall aim of the book is to increase an understanding of the issues and concerns in the management of information system security. In pursuing this aim, the book reviews the analysis, design and management of computer based information systems in two large organisations – a British National Health Service Hospital Trust and a Local Government Council. It is believed that the problems arising in respect of the deep-seated pragmatic aspects of the two case study organisations have consequences for the management of information system security. This claim is validated in the chapters that follow.

The rest of this chapter describes the nature and orientation of work presented in the chapters that follow. Section 1.2 classifies the various adverse events. Section 1.3 presents some definitions that provide a conceptual territory for the research presented in this book. Section 1.4 sketches the chapter outline for the rest of the book.

1.2 Classification of negative events

The US Office of Technology Assessment (OTA 1994) report classifies various adverse events into six categories. First are the events caused by *human error*. A study on information systems in organisations, conducted by the United Nations Advisory Committee for the Co-ordination of Information Systems (ACCIS), found human error to be the cause of 65% of total security losses (ACCIS 1992).

Thus over one-half of the total financial and productivity loss for example is a result of "non" intentional acts. The UK Department of Social Security offers a classical example where errors in the assessment of income support due to the claimants resulted in overpayments to the tune of £540 million and underpayments of £76 million (Dynes 1994). The majority of problems occur because of improper installation and mismanagement of hardware or software, updating wrong files, entering incorrect data, inadequate internal controls and because of inaccurate transaction processing mechanisms.

Second are the adverse events caused by *analysis and design faults*. Ad hoc systems analysis and design can lead to increased vulnerability and threats not only to the information technology systems but also to the organisation as a whole. There are numerous examples of where the use of information technology has had disastrous consequences. In the UK the case of Wessex Regional Health Authority's £43 million information system plan fiasco has often been cited. The system was intended to link together every hospital, general practitioner and district nurse in the authority. The project was a failure and was subsequently abandoned. Though the reasons attributed to the failure were over-complexity and imposition of a centralised structure (see Ker 1994; Watkins 1993; Miles 1993; Computing 1992), the interplay between various factors made the organisation extremely vulnerable which led to significant losses from insider fraud. As Angell and Smithson (1991) point out, this is because the consequences of untried systems are not assessed adequately, thus challenging the entirety of an enterprise. Such problems can invariably be linked to systems analysis and design faults.

Third are the information system security problems that arise because of *violations of safeguards by trusted personnel* who engage in forbidden and unofficial activities. It has been reported that most violations of information system safeguards have been carried out by employees of the organisation (an astonishing 61%). The actual figure is certainly higher since only 9% of the cases have been positively linked with outsiders (Strain 1991). Figures coming from the US are even more startling. Nearly 81% of computer crime is committed by current employees (Brown 1991). These insiders may be dishonest or disgruntled employees who would copy, steal, or sabotage information, yet their actions may remain undetected. In 1993 a fraud came to light against the UK National Heritage Department which had resulted in payments to the tune of £175,000 to fictitious organisations. This was a typical case where the organisation had weak internal management controls that gave an individual the opportunity to subvert the financial system (Audit Commission 1994).

Fourth are negative events arising from *environmental damage*. Typical examples are floods, earthquakes, fires, power failures and bomb attacks. These can destroy not only the main computing facilities but also their backup systems. In recent years the City of London has experienced widespread threats and bomb attacks by the IRA. These have caused extensive damage and loss of service.

Fifth are information security problems resulting from acts by *system intruders*. Although only a small percentage of negative events have been caused by outsiders, it is a growing problem. These people, described as "Hackers" or "Crackers" violate system access controls. The main motivation for such people ranges from monetary gain, and access to corporate and industrial secrets, to the mere challenge of breaking into the system.

Sixth are the negative events occurring because of *malicious software, viruses and worms*. Viruses, worms, Trojan horse, logic bombs and other malicious software can enter computer systems in a variety of ways. Borrowed diskettes, pre-packaged software, and human negligence can all lead to successful system intrusion.

The extent to which organisations face security hazards, as classified above, can be gauged from the findings of the 1994 UK Audit Commission survey. It revealed that in the previous three years the total value of cases reported went up by 183%. The average cost for a security breach resulting in a fraud has been estimated at £28,170 per incident, a 38% increase in the last three years. Astonishingly 60% of the organisations surveyed had no security awareness training. The problems of information system security inevitably cause many organisations to suffer severe losses of markets, undergo restructuring, merge, or even to cease operations.

1.3 Definitions

Four families of definitions are required to set out the conceptual territory of this book. The argument in the subsequent chapters is implicitly rooted in these definitions.

Organisation. We begin with the premise that there is no single framework encompassing all domains of knowledge which helps in the study of organisations. In recent years contributions to the study of organisations have come from different domains. Natural science, mathematics and engineering viewpoints have been heavily criticised because they lead to inconclusive and inapplicable results (see for example Galliers and Land 1987; Jones and Walsham 1992). This has led researchers to consider, for example, ideas afforded by contingency theory, resource dependency theory, and more recently, structuration theory. Others have used concepts drawn from semiotics, the theory of signs, to understand administrative and business systems and the use of information in the society at large (e.g. Kitiyadisai 1991; Backhouse 1991; Liebenau and Backhouse 1990; Stamper 1973).

The emergent belief of most studies is to view organisations as evolving social forms of sense making. Consequently, they allow different groups to relate to each other and to the environment. Walsham (1993) views this to be a dynamic process of action/context interweaving, which is fundamental to the understanding of the process of organisational change. Liebenau and Backhouse

(1990) view organisational environments as constituted of the informal, formal and technical parts which are in a state of continuous interaction. Many authors have attempted to explain the nature of organisations on the basis of a similar categorisation (e.g. Galliers 1993; Land 1992; Backhouse *et al.* 1991).

Traditionally, organisations have been viewed as formal systems characterised by bureaucracy, where concern for rule and form replaces that of meaning and intention. These formal systems were essentially concerned with inter-organisational (between the organisation and its customers, suppliers, financial institutions, etc.) and intra-organisational (between different departments) information. In present times many computer based systems have been used to automate the administrative tasks of the formal systems.

An analysis of an organisation solely on this basis ignores the sub-culture where meanings are established, intentions understood, beliefs, commitments, responsibilities, are made, altered and discharged. This is essentially the informal component. With the establishment of an organisation, a system of fairly cohesive groups with overlapping memberships is created. These social groupings of the informal system have a significant bearing on the well-being of an organisation. The groups and even the individuals may have significant power and may be in a position to influence other informal groups or even the formal structures.

Information systems. Information systems have indeed come of age and are seen as the very core of business. Therefore it is important to understand the very notion of an information system. An information system is not restricted to the physical artifacts or the use of technology in organisations, but is concerned with the repertoires of behaviour of an organisation (Liebenau and Backhouse 1990). This conception of an information system is founded on the understanding that the wealth of a business is largely dependent on its ability to organise. This ability entails working with information and therefore handling it effectively. Information handling is a purposeful activity which is sustained over a period of time (Avgerou and Cornford 1993). Furthermore, business is carried out not by 'doing things' but by talking and writing (i.e. communication). As the activities of a company grow, informal means of communication need to be supplemented by more formal systems. The formal systems help in preserving the "uniformity of action and standardisation of meaning" (Stamper 1973). The complex interplay of the formal and the informal systems in an organisation gives rise to the management systems that are in place. The advances in new technology and the emergent organisational forms introduce new capabilities and 'connectivity' for information processing (Trubow 1993). It becomes difficult to ascertain clear lines of authority and decision making, changes in accountability and responsibility and the nature of the planning processes (Rockart and Short 1991). Hence information systems and organisations have become indistinguishable from each other. This is indeed the essential character of organisations and is the central concept in understanding the nature of information systems (see for example, Land 1992; Liebenau and Backhouse 1990; Klein and Hirschheim 1987; Stamper 1973).

Computer based information systems. The formal and informal systems are two different kinds of information systems within an organisation. There is severe tension between them. The formal system is rule based and provides uniformity across time and throughout the organisation. Often, because of the insensitivity of the formal system to the local conditions, it tends to impose inappropriate rules and procedures. These are generally resented and the overall operations of the system may be distorted. Problems may be further compounded when computers are used to implement formal systems. The boundary between the formal and informal is the one which is to be determined by decision makers after assessing those factors which can be handled routinely. Some of the operations could be computerised, "but there will also be a number of factors which, although formalisable, are best left to being handled informally" (Liebenau and Backhouse 1990). Computer based information systems therefore automate a small part of the formal system. The formal system as such has no existence except when it is deliberately created alongside the informal system.

Information system security. It emerges that, from the above three explanations, information system security concerns not just the security of the technical edifice but also that of the formal and informal systems within an organisation. Hence the management of information system security goes beyond the relatively focused concerns for the integrity of data held in a data management system (the technical system, i.e. computer based information system). Rather, it connotes the maintaining of a set of values. We speak of a person of integrity where that person is incorruptible, where they are able to retain the completeness of the system of values which they aspire to embody. In this sense avoiding unauthorised modification of data in a computer based system is only part of the information system security concern. Equally important, if not more so, is the consistency with which decisions are taken, and the concordance between these decisions and the overall objectives of the organisation. Here we take into account the consideration given by the members of the organisation to the spirit behind the letter of regulations in the performance of routine tasks. In this sense information system security also relates to the consistency with which members interpret data and apply that interpretation to inform their decision making. Hence where there is a discordance between, on the one hand the formally specified systems of authority, of information use, and on the other hand those that exist informally, in practice, then the integrity and security of the whole structure is threatened.

In the light of the above definitions, the following interpretations can be made:

- Since our ability to organise is related to our competence to handle information, it can be argued that it is information that holds organisations together and drives them along. Therefore organisations can be viewed as communication systems (Backhouse and Dhillon 1995b; Dietz 1992; McCall and Cousins 1990; Liebenau and Backhouse 1990), and any disruption in the communication process leads to security and integrity problems in an organisation (Backhouse and Dhillon 1996). Hence the meanings of actions and behavioural patterns have implications for information system security.

- an adverse event occurs because of inconsistencies with respect to the expectations and obligations of different roles (Strens and Dobson 1993). This provides the occupier of a role with an opportunity to commit an offence (Audit Commission 1994).
- occurrence of an adverse event is grounded in the culture of an organisation and the normative structures in place (Dhillon and Backhouse 1994).

These interpretations are articulated into a framework for managing information system security in chapter 3. The framework, based on concepts rooted in semiotics, is then used to tease out information system security issues within two organisations.

1.4 Organisation of the book

This section sketches out the organisation of the book and summarises the content of the chapters that follow. It is illustrated in figure 1.1.

Chapters 1, 2 and 3 lay the theoretical and conceptual foundation of this book. After an orientation in chapter 1, chapter 2 reviews the context of information system security. It evaluates research in the areas of information systems and security. The implicit argument is that while research in information systems has begun to consider the social aspects during the analysis and design processes, researchers in the security domain are still caught in an undesirable orthodoxy. They have been unable to shrug off their 'computer legacy' and are largely *functionalist* in their approaches.

Chapter 3 sketches out a framework for interpreting information system security. It identifies the sociological and philosophical orientation of this book and adopts a conceptual framework that helps in analysing security issues within an organisation. A particular mode of inquiry, that of considering the implications of contextual issues for organisational actions and meaning structures, is advocated. Such an approach is rooted in semiotics.

Application of the framework for managing information system security is described in chapters 4 and 5. Chapter 4 presents detailed findings from the British NHS Hospital Trust case. The main focus is on interpreting the security implications related to the introduction of an integrated information system.

Chapter 5 presents detailed findings from the British Local Government case. The focal concern is with the introduction of federal information technology infrastructures within the organisation. It analyses the implications for the security of the Local Government Council.

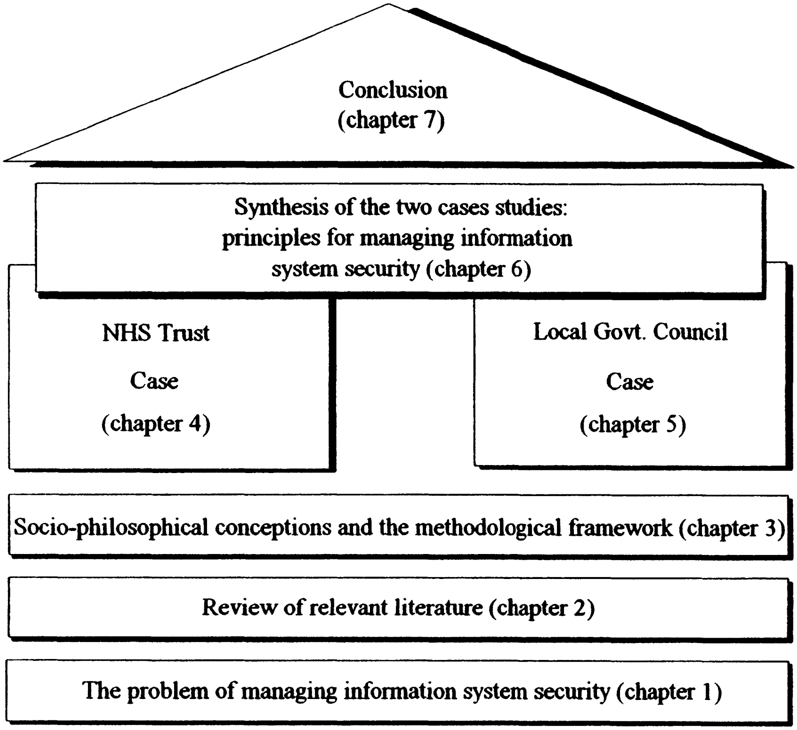

Conclusion (chapter 7)
Synthesis of the two cases studies: principles for managing information system security (chapter 6)
NHS Trust Case (chapter 4)
Local Govt. Council Case (chapter 5)
Socio-philosophical conceptions and the methodological framework (chapter 3)
Review of relevant literature (chapter 2)
The problem of managing information system security (chapter 1)

Figure 1.1 Structure of the book

A synthesis of key issues is presented in chapter 6. This is done in light of the theoretical and philosophical assumptions set out in chapters 2 and 3. Discussion revolves around four key themes – security policy, evaluation of security, design considerations in security and implementing information system security.

Finally chapter 7 concludes the discussion generated in the previous chapters. It summarises the main contributions of this book and identifies the drawbacks. The methodological problems implicit in the use of the framework are explicated, and the theoretical concerns related to advancement in knowledge about the management of information system security are underlined. Finally future research directions in the use of the concepts are identified.

2 The context of information system security

2.1 Introduction

The management of negative events within organisations has become an issue commanding ever more attention from the various professions attending to the information needs of computer using organisations. However the basic need for developing secure information systems has remained unfulfilled. This is because the focus has been on the means of delivery of information, i.e. the technology (Galliers 1993), rather than on the various contextual factors related to information processing (Dhillon and Backhouse 1994; Hitchings 1996). As a consequence we are caught in the 'technology trap'. Warman (1993) defines this as being the "situation that occurs when technology is introduced into problem situations by technical staff within organisations, without complete consideration of the implications" (p32). Although information system security is increasingly being considered as an organisational issue, the effort to prevent negative events has been aimed at protecting the technical infrastructure. This is largely because of the functionalist orientation of those responsible for managing information system security. As a result the security professionals have been unable to address the social attributes of organisations.

The scope of this chapter is to review and assess the current body of knowledge in the subject of information system security. The subject is broken down into its two constituent disciplines of information systems and security. The chapter is organised into five sections. After the introduction, section 2.2 presents an intellectual map that is used to traverse the literature. Sections 2.3 surveys the trends in information systems and security research. Paradigmatic orientation of the respective literature is identified and the systematic position of ideas presented in this book *vis-à-vis* the current research is established. Section 2.4 discusses and summarises the key themes of this chapter. Section 2.5 presents the main conclusions.

2.2 The intellectual map

In order to review the vast literature in information systems and security, we need a conceptual framework that not only helps us to classify the works but also to trace their intellectual origins. Theorists such as Burrell and Morgan (1979), Lane (1994) and Walsham (1993) assert that it is important to understand the theoretical concepts that form the basis of a methodological approach. This allows researchers to cut through the surface detail, which overlays the approaches, and see the world which they purport to analyse. This gives a clear indication of the philosophical assumptions of the different approaches.

A large number of approaches to information system security, at the present time, offer the same type of knowledge as that of natural science. They can be characterised as analytical, value-free and grounded in positivism. There are occasional efforts which consider the subjectivism of the applications and these researchers have increasingly looked towards social sciences for a suitable theory of knowledge. Sociology, in particular, offers a wide array of theories which can provide interesting insight. Burrell and Morgan (1979) organise these along two axes and present four paradigms of sociology.

Burrell and Morgan believe that all theories of organisation are based upon a philosophy of science and a theory of society. Consequently, they consider the assumptions about the nature of science to be located along the subjective–objective continuum, and assumptions related to the nature of society along the regulation–radical change continuum. The objective nature of social science is usually described as 'sociological positivism'. It is characterised by the application of models and methods derived from natural science to study human affairs. The subjective dimension stands in complete opposition to this and denies the relevance of models and methods of natural science to studies in this realm. 'Regulation', according to Burrell and Morgan, emphasises the stability and cohesiveness of the society, while 'radical change' views emphasise societal conflict and domination. Using these two dimensions, four paradigms have been suggested: functionalist; interpretive; radical humanist; radical structuralist.

Functionalist paradigm. The functionalist paradigm represents a perspective that is firmly rooted in the 'sociology of regulation' and approaches the subject from an objectivist point of view. Therefore it is concerned with the 'regulation' and control of all organisational affairs. Researchers grounded in this paradigm tend to provide practical solutions to practical problems. In the tradition of Durkheim, functionalists assume the social world to be composed of concrete empirical artifacts. They assume that such artifacts and their relationships can be studied by deriving approaches from the natural sciences.

Interpretive paradigm. Interpretivism, arising from the work of Weber, is grounded in the philosophy of phenomenology. It is concerned with the subjective understanding that individuals ascribe to their social situations. Although interpretivists agree with the regulative principles of the functionalists, they believe in a subjective analysis of the social world. Their fundamental concern is to study the world as it is. The core concept in interpretive sociology is intentional acts. The emphasis is to understand the acts, and link them with the meaning of conduct. Consequently they consider social reality as "a network of assumptions and intersubjectively shared meanings" (Burrell and Morgan 1979; p28). Reality, therefore, is an emergent property of the actions of individuals.

Radical humanist paradigm. This paradigm opposes the regulation theories and espouses radical change. Radical humanists view society as anti-human and therefore stress the emancipation of human beings so that they can realise their full potential. Besides, structural conflicts and modes of domination are also explored. The basic notion underlying radical humanism is "that the consciousness of man is dominated by the ideological superstructures with which he interacts, and that these drive a cognitive wedge between himself and his true consciousness. This wedge is the wedge of 'alienation' or 'false consciousness', which inhibits or prevents true human fulfilment" (Burrell and Morgan 1979; p32).

Radical structuralist paradigm. This paradigm also presents a viewpoint which opposes the regulation view of society. Radical structuralists although advocating radical change, share the objectivist standpoint of the functionalists. The key notion advocated by radical structuralist is that "change in society inevitably involves a transformation of structures which, even given favourable circumstances, do not fall or change of their own accord" (Burrell and Morgan 1979; p358). Consequently they consider the structures to change radically, thereby generating conflict and disruption in the *status quo*.

The four paradigms, discussed above, are defined by the meta-theoretical assumptions that form the frame of reference and the mode of theorising[1]. Each paradigm emphasises the commonality of perspective, although there may be much debate among those who adopt different standpoints. According to Burrell and Morgan theorists belonging to a particular paradigm may not even recognise the alternative views of reality which lie outside their boundaries. They also assert that the four paradigms are mutually exclusive and contradict each other. Consequently no socio-theoretic viewpoint can belong to more than one paradigm at any given time.

The fourfold classification of social theory, as proposed by Burrell and Morgan, is not without its critics. Many sociologists have considered the classification to be overly simplistic (see for example Hopper and Powell 1985; Chua 1986). Others regard the two analytical dimensions to be synthetic and incapable of dealing with subtleties of social theories (see for example Gutting 1980; Reason and Rowan 1981). In recent years, however, classification of social theories based on philosophical orientation has been advocated in the literature. Ritzer (1992), for example, stresses the paradigmatic importance of sociology. He suggests that this helps in understanding the fundamental images of the subject matter of sociology. Despite the criticisms voiced concerning the classification proposed by Burrell and Morgan, it has been widely used in the literature. Lane (1994), for example, uses it to trace the philosophical origins of operations research and system dynamics. Hirschheim and Klein (1989) have applied it to the area of information systems development. Such uses and applications give credibility to the Burrell and Morgan classification. Therefore the research presented in this book adopts the four paradigms as a means to classify the literature in information systems and security and to interpret the intellectual origins of the respective approaches.

2.3 Reviewing the context of IS security

This section classifies research in information systems and security. It identifies the key characteristics of particular research efforts and systematically places them within the socio-philosophical framework of Burrell and Morgan.

2.3.1 Functionalist orientation in managing IS security

Most of the research in information systems in the 1970s and the early 1980s was confined to the functionalist paradigm. Although there has been a tendency to move away from this paradigmatic thought, much of the current research in information systems and security is still functionalist in nature. With respect to the analysis, design and management of information systems, functionalist researchers purportedly investigate the causal laws, thus taking a rationalistic view of the phenomena under investigation, and furthermore they tend to express the objective and expert viewpoint of management.

Information systems literature

Alongside numerous other approaches, contingency theory research belongs to this paradigm. Contingency theory, as introduced by Woodward (1965), explored the relationship between organisational structures and technical systems. She revealed that organisational effectiveness was the consequence of a match between a situation and a structure. Information systems researchers have used contingency theory concepts to establish matches between the organisation and its environment. Ives *et al.* (1983) for example, used the approach to determine information system success based on user satisfaction. Majority of the earlier literature on identifying user requirements is also based on contingency theory (e.g. Bailey and Pearson 1983; Davis and Olson 1984; Baroudi *et al.* 1986).

Although contingency theory still dominates the information systems domain, it presents a simplistic viewpoint for research and practice. Human beings and organisations are far more complex than implied by this theory. The socio-technical designs of Mumford and Weir (1979), though not strictly functionalist in nature, are subjected to criticism on similar grounds. This is because they do not consider organisations as loose couplings where conflict, politics and power dominate. The use of user-satisfaction as a indicator of system success has also come under severe criticism (e.g. Melone 1990). This is because there is an attempt to quantify the variables without understanding the relationships. An abstract concept such as user participation cannot be understood in terms of any single organisational activity and thus poses complex problems of quantification.

Typical examples of functionalist thinking are also found in the mechanistic models of organisations as found in the 'bureaucratic phenomena' of Weber (1947) and 'scientific management' of Taylor (1911). Such thinking has had a significant influence on the development of information systems within organisations. Kling (1987) terms these engineering conceptions as 'discrete-entity' models. He suggests that the focus of mechanistic models is just on economic, physical and information processing aspects of technology. Consequently, such models ignore the context of complex social actions in which information technology is developed. Many information system professionals, still locked in the mechanistic viewpoint of organisations, tend to neglect the socio-political elements of information systems. This often results in ill-suited and inflexible information systems.

Most of the information systems strategy literature, focusing on competitive advantage, is also functionalist in nature. The competitive strategy of Porter (1980) and the value chain of Porter and Millar (1985) have significantly influenced the strategic thinking of information systems researchers. This has resulted in information systems strategy researchers and practitioners being concerned more with the overall business performance than with the data processing activities. Many other strategists have developed variants of Porter's conceptions. Typical among them are the Strategic Option Generator (Wiseman 1985), Strategic Opportunity Matrix (Benjamin *et al.* 1984) and the Strategic Grid (McFarlan *et al.* 1983).

An extreme form of functionalist thinking is reflected in many of the current systems analysis tools and techniques. DeMarco (1978), for example, notes that "political problems aren't going to go away and they won't be 'solved'. The most we can hope for is to limit the effect of disruption due to politics. Structured analysis approaches this objective by making analysis procedures more formal" (p13). With respect to requirements assessment for designing databases, McMenamin and Palmer (1984) assert that there should be one reality and it should be same for everyone. Only if the system requirements meet this criteria, will these be termed as "true requirements". Therefore developers are urged to develop systems that model this reality (Griethuysen 1982). In implementing such systems, there is an equally high proportion of functionalist strategies. Most of the planned change literature falls in this category. Prominent among these are the implementation (Alter 1992; Lucas 1981), counterimplementation and counter-counterimplementation strategies (Bardach 1977; Keen 1981).

However, in recent years there has been an increased emphasis on social considerations in designing, implementing and managing information systems. This has resulted in functionalist approaches being criticised for two of its basic assumptions. First, that there is an objective empirical reality and that positivist methods are the best way to make sense. Second, that the social world is best conceived in terms of an integrated order. Consequently, it is further assumed that system and organisational objectives are legitimate and have been agreed upon. Because of these assumptions, behaviour, intentions, and domination patterns of people have largely been ignored. Many authors now agree that the positivist means propounded by functionalist thinkers are in fact inappropriate for the study of systems (see for example Walsham 1995; Boland 1985; Klein and Lyytinen 1985). This is so because they fall short of giving a 'rich picture' about the complex interplay between the technological structures and the behavioural patterns.

Though the more recent forms of functionalism (Alexander 1985) have recognised the shortcomings, they still purport rationality and discrete thinking. Typical examples can be found in the works of Knol (1994) and Wolstenholme *et al.* (1993). Their concern has been to provide technical, computer based solutions with only a limited understanding of the nature of the organisation.

Security literature

The focus of most of the research in information system security is concerned with the formal automated part of an information system. Traditionally this has been studied under the banner of 'Computer Security'[2]. This sub-section reviews the security literature under three sub-headings: checklists, risk analysis and evaluation.

Checklists

One of the most prominent methods for specifying security of technical systems has been checklists. Checklists help in identifying every conceivable control that can be implemented. The underlying idea is to ask the question: "what can be done rather than what needs to be done" (Baskerville 1993). In the functionalist tradition, checklists tend to concentrate on means not ends. Many of the prevalent security checklists were constructed as evaluation guidelines, enabling an analyst to check the computer based system and determine the necessity of existing controls and the possibility of implementing new ones. Typical examples in this category are IBM's 88 point security assessment questionnaire (IBM 1972), the SAFE *Checklist* (Krauss 1972; 1980) and the *Computer Security Handbook* (Hoyt 1973; Hutt *et al.* 1988). The *AFIPS Checklist for Computer Centre Self-Audits* (Browne 1979), while addressing similar issues of disaster planning, encryption, off-site backup and physical security, marks a slight departure in its approach from the other checklists. Rather than providing a simple taxonomy of threats, it develops a kernel style framework of threats and the related defences. The AFIPS and the SAFE checklists are in general oriented towards computer centre audits.

The checklist approaches, although still widely used, carry less conviction when searching for theoretical foundations in security. They indicate where exclusive attention has been given just to the observable events without considering the social nature of the problems. Checklists inevitably draw concern on to the detail of procedure without addressing the key task of understanding what the substantive questions are. Procedures are constantly changing and for this reason offer little in the way of analytical stability.

Risk analysis

Most risk analysis approaches grounded in the functionalist paradigm draw mechanical and biological analogies (e.g. Veen *et al.* 1994). Prominent work in risk analysis and security evaluation methods takes this orientation and consequently adopts a prescriptive and normative mode. The methods suggest that negative events can be prevented and information systems be made secure if countermeasures are developed and implemented in a logical sequential manner. Practically all risk analysis approaches (e.g. Kailay and Jarratt 1994; Birch and McEvoy 1992; Fisher 1984; Parker 1981) prescribe methodologically discrete steps. Such approaches can be considered to have developed linearly and be controlled 'scientifically'. The Structured Risk Analysis methodology of Birch and McEvoy (1992), for example, views an information system in terms of data structures, data processing and events in a system. The fundamental principle in evaluating risk is to see the correspondence between a threat and a vulnerability. The approach is grounded in systems theory concepts. Other risk analysis and evaluation approaches also have similar philosophical underpinnings (e.g. Fisher 1984; Parker 1981; Zyl *et al.* 1994).

Risk analysis has indeed become the flagship of modern security management, and has enabled organisations to cost-justify new information system security and avoid the implementation of unnecessary and expensive controls. Practically all researchers in the information system security area use risk analysis in one form or another. Risk analysis techniques provide a means of forecasting critically the financial benefits *vis-à-vis* the initial investments. Such management science principles laid the foundation for techniques that were proposed by researchers such as Courtney (1977)[3] and Wong (1977). The US Department of Commerce declared risk analysis based on Courtney's technique as the government standard (US Department of Commerce 1979). Consequently, this technique has been widely used and forms the basis of a number of proprietary variants (e.g. Badenhorst and Eloff 1990).

Recent years have also seen the emergence of automated risk analysis methodologies, such as CRAMM (CCTA Risk Analysis And Management Methodology), used to conduct risk analysis and other related management reviews. Another widely used automated security risk analysis tool is RISKPAC (Computer Security Consultants 1988). Besides seeking to provide a balance between quantitative and qualitative risk analysis, RISKPAC also calculates annualised loss expectancy, thereby adhering to Courtney's conventional risk analysis.

The opportunities offered by risk analysis have also been a subject of interest to researchers. Merten *et al.* (1982) look at the technique from a managerial perspective, while Boockholdt (1987) cites its importance in establishing security and integrity controls. Anderson *et al.* (1993) outline risk data repository for a 'dynamic risk evaluation'. Krueger (1993) proposes a 'functional control matrix' for risk assessment which is based on the work done at The World Bank. Saltmarsh and Browne (1983) and Gallegos *et al.* (1987) differentiate between risk analysis and risk assessment – the former being the process of identification while the latter determines the degree of exposure. Using this differentiation, Gallegos *et al.* comment on the usefulness of risk analysis in establishing monetary value of the risks.

Risk analysis has had an influence on a number of other approaches. Notable among the earlier work is Parker's (1981) program and Fisher's (1984) methodology. Both approaches use risk analysis as a means to design controls. However, Parker introduces a different kind of analysis, the 'exposure analysis', which eliminates the elements of guesswork and consensus determination. He also proposes an alternative threat model. Loch *et al.* (1992) have gone further to develop a four-dimensional model of IS security which focuses on threat identification. Solms *et al.* (1993) apply risk analysis approaches to develop a 'process approach' to information security management.

Baskerville (1988) in contrast attempts to minimise the importance attributed to risk analysis by embedding controls in the logical model of an information system. Baskerville feels that the "best approach to the development of security analysis and design methodology, both for office use and for field practice in general, would essentially be to nest it as a component part of an existing, established, successful overall information systems analysis and design methodology" (p88). He suggests that a structured security analysis and design can be carried out in much the same way as a structured systems analysis. He chooses DeMarco's structured systems analysis and specification approach and implements controls in its logical design phase. Control identification is carried out by developing formal heuristics. Although starting from a different set of assumptions, at a functional level Baskerville's approach is not very dissimilar to the others.

Criticism of the use of risk analysis as a basis for developing secure systems has always been strong. Clements (1977) regarded classical probability theory to be inappropriate in assessing the security risks because threats are invariably random in nature. He proposed a methodology based on the theory of fuzzy sets for evaluation of data processing installations.

Whatever the claim of one risk analysis method compared to another, there is very little difference in the basic theoretical assumptions. A careful consideration of most risk analysis approaches suggests that indeed the boundaries between different classes of risk analysis are uncertain. Despite the diversity reflected in the literature, the issues that separate the different classes are of minor rather than major significance. As Burrell and Morgan note, "the real big issues are rarely discussed, lying hidden beneath the commonality of perspective which induces organisation theorists to get together and talk with each other in the first place" (p120).

Evaluation

Another category of research in computer security is in evaluation methods, whose rationale stems from the need to measure security (Longley 1991). Although it is often difficult to place a value on the level of security, a number of techniques exist which help in grading the security of systems. Early work on establishing such levels of assurance was sponsored by the US Department of Defense. The emphasis was to prevent 'unauthorised disclosure of information'. Among the various models of secure systems, the *Bell La Padula Model* (Bell and La Padula 1976) was the most prominent. The model deals with mandatory and discretionary access control with the primary objective of preventing illegal disclosure of information. Such an orientation is typical of functionalist approaches.

In 1983 the National Computer Security Centre in USA published the Trusted Computer Systems Evaluation Criteria, targeted at Automatic Data Processing systems. These provided computer vendors with an evaluation procedure to develop trusted computer systems. Today these criteria form an integral part of the US Department of Defense security procedures. Recently research has been carried out to improve and supplement these evaluation criteria. Chokhani (1992), for example, expands upon these criteria and proposes an Information Security (INFOSEC) approach to such an evaluation. However, the improved evaluation method takes a discrete event oriented approach. This creates a narrow conception about security which delimits it from the organisational context.

Hoffman *et al.* (1978) adopted a different basis for security evaluation. They proposed an automated tool, SECURATE, which is a design and selection process. The system automates the security analysis process and provides detailed ratings of a system security profile. SECURATE calculates the security ratings on the basis of fuzzy set theory and ultimately outlines the strengths and weaknesses in system design. Critics have however contested the statistical validity of fuzzy metrics.

Apart from in the US, evaluation criteria have been established in other countries as well. In the UK, for example, the Department of Trade and Industry and the Government Communications Headquarters produced a series of 'Green Books'. These were specifically intended for the Commercial Computer Security Centre. Other countries have also been quite active in this area. In an attempt to harmonise the work on information security standards in Europe, France, Germany, the Netherlands and the United Kingdom decided to combine the best features of each of the national initiatives. As a consequence, in May 1990, the first draft of the Information Technology Security Evaluation Criteria was issued. The text is referred to as the 'White Book'. Evaluation criteria, while having found public approval, still fail to provide answers to many important questions and are unacceptable to a body of researchers in the area (e.g. McLeen 1990). Again the main criticisms centre on the functionalist nature of the approaches. The national level initiatives tend to focus on 'The One Best Way', as advocated by Taylor in scientific management. The White Book, for example, stresses but fails to take a holistic view of the organisation and hence is extremely static. Because of such an orientation, an over-emphasis on the explanation of the *status quo* results.

The research carried out in the past decade or so has indeed enriched the field of information system security. It has been possible to implement legislative measures, especially in relation to a variety of technological crimes and privacy related issues (Turn 1982; Bequai 1987). These have also helped in implementing operational security, making it possible to establish management control by setting objectives and guidelines for accountability, surveillance, and authority (Hsiao *et al.* 1979; Weber 1988; Norman 1983). Threats and risks can also be identified with a reasonable amount of precision. Since users now have greater access to computer based information systems than before, identification and authentication methods have been well researched. However, the focus of attention has shifted and in particular database access control has received much attention (Highland 1985). Database access control mechanisms often have a legislative bearing, and this has led to relating access control issues to those of privacy (Adam and Wortmann 1989).

In spite of some basic benefits accruing from the evaluation methods, there is limited long term usefulness. The security evaluation approaches run into serious problems because they tend to provide essentially rational explanations of social affairs. The traditional approaches, developed for military use, have now been translated for commercial use. Since the social world of a defence environment is significantly different from a commercial setting, there are compatibility and coherence concerns.

To summarise, the main characteristics of the risk analysis and security evaluation approaches grounded in functionalist tradition can be enumerated as follows:

1. organisations and the information systems are considered in terms of strict boundaries which differentiate them from each other and the environment.

2. information systems and security management are conceptualised as being processual in nature and hence focus on the input, throughput, output and feedback mechanisms.

3. organisations and their information systems are considered secure if the needs of models (subsystems) are satisfied (i.e. by having secure subsystems, we can have a secure organisation).
4. different models that help in securing parts of an information system are mutually interdependent.
5. overall security can be achieved by analysing the behaviour of constituent elements of the system.

It will become clear from the discussions in the following chapters that the aforementioned characteristics of the prevalent approaches provide a very narrow conceptual framework with which to address information system security issues.

2.3.2 Interpretive orientation in managing IS security

An alternative view to functionalism is that of interpretivism. While most of the current and past research in information systems and security is confined to the functionalist paradigm, researchers have begun gradually to consider the philosophical aspects of interpretive sociology. This trend towards providing explanations within the realm of individual consciousness and subjectivity is more prominent among the information systems literature than in security research.

Information systems literature

The common theme in most research efforts is to appreciate the social implications of computer based information systems. Consequently there is an increased awareness of the cultural and informal aspects of information handling. Research in this paradigm does not take the 'what is' approach of the functionalists. Rather the organisation and social world is studied 'as it is'. The social world therefore is viewed as an emergent process which is created by the individuals concerned.

One of the main proponents of interpretive research is Walsham (1993). In a recent work he uses Gidden's (1984) structuration theory and develops a synthesised framework for interpreting information systems in organisations. Particular attention is given to the content, social context and social processes. Walsham attempts to address this question by establishing a link between the context and the process. In order to study the context (in the domain of information systems) Walsham draws on the 'web models' of Kling and Scacchi (1982) and Kling (1987). The web models study the social context of information systems by considering the social relations of the participants, the infrastructure of the available support and the history of previous developments. Walsham studies processes in terms of the culture and politics that prevails in an environment. The process model so generated draws heavily from the work done by Boland and Day (1989), Zuboff (1988) and Markus (1983). In the final synthesis he uses structuration theory to establish a link between the context and the process.

Walsham's research also draws on the contextualist analysis of Pettigrew (1985). Pettigrew's contextualism has inspired many other researchers associated with management (e.g. Fincham 1992) and information systems (e.g. Symons 1991; Madon 1991). The essence of the approach is on unfolding the interaction between structure and process. It views change as an outcome of an interplay between the historical, processual and contextual aspects of an enterprise (Whipp and Pettigrew 1992). Criticism of contextualism has come from Murray (1989), who argues that though contextualist research provides an insight into the trends and events in historical, cultural and political terms, it does not explain why the events take place.

Information systems research has seen another trend. Recognising the shortcomings of the one-dimensional descriptions of functionalists, many researchers have extended and modified the frameworks developed in the past. Galliers and Sutherland (1991) for instance have revised Nolan's (1979) Stages of Growth Model. Although the basis of the theory have come under criticism (Benbasat *et al.* 1984), the ideas provide a useful basis for strategic planning. A similar trend is also seen in the work of Ward *et al.* (1990). They have developed the portfolio model for information systems strategic planning based on the generic strategies of Parsons (1983). Ward *et al.* consider organisational reality to be meaningfully constructed from the point of view of actors directly involved. Such conceptions in developing frameworks suggest a trend towards a more interpretive explanation rather than a causal one as propounded by the functionalists.

A shifting emphasis of researchers towards the social considerations in information systems research led to importance being given to power and politics in organisations. Some pioneering work was done by Keen (1981) on organisational change and by Markus (1983) on the power and politics of information system implementation. This has given rise to a variety of approaches which consider emergent forms of organisations as a consequence of social interactions. In examining the influence of information systems on organisational structure in particular, many researchers acknowledge the importance of social phenomena, such as power, authority, and responsibility (Bloomfield and Coombs 1992; Roach 1992; Fincham 1992; Buchanan and Linowes 1980). Some theorists have even regarded designing information systems as similar to designing power systems (Boland 1986). Others have viewed computer based information systems as social resources having little influence on power systems (Kling 1980; Kling 1991; Wynne and Otway 1982). Mintzberg (1983), writing on the theory of management policy, highlights the concept of power in relation to influence, authority and control. He regards power to be central to all management activities. While he discusses the various issues related to this social phenomenon, he does not comment upon the manner in which the structures of power, authority, influence, control, and responsibility can be identified.

New research directions in information systems attempt to bridge a gap between man and machine, whole and part, the unique and the repetitive. Semantics, the study of relationships between signs and what they refer to has been used in the study of information systems (e.g. Backhouse 1991; Andersen 1990). The inherent argument in this strand of research is that symbols have meanings that are socially determined and that culture mediates between the formal systems and reality. Liebenau and Backhouse (1990) stress that in analysing and developing an information system, consideration should be given to the assumptions, beliefs and expectations of agents involved. A related study by Lehtinen and Lyytinen (1986) considers information systems as formal language-based systems whose use can be studied as linguistic processes. Lyytinen and Klein (1985) have used these concepts as a basis for a theory of information systems. Dobson *et al.* (1991) uses speech act theory for evaluating conversation structures when determining requirements for computer supported co-operative work. In a similar spirit Wand and Weber (1990) adopt an ontological approach in addressing issues concerned with the semantics of information systems. More recently Leifer *et al.* (1994) stress the importance of "deep structure information" in eliciting requirements for an information system. They propose a "focus group" technique in conducting such an exercise. These studies take a processual mode of enquiry and attempt to interpret social actions over a period of time.

In recent years the interpretive approaches have also been a subject of much debate and criticism. Orlikowski and Baroudi (1991), for example, debate the relative merits and demerits of interpretive and positivist approaches. Lee (1991) and Gable (1994) have explored the possibility of combining largely positivist and interpretive approaches. In the Burrell and Morgan tradition such combinations and meta-theorising is not possible, although more recent research in sociological theory is sympathetic to such trends. Ritzer (1992), in particular, is a strong advocate of developing integrated sociological paradigms.

Security literature

Interestingly, although information systems researchers have begun to consider the design of systems as a social act, their colleagues in the area of security are still locked in a mechanistic, technical vision. Consequently, they do not take account of any conflict of interest among the stakeholders and security design is seen by an instrumental interpretation of events. In fact there has been little research in information system security that can be termed as interpretive in nature. Functionalists would not even acknowledge the existence of such research efforts. For them the approaches are 'abstract' and 'too general'. However, because of increasing dissatisfaction with the prevalent security approaches, there is a growing body of researchers that has begun to consider alternative philosophical viewpoints in an effort to develop secure information systems.

Among this group is work by Willcocks and Margetts (1994) to assess information system risks on the basis of Pettigrew's contextualism. The conceptual framework developed by Willcocks and Margetts highlights the value of historical, context oriented, processual analysis and underlines the importance of social and qualitative aspects of information system security.

The technique of risk analysis has been a subject of debate among many researchers. Beck (1992) and Baskerville (1991) for example believe that over reliance on risk analysis as a technique in the design of secure information systems has negative consequences and there are few benefits in using the technique for predictive modelling. Baskerville (1991), recognising the utility of the technique in establishing the feasibility of information systems controls, feels that its predictiveness is of less value and its real usefulness lies in it, being an effective communication tool, especially between security and management professionals. Interestingly, Baskerville's earlier work in designing information system security was highly structured and mechanistic (see Baskerville 1988). In recent years he has shown an increased tendency towards interpretivism, especially in the area of risk analysis.

Newer research directions have considered the usefulness of traditional interpretive social theories in understanding the security issues. Examples are found in the work of Dobson (1991) and Strens and Dobson (1993). Their main concern is to provide explanations in terms of roles (of people), actions, goals and policies. In doing so they have used Searle's (1969) speech act theory to specify an organisation's security requirements. Although they begin with an interpretivist paradigm in mind, using Searle's and Austin's (1962) concepts in a mechanistic, linear manner shows a tendency towards functionalism.

Backhouse and Dhillon (1995; 1996) have also considered information system security from an interpretivist viewpoint. They correlate security concerns with organisational communication and intentional acts of agents involved, and security is regarded as an outcome of communication breakdowns. They draw upon semiotics, the theory of signs, to interpret the security implications of organisational actions. Researchers in other fields have also begun to consider organisations as social forms with patterned, ritualised and conventionalised interactions (e.g. Manning 1992).

An interpretivist analysis of information system security is certainly advantageous. It provides a holistic view of the problem domain, rather than the simplistic, one-dimensional, explanation espoused by functionalists. At the same time interpretive approaches lack a prescriptive component and are therefore of less utility to a security manager. Moreover the explanations appear to be enshrouded in complexity, largely because of a sophisticated sociological and philosophical basis, and as a result the audience of such security approaches is only a small group of academic researchers.

2.3.3 Radical humanist orientation in managing IS security

Information systems and security researchers within the radical humanist paradigm aspire to the liberation of managerial consciousness from cognitive domination. Radical humanists believe that the primary goal should be to divert management away from developing hierarchical and technological superstructures and towards harnessing the competence of people. Hence information systems and security approaches within this paradigm focus neither on technology nor on rational models, but on an emancipated body corporate.

Information systems literature

Traditionally, the notions of emancipation and of computer based systems have been at odds with each other. Computer based systems are usually considered as a means of managerial and social control (Huber 1982). They increase the domination of instrumental reason and therefore tend to create a social "iron cage". Emancipation on the other hand aims to free the human being from all sorts of restraints (legal, social, political, intellectual or moral).

Information systems research within the radical humanist paradigm is rather limited. Only a few authors (e.g. Lyytinen and Hirschheim 1989; Nissen 1989) have used concepts rooted in this paradigm. Lyytinen and Hirschheim (1989) use Habermas's social action theory to understand and describe information systems. Accordingly, "information system development and use is seen as manifestations of social action, and are always socially determined and conditioned" (p117). They conclude that computer based systems and emancipation are not necessarily antithetical, only paradoxical. In fact Lyytinen and Hirschheim (1989) assert that computer based systems can promote physical and organisational emancipation by establishing new discursive processes. Moreover they can also promote physical, psychological and organisational emancipation by debating all system related changes.

A slightly different stance is taken by Nissen (1989). Using Habermas's concepts he focuses on developing responsible human action. The basic premise of this work is that any computer based system "intends to influence how people act" (p99). Hence the main argument is that "whoever wants to work with information systems development and to act responsibly has to develop information systems which encourage and facilitate responsible human action by all the people affected" (p99).

A synthesis of emancipatory approaches for analysis, design and management of information systems is provided by Hirschheim and Klein (1989). According to them, if computer based systems development proceeds in a radical humanist tradition, then there would be three knowledge interests in mind:

> Systems would have features to support the technical knowledge interest and these would be similar to those developed under the functionalist influence. Other features would support the creation of shared meanings and reflect the knowledge interest in mutual understanding. This is similar to systems inspired by social relativism. Finally there would be a comprehensive set of features to support emancipatory discourse. This means that information systems are developed that facilitate the widest possible debate of organisational problems such that truly shared objectives could be agreed upon as policies for achieving them (p1208).

Security literature

As is the case with information systems research, there are only a few security approaches that espouse radical humanist principles. Prominent among them are the ideas propounded by Angell (1994), who, when discussing the impact of globalisation on today's businesses, takes a radical stance on the implications for the security of information systems. He criticises the functionalist perspective on the grounds that logic, rationality and technology are the vehicles of cognitive dominance that lead to the alienation of humans. This in turn becomes a barrier to the achievement of full humanness. He criticises the functionalist approaches to security on the basis of 'sheer complexity', 'profound uncertainty' and 'linear thinking', especially on the part of security managers (Angell 1993). Underlying this criticism is his concern with the 'pathology of consciousness', because of which humans see themselves to be trapped within a mode of social organisation that is created and supported in their everyday lives. Angell appears to be influenced by anarchism. Sociologists have classified such viewpoints as 'anarchistic individualism'. Anarchistic individualism is not a unified intellectual movement. It represents a perspective that advocates total individual freedom without any restrictions of external or internal regulation.

Research done by Webler *et al.* (1992) can also be categorised as radical humanist in nature. They use critical theory concepts to locate the activities of risk identification and risk assessment in the context of a social theory. Subsequently normative guidance for correcting the deficiencies inherently associated with these activities is provided. Webler *et al.* (1992) use Habermas's concepts of 'communicative rationality' and the 'ideal speech situation'. It is argued that these have "immediate ramifications of risk communication" (p23).

It may seem that the emancipatory approach to developing information systems and managing security holds great promise. However, this approach may be subjected to criticism on the grounds that an emancipated employee of an organisation might lose interest in the core business, introducing significant risks. Thus, while the cognitive domination aspects of radical humanism are appreciated, the implementation strategies largely remain vague and unclear.

2.3.4 Radical structuralist orientation in managing IS security

Information systems and security researchers in the radical structuralist paradigm attempt to explore the myths perpetuated by the functionalists. Radical structuralists believe that the business environment, social organisation and computer based superstructures are locked into a dynamic process of dialectical materialism. Therefore, they do not view organisations as monolithic structures with singularity of purpose and direction. Instead organisations are considered to be loosely coupled coalitions with conflicting interest groups. It is assumed that the various groups are in discordance with each other, but order can be restored through negotiation.

Information systems literature

In developing systems grounded in the radical structuralist paradigm, designers tend to take sides with the end users in the organisation. It is presumed that there is a conflict of interest between the top management and the users and that the system developers intervene in order to resolve discordance. The conflicts could centre around prestige, power or resources. Therefore the system development process is seen as a catalyst in resolving problems primarily through participation. Participation however is biased towards the end users. Systems developed with such an emphasis promote enhancement of craftsmanship and the working conditions.

Pioneering work by Ciborra on the contractual view of information systems falls into this paradigm. His focus is on interaction or bargaining between individuals both within an organisation and with the environment (Ciborra 1987). Ciborra therefore believes that conflicts in organisations can be exposed and then negotiated and those affected by the situation can be actively involved. As a consequence, competitive advantage with respect to computer based systems can be achieved, not by developing top level policies and strategies, but by 'tinkering at the grassroots of the organisation' (Ciborra 1994; 1991).

There are a number of success stories that support the radical structuralist viewpoint. Typical examples are the ECONOMOST (Clemons and Row 1991) and SABRE (Hopper 1990) systems. In both cases competitive advantage was created by the end users, not the top management. In fact systems such as these were derived from experimentation at the bottom rungs of the organisation, as opposed to the implementation of extensive management theories (Hopper 1990; Venkataraman and Short 1990; Clemons and Row 1988).

In spite of the information system success stories grounded in the radical structuralist viewpoints, there is much criticism of the basic assumptions. One could argue that not all problem situations can be viewed as potential conflicts. In many instances the core ideal may be co-operation. Others have noted that new technology creates demarcation disputes among different stakeholders (see for example Ehn 1988), and this runs counter to the basic premise of radical structuralists.

Security literature

Information system security researchers have not really used any concepts of the radical structuralists, although earlier work done by Lane (1985) shows some inclination towards this paradigm. This resemblance is merely superficial, since Lane's work represents an assemblage of loosely coupled ideas. Different facets of his work bear comparison with not only the work of radical structuralists but with that of interpretivists and functionalists as well.

It is however interesting to note that Lane's work was primarily inspired by issues related to risk analysis. Lane considers the behaviour of people to be a major factor in security. He argues that not only should it be the first factor to receive attention, but also be a key component of the risk analysis process. Lane proposes that in an organisation, staff with special responsibility should be designated. This he considers to be an effective way of reducing risks in computer based systems. He also proposes the division of responsibility and the division of knowledge about the system amongst many personnel. Lane's concepts show a slight departure from the underlying principles of other approaches but he has been unable to show how his 'psychological model of human action' can perceive 'social causality'.

2.4 Summary and discussion

This section synthesises the discussion so far. The preconceptions and dispositions of researchers are considered with respect to information systems and security. The paradigmatic orientation and preponderance of particular kinds of research is identified. Finally, comments are made about the systematic position of this research in the light of the Burrell and Morgan framework.

With respect to information systems researchers, there is a growing disillusionment with the narrow, one-dimensional viewpoint afforded by functionalist thinking. Although the importance of social issues related to computer based information systems has been recognised, researchers are still locked into conventional thinking. In reality, computer based systems dynamically interact with the formal and informal environments in which they are used. Hence it is important to understand human interactions, patterns of behaviour and meanings associated with the actions of individuals. Even 'modern' functionalists have recognised the importance of such issues. One group of sociologists has gone a step further to establish a new kind of functionalist thinking – neofunctionalism (for a fuller discussion see Alexander 1985). Trends can also be observed in other information systems related areas, where increasingly consideration is being given to the 'softer' issues. A case in point is the emergence of 'soft OR' (see Forrester 1994; Lane 1994). This has resulted in moving operations research away from its traditional engineering preconceptions.

By contrast to mainstream information systems work, the majority of the information system security researchers are still locked in a functionalist way of thinking. The earliest risk analysis (e.g. Courtney 1977) and security evaluation approaches (e.g. Bell and La Padula 1976) and the more recent security evaluation and design methods, are founded on functionalist conceptions, most being influenced by systems theory. While the utility of such methods, tools and techniques is evident, their focus is rather limited, restricting security to be viewed in an extremely narrow perspective – predominantly as managing access control. The concern therefore has been on maintaining a security perimeter around information processing activities. Although such concepts work well when organisational structures are hierarchical and information processing largely centralised, problems arise when organisational structures become flatter and more organismic in nature. This requires a broader vision for addressing security concerns. Recognition therefore needs to be given to social groupings and to the behaviour of people.

While recognising the significance of social issues, an increasing number of researchers have begun to explore alternative philosophical viewpoints. The review of literature in the previous sections has identified information systems and security researchers who are associated with the interpretive, radical humanist and radical structuralist paradigms. In terms of the use of social theories, there has been an extensive use of phenomenology, hermeneutics, critical theory and conflict theory. Table 2.1 summarises the research in information systems and security in terms of paradigmatic orientation, relevant theory and seminal work.

This book is an attempt to move the information system security thinking away from its functionalist traditions and align it with the mainstream information systems concepts. In taking forward the theory building exercise, this book adopts the viewpoint and process recommended by Burrell and Morgan (1979):

> Theorists who wish to develop ideas ... cannot afford to take a short cut. There is a real need for them to ground their perspective in the philosophical traditions from which it derives; to start from first principles; to have the philosophical and sociological concerns by which the paradigm is defined at the forefront of their analysis; to develop a systematic and coherent perspective within the guidelines which each paradigm offers, rather than taking the tenets of a competing paradigm as critical points of reference. Each paradigm needs to be developed in its own terms (p397).

Table 2.1 Summary of information system and security research

Paradigm	Theories used	IS methods and seminal work	Security methods and seminal work
Functionalist	System theory; Contingency theory	IS success (Ives *et al.* 1983); Requirement identification (Bailey and Pearson 1983; Davis and Olson 1984; Baroudi et al 1986), Systems development (DeMarco 1978)	Traditional risk analysis approaches (Courtney 1977; Parker 1981; Fisher 1984); Security evaluation methods (Bell and La Padula 1976; Solms *et al.* 1994)
Interpretive	Structuration theory; Phenomenology and Hermeneutics; Semiotics; Contextualism	Information systems strategy, system design and implementation (Walsham 1993; Boland 1985); Use of signs in system specification (Liebenau and Backhouse 1990)	Risk analysis and the communicative content (Baskerville 1991); Speech act theory and security development (Dobson 1991); Pragmatic considerations and security (Backhouse and Dhillon 1996)
Radical Humanist	Critical theory; Anarchistic individualism	Theory of information systems and system specification (Lyytinen and Klein 1985)	Strategic security options of Angell (1994); Critical theory and risk analysis (Webler *et al.* 1992)
Radical Structuralist	Conflict theory	Contractual view of information systems (Ciborra 1987)	Not found (except some concepts by Lane's 1985)

In essence, research presented in this book does not build on criticisms of research grounded in other paradigms and thereby be involved in 'academic demolition'. In fact it appreciates the usefulness of many of the approaches, although to a limited degree. For example, risk analysis, rooted in the functionalist paradigm, is extremely useful in evaluating security, but an entire security strategy cannot be based on it. Similarly the traditional evaluation methods can be useful in assessing the extent of security, but a corporate strategy to prevent the occurrence of negative events cannot be based on the highly structured security evaluation criteria.

Because of the usefulness of a socio-organisational perspective in information system security, research presented in this book is rooted in the interpretive paradigm. This is justified on the basis of two issues. The first relates to the ontological status of the subject of investigation, and the second concerns the nature of models that are used as a basis of analysis.

With respect to the ontological status of security, it is worth reflecting on the basic beliefs presented in the sections so far. Most security research has been classified as belonging to the functionalist paradigm and these theorists have treated security as something tangible and concrete. The survey of literature has shown that such researchers have an objective view of reality and they consider information systems and organisations as concrete entities. Viewing organisations and information systems on this basis results in inter- and intra-organisational social relationships being considered as incidental. Security is therefore seen as a means to protect something tangible and hard. However, the occurrence of negative events, for which security is provided, cannot be viewed as discrete events. The prevention of such events therefore means more than just 'locks and keys'. It has to relate to social groupings and behaviour. Investigation into such matters is the main concern of this book.

2.5 Conclusion

The contribution of this chapter is twofold. First, it presents the current research directions in studying information systems and security. It identifies a trend in information systems research, moving away from a narrow technical and functionalist viewpoint. With respect to information system security, the review of literature identifies the dominance of functionalist preconceptions. There have only been a few isolated attempts to break away from this tunnel vision. The critique of the current approaches leads to a socio-organisational perspective being adopted in this book. This standpoint is systematically classified to be within the interpretive paradigm of Burrell and Morgan.

Second, the concepts presented can be justified by recognising the fact that the use of a socio-organisational perspective for understanding information system security is still at a theory-building stage. The literature search for the main idea propounded in this chapter found practically no case studies that used a socio-organisational perspective for evaluating information system security. This points to the need for empirical research to develop key principles to facilitate the prevention of negative events and therefore to help in the management of information system security. This book makes such a contribution.

[1] This definition of a paradigm differs somewhat from Kuhn's conception. A paradigm according to Kuhn is a universally recognised scientific achievement that for a time provides models, problems and solutions to a community of practitioners.

[2] In the security literature there is confusion about the use of terminology. The terms 'Computer Security' and 'Security of Information Systems' (and their extensions) are often used interchangeably. We shall however restrict our usage in accordance with the definitions in chapter 1.

[3] Courtney (1977) defines risk (R) in terms of the probability (P) of an exposure in a year and the cost (C), or loss, associated with the exposure. Therefore risk is calculated as: $R = P \times C$

3 A framework for interpreting the management of IS security

3.1 Introduction

The previous chapter identified the socio-philosophical orientations of research in information systems and security. This chapter establishes a framework for interpreting the management of information system security. It was noted earlier that in managing information systems the importance of understanding socio-organisational aspects has gained importance. Hence there has been an increased use of interpretive approaches in the analysis, design and management of systems. However, researchers in the information system security domain are still locked in their functionalist traditions and most of the approaches are based on positivistic conceptions of the nature of reality. As Galliers (1991) points out, these methods are more suited to the natural sciences. One indeed questions the appropriateness of these methods (Galliers 1991; 1993; Hirschheim 1985). This also raises questions as to how such methods will help a practitioner in the management of information system security.

There have been numerous demands on part of researchers to consider the ontological and epistemological beliefs of management approaches. It has been argued that assessment of a particular scientific discipline must proceed with an implicit or explicit understanding of what the discipline is and how it develops (see for example Banville and Landry 1989). Preston (1991) in particular calls upon information systems researchers to examine the underlying assumptions and theoretical constructs that shape their understanding. This chapter, in conjunction with chapter 2, can be considered as one response to Preston's appeal.

This chapter is organised into four sections. After an introduction, section 3.2 focuses on the underlying beliefs of any methodological approach. Section 3.3 presents the detailed framework that can be used for interpreting the management of information system security. Section 3.4 draws out the conclusions of this chapter.

3.2 Choosing an appropriate methodological base

This section identifies the underlying assumptions of the research efforts and assesses the socio-philosophical orientation of this book. Various theoretical considerations are also specified.

3.2.1 Sociological and philosophical assumptions

The choice of an appropriate approach turns on a set of assumptions about ontology, epistemology and human nature. These are depicted schematically in figure 3.1. According to Burrell and Morgan (1979), the basic assumption is that "all theories of organisation are based on a philosophy of science and a theory of society" (p1). Accordingly, the systematic position adopted in this book is placed within the interpretive paradigm (see chapter 2).

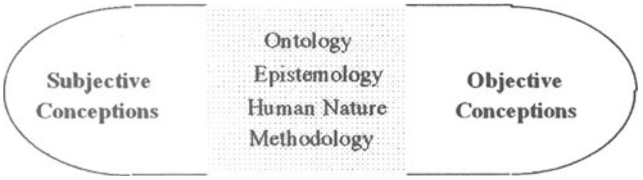


Figure 3.1 Scheme for analysing assumptions about the nature of social science. Based on Burrell and Morgan (1979)

Interpretive approaches considers our knowledge as a social construction of reality. The reality that we wake up facing is a human construct left over from yesterday (Frye 1981): it is socially sustained and socially changed. In the interpretive tradition, organisations and information systems are therefore human constructs that are shaped by factors external to individual cognition. Consequently they allow different groups to relate to each other and to the environment. Walsham (1993) views this as a dynamic process of action/context interweaving, which is fundamental to understanding the process of organisational change and the role of information systems. Liebenau and Backhouse (1990) have viewed organisational environments as constituted of the informal, formal and the technical parts which are in a state of continuous interaction. These concepts help us in understanding the nature of information system security by evaluating the names, concepts, labels and signs which are used to structure reality. Doing so takes us closer to a nominalist position which does not admit to there being any 'real' structure (Burrell and Morgan 1979). Burrell and Morgan regard 'names', 'labels' and 'signs' as artificial creations which are used to describe and make sense of the external world. A sign is an object or an event which stands for something else. It therefore enables a person to act according to the thing that it signifies. This requires a deeper understanding of the social world, where reality is considered to be the product of individual cognition. These concepts form the ontological basis adopted in this book and take us away from the more common 'realist'[1] stance.

Epistemologically the concepts presented in this book are inclined towards an anti-positivist[2] position. They discount the use of approaches which are rooted in the natural sciences. Consequently in searching for regularities and causal relationships between different elements of information systems, the emphasis is not to verify or falsify hypotheses but to develop a deeper understanding of the contexts. The research presented in this book considers the organisational environment to be relativist and therefore information system security is considered in terms of the coherence of the informal, formal and technical components of information systems. Security therefore is interpreted from the 'inside' rather than the 'outside'. A pragmatic orientation is the key characteristic of the approach presented in this book.

Assumptions about human nature significantly determine the choice of a methodological approach. Such assumptions stem from models of man as reflected in any given social-scientific theory. The models could either be determinist, which regard people and their activities as completely determined by their situation, or voluntarist, which consider people to be completely autonomous and free-willed. Concepts in this book are inclined to neither of the two extremes. Activities of human beings are regarded as a consequence of a complex interplay of situational and voluntary factors.

So, based on these ontological and epistemological assumptions, how does one understand the social world and the context of information system security? As noted in chapter 2, there has been an over-emphasis on basing research on systematic protocol and technique. The information system security domain presents a rich source of behavioural issues which have not been adequately understood. Since security of information systems can only be interpreted by developing a deeper pragmatic understanding of the social context, the security professional needs to obtain first-hand knowledge by 'getting inside' the situations.

3.2.2 Theoretical considerations

In order to develop a framework based on the philosophical stance adopted above and assess its applicability, we need to develop a sound theoretical perspective. As Dubin (1969) suggests "understanding is only achieved when we know how and why the elements of a theory interact over time". However, we must recognise that a "theory is both a way of seeing and a way of not seeing" (Walsham 1993; p6). It is for this reason that practitioners make major criticisms about the use of theory. According to them real human activity does not use theory consciously, hence it has little or no significance in practice. Walsham (1993), however, considers that what is needed is an appropriate blend of theory and practice which can be used by individual practitioners. Moreover, this synthesis may provide a means of communicating knowledge to others.

In developing a framework for interpreting the management of information system security, a number of theoretical approaches can be used. Most are rooted in research evaluating and understanding computer based information systems in organisations. Kling's (1987) Web Models, Checkland's (1981) Soft Systems

Methodology, Pettigrew's (1985) contextualism, Lyytinen's (1985) language action view, Mumford and Weir's (1979) socio-technical designs, all provide useful insight (see chapter 2). Kling's web models of social interaction appear useful. In a study by Kling and Iacono (1989) information systems have been related to organisational structures and to the manner in which they become institutionalised. However, since the management of information system security is a dynamic process, they are less appropriate in the present context. Pettigrew's (1985) contextualist approach appears to overcome this problem. His analysis is concerned with three elements: the process component, the context component and the outcome component. He regards problem-solving and decision-making processes as containing elements of 'muddling through' and views organisations as systems of political action. The main drawback of using this approach is that there is not enough emphasis on the connection between what he terms the outer context and the other contextual levels. This is in spite of the fact that he claims this to be the vital element of his approach. At a more general level though, Pettigrew emphasises the utility of understanding the socio-political elements of the context, but falls short of providing a means of identifying the various interest groups which wield power.

In addition to the drawbacks identified above, one fundamental problem with contextualist analysis is that it does not provide a complete method of analysing the linkages between the contexts and the processes. Pettigrew however does emphasise the importance of analysing these linkages. In work done by Walsham (1993), many of these problems have been overcome. One of the main contributions of his work has been in providing a means of analysing the linkage between the contexts and the processes. This he does by using Gidden's structuration theory. However, the main criticism of Walsham's interpretive approach is the use of structuration theory itself. Structuration theory (Giddens 1984) can be associated with a recent trend in sociological theory towards integration, synthesis and metatheorising (e.g. see Ritzer 1992). The theory thus aims at resolving the debate between those who emphasise the role of human agents and human actions as opposed to the structure of social systems. Although the separation of structure and interaction into three dimensions is a useful conceptual schema, it is difficult to apply it to empirical studies. However, it can provide insight into interpreting information system security.

Other theories belonging to the interpretive paradigm that have been used in information systems research are rooted in the phenomenological and hermeneutic schools of thought (e.g. Habermas 1972). Idhe's ideas on the phenomenology of instrumentation have been used particularly in developing perspectives for analysing aspects of information systems (Rathswohl 1990). A phenomenological analysis assumes there to be a correlation between actual human experiences and the possible range of conduct. Consequently, it takes the form of a methodical study of consciousness for the purpose of understanding the structure and meaning of human experiences (Boland 1985). Within the domain of information systems, phenomenology provides an alternative to empiricist methodologies. The focus remains on how an information system is experienced and used by humans.

In recent years concepts drawn from semiotics, the theory of signs, have been extensively used in understanding information systems. Semiotics traces its roots to the work of Saussure (1966) and Pierce (1958). However, the Saussurian and Piercian perspectives are significantly different in terms of the nature of the sign[3]. In studying the representation of signs and how signs take meaning in everyday life (Eco 1976), semiotics bases itself largely on a linguistic model. The use of language as a sign system is however paradigmatic. In semiotics a sign system is created by an individual who is the interpreter, referent, user and reproducer of a common meaning in a given context. The greatest strength of using semiotics is that objects, things, words or any sign vehicle that carries a message, have no inherent meaning (Manning 1992). Meaning is attached only by the context and by norms. This is a very useful concept in interpreting the management of information system security since the relevance of the security measures is considered in relation to the organisational environment. Ontologically, this is a nominalist position and also forms the basis for the framework for interpreting the management of information system security.

3.3 The framework

Methodological approaches can either be ideographic or nomothetic in nature (see for example Blumer 1969; Burrell and Morgan 1979). Ideographic approaches are based on the view that organisations and the social world can only be understood by obtaining first-hand knowledge of the subject under investigation. Hence these approaches stress the importance of getting close to the subject, exploring in detail the life history and the background. These approaches encourage the researchers and practitioners to get involved in the everyday flow of life of the organisation and develop insights about encounters with one's subject. Ideographic approaches emphasise that the subject should be allowed to unfold its nature and characteristic during the process of investigation and analysis. Nomothetic approaches, on the other hand, focus on the process of testing hypothesis with scientific rigour. The main preoccupation of scientific approaches is to construct scientific tests and use quantitative techniques for data analysis. Typical examples of such techniques are the survey questionnaires, personality tests and other standardised research instruments. It is contended that the data collected by these means helps organisations to identify prescriptions for management problems. Since the primary concern of the framework presented in this chapter is to understand the underlying causes and the related patterns of behaviour leading to the occurrence of negative events, an ideographic methodological approach is used.

3.3.1 Implicit assumptions

It is the contention of this book that to solve the problem of managing information system security, one needs to understand the deep-seated pragmatic aspects of an organisation. Solutions to the problem of security can be provided by interpreting the behavioural patterns of the people involved. Through the help of two case studies, this book shows how such an analysis can be conducted. It also draws out some general principles that would guide practitioners to better manage information system security.

The conceptual framework adopted in this chapter considers the management of information system security to be constituted of the following elements of interest:

- The business environment of an organisation and its impact on the development and use of computer based information systems.
- The organisational culture and its consequences for the analysis and design of information systems and the emergent implications for the management of information system security.
- The expectations and obligations of different roles in an organisation and implications for information system security.
- The meanings of actions, patterns of behaviour and interpretations for information system security.
- The logical specifications and management of information system security.

There are a number of methodological approaches which help us in analysing the deep-seated pragmatic aspects and exploring the elements of interest identified above. However, what is needed is a methodological framework that views organisations in terms of their stable underlying patterns of behaviour, for it is these behavioural patterns that contain the deep-seated pragmatic aspects of an organisation.

3.3.2 Conceptual framework for interpreting the management of IS security

The approach used in this book is based on understanding social norms and individual affordances. This helps in interpreting the patterns of behaviour at social and individual levels (see Liebenau and Backhouse 1990; Stamper *et al.* 1988). The approach assumes reality to be an outcome of human interactions which generates shared norms and experiences. The fundamental concept used in the conceptual framework is that of a 'sign' and its referents (i.e. a pattern of behaviour in the 'real' world). This allows an analyst to view organisations and their information systems as sign processing systems where people do the processing (Liebenau and Backhouse 1990). Proponents of these ideas argue that by understanding the concept of a sign and its related properties, it is possible to improve the analysis and design of computer based information systems (see for example Zuurbier 1992; Marche 1991; Andersen 1991; Stamper 1991; Scholz 1990).

Concepts in this book draw heavily from the work done by Liebenau and Backhouse (1990) and Stamper (1973; 1991). These authors use semiotics to understand the analysis, design and management of information systems. Semiotics considers sign processing systems at four levels: pragmatics, semantics, syntactics and empirics. Consequently, four classes of activities are identified. These are represented in the form of a 'staircase' model in figure 3.1. These classes represent very different ways of understanding the signs and evaluating the properties. Associated with each class is a group of established disciplines. Semiotics, therefore, is not so much a new subject, as a regrouping of ideas from many disciplines (Stamper 1985). The various classes of activities are summarised below:

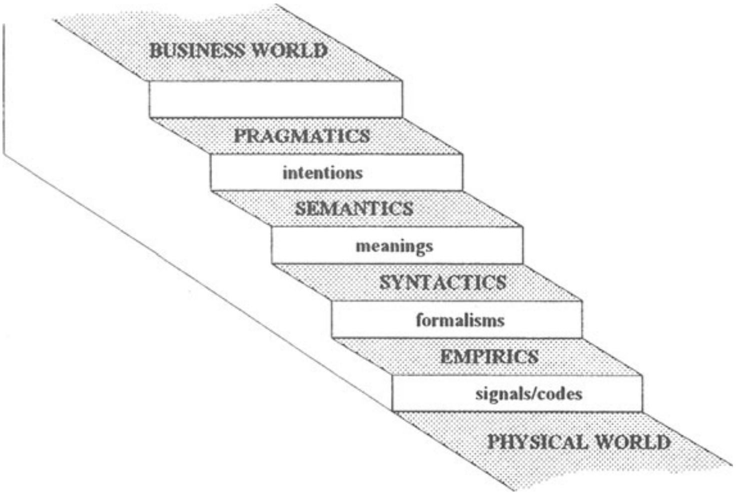


Figure 3.2 The steps from a physical world to the business world (reproduced from Liebenau and Backhouse 1990)

Pragmatics. This level describes the context of an organisation and behavioural aspects of human activities. It is assumed that, in any organisational setting, meaningful signs are employed to perform acts of communication. Understanding the nature of communication processes and the shared assumptions of people helps in evaluating the information handling activities of an organisation. This also allows us to comprehend the ambiguities arising because of interactions among people. The beliefs, expectations, commitments, intentions and communication patterns of people constitute the pragmatic structures. The repertoires of pragmatic structures unfold the social world which is characterised by the norms of groups and broad cultures stiffened by explicit rules and laws. One means of understanding the pragmatic structures is by analysing the silent messages afforded by individual actions. The framework adopted in this book uses Hall's (1959) culture map to draw such interpretations (see appendix).

Semantics. This level focuses particularly on analysing the meaning of acts of communication. It is assumed that communication of intentions involves the interpretation of signs. The process of interpreting signs is concerned with evaluating the meaning content of communications. Often actions of individuals have different connotations for different people. Hence it is important to understand the behaviour of people and identify responsible individuals. Inability to comprehend the behavioural and normative issues can have severe implications for the analysis and design of computer based information systems.

Syntactics. This level is concerned with the system of rules and regulations. No consideration is given to the semantic content of the signs and the behaviour of the people. The focus is on formal relationships among signs and the operations to which they may be subjected. Hence organisational tasks are considered as formal co-ordinating mechanisms. The rules and procedures are however established after pragmatic and semantic reviews. The function of a well defined syntax is to exploit the structural features of a complex sign, thus allowing us to express relationships. This brings in consistency and integrity into our developmental activities.

Empirics. This level is concerned with establishing a means of communication and information handling. Empiric issues largely relate to the statistical behaviour of control systems. Hence, of focal concern are the routine information processing activities of an organisation. With respect to the design of computer based information systems, empirics allows us to specify the appropriate technical support for the systems.

The top and bottom landing of the staircase model depicts the business and the physical worlds respectively. The business world is created by a repertoire of pragmatic structures representing relationships between people. These are culturally determined and are governed by explicit behavioural norms. The physical world is concerned with creating physical phenomena from which we can construct signs. At a practical level this could be concerned with choosing the right hardware. The four-fold classification has primarily been established to solve organisational problems. Their underlying assumption is that problems are linked to the communication of information. Since information is integral to organisations, it is important to understand it as a social process. Furthermore, the use of information is seen as a process of manipulating signs. The four levels can be interpreted as a series of steps by which the physical world is constructed (figure 3.1). Beginning with the social world, people develop patterns of behaviour, systems of norms, values, expectations and obligations. These bind individuals and groups together. Next we assign meanings to different actions and behaviours. Gradually rules and procedures are established. Finally, cause and effect properties of the physical devices are established. With respect to information systems, moving up and down the staircase facilitates a deep understanding of the organisation and the related information handling activities.

3.3.3 Method for using the concepts

There are six discrete steps in using the staircase model for interpreting information system security (see table 3.2). First, the business world is evaluated. The mission statement and purpose of the organisation are analysed. This is subsequently co-related with specific business and operational strategies. These strategies are analysed in relation to the security of information systems. Furthermore the ethical aspects of human actions are analysed. Second, the pragmatic elements of the organisation are looked into. Here the concern is to understand the organisational norms and the prevalent security culture. This determines compliance of human actions to legislative and other formal procedural controls. The review of security culture also elicits the level of awareness among members of the group. Third, at the level of semantics the meanings of our actions are analysed. This leads to an analysis of misapplication and misrepresentation of rules. Identification of a responsibility structure at this stage helps in commenting on the structures of power and authority and thereby considers issues related to accountability and attribution of blame. This is important especially in maintaining the security of information systems. Fourth, the concern is to analyse the security review and audit practices, if these are in place. Fifth, the technical security issues such as viruses and encryption are examined. Sixth, the hardware and physical security issues are analysed.

The first three levels of the framework facilitate a deep understanding of organisational practices including those for information system security (table 3.2). Such an understanding provides a richer picture of the problem domain and is more useful than a superficial functional analysis that is usually practised (the bottom three levels of the framework). In light of the framework for conducting a security review, it can be interpreted that the majority of the information system security approaches presented in chapter 2 are confined to the bottom three levels. Hence, it can be argued that not only are these approaches functionalist in nature, but they also impose restrictive technical solutions. The analysis from the case studies presented in chapters 4 and 5 will show the limits of the current approaches in addressing security concerns arising at the business, pragmatic and semantic levels.

Table 3.1 Levels of analysis

Analytical level	Brief description	Factors of interest in information system security
Business world	Shared patterns of behaviour; system of norms, values, expectations and obligations	Mission and purpose of the business; ethics; security policy
Pragmatics	Culture; context; intentions	Organisational norms and security culture; compliance; education, training and awareness
Semantics	Meanings of human actions	Consequences of misinterpretation of data; misapplication of rules; allocating responsibility; attributing blame
Syntactics	Rules and procedures	Security reviews and audits; data integrity and availability rules and procedures; program bugs; software piracy
Empirics	The statistical behaviour of control systems and the choice of communication channels	Coding; signalling; viruses
Physical world	Physical devices etc.	Hardware security; physical security

The basic objective of the method presented above is to provide a means of evaluating social reality and guiding practitioners and researchers in eliciting particular information system security concerns. However, formal procedures of any kind tend to impose a rigid structure. The researcher should be aware of this shortcoming and remain open to ideas and to new conceptual elements that emerge as research progresses.

3.4 Conclusion

The main contribution of this chapter is to present and justify an interpretive approach as a means of inquiry. The analytical method has been derived on the basis of the sociological and philosophical beliefs suitable for analysing information system security. These beliefs are concerned with the nature of the problem at hand and the various theoretical considerations. The utility of identifying the assumptions at the outset is two-fold. First, it is possible to formalise an analysis process. This is important especially when the problem domain is characterised by complex intertwining of social interactions. Second, the ontological and epistemological clarifications pave the way for choosing an appropriate approach.

Problems in information system security have rarely been addressed methodically by using beliefs rooted in the interpretive paradigm. This chapter stresses that theory building in the area of managing information system security can be accomplished through empirical investigation. The objective of this investigation is to interpret complexities of the social phenomena. Chapters 4 and 5 show how these concepts can be applied in real situations.

[1] According to a realist, a social world has a reality of its own. Ontologically it exists prior to any human being and therefore is as hard and concrete as the natural world.

[2] Giddens (1974; p1), maintains that 'the word "positivist" like the word "bourgeois" has become more of a derogatory epithet than a useful descriptive concept'. However in the current context it is used to describe concepts that characterise the epistemology and not empircism.

[3] Saussure conceived of a sign as being composed of two parts, a signifier and signified, while Pierce conceptualises it in terms of an interpretant, representamen and object.

4 The case of managing IS and security in a Hospital Trust

4.1 Introduction

The case study described in this chapter concerns the introduction of a new computer based integrated Client Information System (CIS) into a Hospital Trust. At the time of the study most of the system modules had been developed and were being tested largely for technical aspects. The system was being introduced during a period when the organisation was experiencing significant changes. It was an environment where new structures were being created and the existing ones changed. Indeed, the case study was selected primarily because of these factors. The analysis of these structures, formal and informal, provides insight into the management of information system security.

The chapter discusses the economic, political, social and technological factors that are influencing the organisation. These are examined at a wider contextual and organisational level. Section 4.2 describes the nature and orientation of the Hospital Trust and recognises the growing importance of information systems in managing the health service. Section 4.3 presents an analysis of the case study. It uses the conceptual framework developed in chapter 3 to examine the management of information system security. Section 4.4 identifies the emergent themes for discussion. These form the basis for developing a synthesised perspective in chapter 6. Section 4.5 concludes the interpretation of information system security in the Hospital Trust.

4.2 Organisational background

In order to gain an understanding of the wider context of organisational events and actions, it is necessary to evaluate the environment of the Hospital Trust. This is because organisational processes, structures and information systems have largely been determined by the wider contextual changes in the UK NHS. The first part of this section discusses the broader sectoral context and traces the history of changes in the Health Service. The second part describes the setting of the case in question. This is followed by a discussion of the IT infrastructure in place.

4.2.1 The National Health Service in the UK

The UK National Health Service was formed in 1948. It inherited a tripartite structure of health services. The General Practitioner (GP) was the first point of contact in event of any illness. Acute services were provided by voluntary hospitals, while longer-term care was the responsibility of the municipal hospitals. Preventive health care fell within the jurisdiction of the local authorities. The early years of the National Health Service saw little change. Efforts were concentrated on administering what was present. In a hospital, a consultant was designated as 'consultant-in-administrative-charge', an appointment based on seniority rather than on managerial ability. During this period there were a few attempts to organise the medical work. Prominent among these were the recommendations of a series of 'Cogwheel Reports'. The primary suggestion was to amalgamate clinical specialities of a similar nature into divisions. Representatives of the divisions would voice their concerns to the chairman who would in turn have a liaison with the nursing staff and the administration. The main management emphasis of Cogwheel Reports was on the efficient use of resources. The question of styles or skills of management necessary for achieving efficiency was completely ignored. There were simultaneous improvements in the nursing arena as well. The Salmon Report of 1966 was pivotal in bringing about changes in nursing management structures. Consequently, existing nursing hierarchies were formalised. This gave nursing greater autonomy from doctors.

The beginning of the changes

The 1974 saw the first major reorganisation of the NHS. The primary purpose was to unify the tripartite structure into a single integrated organisation. The main motivation behind the reorganisation was to have a good liaison between the hospital system, general practice and the community and public health services. It was envisaged that this would facilitate overall planning of the health services. The basic entity of the new organisation was the health district. A District Management Team was set up to oversee the functioning of the districts. It comprised the district nursing officer, the district community physician, the finance officer, and the district administrator. Besides, the team also included the chairman and vice chairman of the District Medical Committee, a hospital consultant, and a GP. Regional Health Authorities were established but the district became the focus of development and implementation of plans. Decision making by the District Management Team was based on the principles of consensus management. It was a period when the principles of self-organisation were applied to the entire service. The philosophy was that each speciality would manage itself separately, but come together to manage the service as a whole. Thus doctors would manage doctors while the nurses would manage the nurses. Ultimately, there would be consensus management through committees and consultations. The period represented the "apotheosis of health service syndicalism[1]" (Klein 1983).

From consensus management to an internal market

Though consensus management was the dominant force until 1983, it was not by any means an ideal style for the NHS. The clinical services remained largely unmanaged. The nursing profession, because of a high proportion of relatively unskilled workers, was unfit to assume professional and managerial responsibilities (Strong and Robinson 1992). It was not possible to tackle the relations between the key NHS specialities. This led to huge fragmentation of the specialities and to strong internal loyalties. Consequently, it was increasingly becoming difficult to provide an efficient and a co-ordinated overall service. Though the national health service arrangement was considered to offer real and politically viable solutions to many of the health care delivery problems, the arrangement was flawed.

The rampant power of the medical profession which resulted in an inadequate management structure and a fragmented corporate culture, formed the basis on which Griffiths could justify his 1983 management inquiry report. Roy Griffiths was a businessman and head of Sainsbury plc, the supermarket grocery chain. He brought with him the experience of financial success and quality products. The recommendations of his report were implemented in 1984 with the introduction of principles of general management into the NHS. The key concern of Griffiths was to contain costs and yet provide quality service.

The changes initiated by the Griffiths report took further form when the Community Care Act (1990) was enacted. The principal objective was to inject a market ideology into the health care delivery process. Consequently, an internal market was established in the NHS. The GP was retained as the first point of contact in the event of any illness and became the provider of primary care. Some GPs however had the facilities to provide some secondary care as well. Managed hospitals, self-governing hospitals and private hospitals took on the role of providing the majority of the secondary health care, the care being purchased by local authorities and general practitioners. In this new environment clinical activity was sustained through contractual agreements between purchasers and providers, thus transforming co-operative professional values into business relationships. The intention of these changes was to specify managers who would be responsible for co-ordination and control of the service. This has been achieved by establishing a single line of command from the hospitals to the Health Secretary through the NHS Management Executive.

The information management initiative at the national level

The introduction of general management principles into the NHS meant that apart from matters of firm leadership and corporate structure, the question of controlling the cost and quality of the service came to the fore. This also meant that the new managers had to know what they were doing and also to have more power and control over the resources. Crucial to improved organisational performance was the need for better NHS information.

There was however a problem in judging organisational performance. Though most of the managers had the best motives, few understood the 'product'[2] itself. Consequently, there was a lopsided emphasis on maintaining the efficiency of the health care delivery process as opposed to quality considerations (Strong and Robinson 1992). The health service therefore saw an increased demand for information. As Scrivens (1987) notes:

> The greed of the NHS for information has grown rapidly in the last decade because of increased pressures from the central government to increase the accountability of the service in its use of public money, to rationalise its resource allocation procedures and to maximise value for money. Recent changes in the management style of the NHS towards general management have increased further the desire for more information about the running of the health care service. The information needs of the NHS are closely related to its concerns about limited resources, increased demand for services and a lack of management in the past (p147).

In response to the increased need for information at different levels in the NHS, the NHS Management Executive (NHS-ME) formed the Information Management Group (IMG). In addition an Information Management and Technology (IM&T) strategy was developed. The purpose of the strategy has been to assist the NHS-ME to achieve the aim of creating a better health service for the nation. The business goal of the NHS-ME forms the basis of the IM&T strategy. In pursuing these goals the strategy aims to create a better health service in the following three ways (NHS Information Management Group 1992b; p 4):

1. Ensuring that services are of the highest quality and responsive to the needs and wishes of patients.
2. Ensuring that health services are effectively targeted so as to improve the health of local populations.
3. Improving the efficiency of the services so that as great a volume of well targeted effective services as possible is provided from available resources.

The Information Management Group considers that the IM&T strategy will help in realising the strategic vision of the NHS which is to support better care and communication. The emphasis therefore is to develop such an environment, where staff use information regularly in the course of providing services. Furthermore the environment should facilitate the sharing of information smoothly, effectively and securely. If such a sub-culture develops, the NHS will see enhanced quality, responsiveness, targeting and efficiency of its healthcare service.

This vision is guided by five key principles. First, information will be person-based, where the system will hold healthcare records for each individual. These can then be referenced by an individual's NHS number. Second, systems may be integrated so that data entered once can be made available to other designated NHS systems. Third, information will be derived from operational systems. This means that there will be a marginal need to establish new systems so as to capture information specifically for management purposes. Fourth, information will be secure and confidential and be made available on a need to know basis to those who are authorised to have it. Fifth, information will be shared across the NHS through a NHS-wide network that will facilitate communication across the service.

All strategic initiatives of the Information Management Group are based on these five core principles. It is envisaged that such initiatives can be realised through specific projects. The current emphasis of the Information Management Group has been specifically to target purchasers and providers of the health services. The 'Developing Information Systems for Purchasers' (DISP) project is a typical example where effort is made to identify business processes of various purchasers and build information systems around them. A parallel effort has been made to analyse the activities of the general practice. This provides a basis for setting standards with respect to computer systems used by GPs. On the providers side, two project initiatives have been under way. First is the 'Community Information Systems for Providers' (CISP) project, solely targeted at community providers. Second is the 'Hospital Information Support Systems' (HISS) project, which explores ways of developing integrated computer systems within hospital environments. The information management initiative of the Hospital Trust discussed in this chapter, under the CISP umbrella.

The Information Management Group considers that in order to support the information systems projects and to facilitate efficient communication and processing of information, a common information management and technology infrastructure is needed. In this regard various measures have been taken. There is specific interest in developing nationally-linked population registers and designing a new format for the NHS numbers. Furthermore there are plans to have a NHS-wide network. The networked environment will support an electronic thesaurus of coded clinical terms and groupings. Although the Information Management Group has set out an overall strategy for information management, it believes that the choice of systems will be based on local priorities and resources. However guidance on user requirements, procurement and quality standards will be provided.

The responsibility for requirements analysis has been devolved to individual units, but the Information Management Group has imposed some strategic thrust on developing computer based systems in the NHS. One such thrust area is the NHS Data Model. The main objective of the Data Model is to define the meanings and relationships between all items of data that are necessary in describing the operations of the units. The Data Model is based on the presumption that organisations share common objectives which can be clearly defined. The use of computers would then lead to an efficient health care delivery process. Such a notion bears close affinity to 'systems rationalism' as described by Kling (1980). Information Management Group describes the basic assumptions of the Data Model as follows:

> Indeed, once the aims and objectives of an organisation have been clarified, its functions delineated and the level of quality required for its outputs and outcomes established, the information necessary to support those aims, objectives and functions becomes readily apparent. Thus the proper identification of information requirements is dependent on the existence of clear service objectives and plans (NHS Information Management Group 1987; p5).

With regard to the use of information by managers, it is envisaged that a massive culture change with respect to information is required. According to IMG, this would necessitate the development of sound, objective and quantifiable measures for managerial activities. Such quantifiable attributes would provide a basis for developing a sense of ownership regarding information. These measures are also reflected in the policy considerations for protecting the flow of information within the NHS (NHS Information Management Group 1992a).

The Hospital Trust, which is the focus of this study operated in this ever-changing turbulent environment. The next section discusses the organisational setting of the Trust. It sketches out the core business activities and the manner in which these have been affected by the wider contextual changes.

4.2.2 The Hospital Trust

The Hospital Trust is a specialist one which currently provides services to approximately 1,500 people with learning disabilities. Although at present about 9,000 people feature on the District registers in the Trust catchment area, it is envisaged that between 14,000 and 17,000 people from the catchment population could be receiving services. These services are provided through three large hospitals. In the future, the Trust plans to rationalise these sites and services, and introduce a geographically dispersed, community-based health service.

Organisational structures

Health services to people with learning disability within the catchment area are provided through the 'Community Mental Handicap Teams'. These Teams show variation in orientation, depending on whether they are run with a social services orientation or health service orientation. The Teams also vary significantly in their composition; some lack members from basic disciplines, such as psychology and nursing, whilst others benefit from a good multidisciplinary staff complement. There are eight districts within which these Teams operate. The major part of the Hospital Trust's 'business' comes from the districts.

In providing services, the Hospital Trust has adopted the model of systematic monitoring, a single line of command and an integrated structure. It is evolving towards being an organisation which is run by generalists rather than specialists. As a consequence, there is a move towards developing hybrid staff members who know something of everyone's job. Such hybrid staff members are developed under five different directorates, viz. Nursing, Finance, Service Development, Medical and Human Resources.

The five directorates manage the health care delivery process through mutual adjustments across departments and divisions and direct supervision within specified functions. Some of the work practices at the service delivery level have been standardised and routinised; consequently, it has become relatively easy to monitor them. The process of therapeutic monitoring for instance is a standardised process, where drug prescriptions are checked for their compliance to very strict formal rules. However, much depends on informal communication among specialisms which helps in achieving co-ordination of work. Within the particular specialisms of nursing and medical, the prevalent ethos is that 'knowledge develops as the work unfolds'. So the success of a diagnosis or a treatment plan of a patient is largely dependent upon the ability of the specialists to adapt to each other. However, within each speciality, there is a significant element of direct supervision. A consultant doctor, for example, directly supervises the registrars and senior registrars.

The health care delivery process

The ultimate objective of the administrators of the Hospital Trust is to help people move from hospitals into the community. In doing so the emphasis is to provide the best possible services to people who come to stay in the hospitals for short periods of time before being relocated into the community. In providing these services, the administration aims to develop and manage high quality specialist health care.

The health care delivery process is viewed as a dynamic system where people with mental health problems enter the hospital, are offered treatment and are discharged into the community (figure 4.1). The emphasis is to encourage patients to stay in the community. The health care professionals consider the advantages of this to be twofold. First, the patients are able to experience and live in a natural environment. Second, the overhead costs of a hospital are substantially reduced. Thus a concerted effort is made to treat the traditional 'long-stay' patients in the community. They are only admitted to a hospital if their condition deteriorates or when they need urgent specialist medical attention. Consequently, most of the patients of the Hospital Trust are being transformed into 'short-stay' patients.

Health care is provided through a 'service specification', which describes a service that is available for use by one or more clients. A service is made up of a number of elements called 'care packages'. A number of service specifications may have care packages which are common to them. The service specifications are specified in the contracts agreed between the purchasers and the providers. The Hospital Trust views the health service as a menu in a restaurant with each dish being a care package. Dishes are chosen for customers (i.e. the care packages) to make up their meal (i.e. the service package). When a client is referred to the Trust, a needs assessment is done and an individual care plan is developed (figure 4.1). The needs assessment and the subsequent care plan implementation is realised by a multidisciplinary team constituted of nurses, physiotherapists, dieticians, doctors, etc. The Hospital Trust model for service planning considers multidisciplinary teams as central to the success of the health care delivery process.

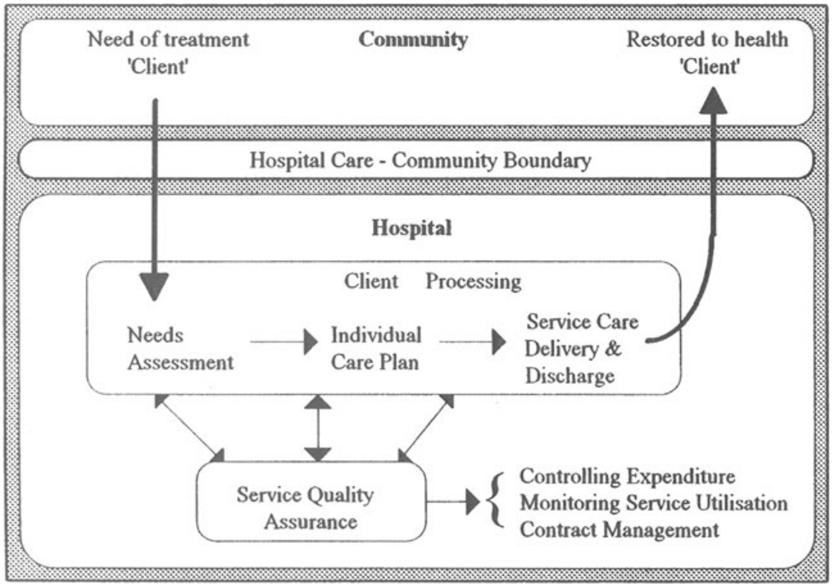


Figure 4.1 The health care delivery process of the Hospital Trust as envisaged by the management

A key problem with health care delivery is the timely availability of information. This was particularly the case in the Hospital Trust. A computer based information system was seen as a means of filling this information gap. It was thought that such a system would not only help the Trust to adapt to the macro environment (where there is an increased pressure on the Trust to provide precise information on its activities), but also to add value to the health care delivery process. With respect to the recent changes in the health services, the traditional health care management system had certain shortcomings. For instance, it was not possible to give due consideration to isolated 'encounters' which could subsequently be consolidated into health plans. It was also not possible to perform audits and assess the effectiveness of resources used. In response to such criticisms a typical integrated information system at this NHS Trust would incorporate care planning functionality in itself. Furthermore, it would also allow case mix management and have clinical audit functionality. Such a system would help the Trust to adapt better to the existing environment. This facilitates the meeting of demands by purchasers to provide information for assessing the quality and effectiveness of services delivered. Such information can be drawn through a process of constant monitoring of care delivery, recording of assessment details and measurement of outcomes. This logic formed the basis of system development activities at the Hospital Trust.

4.2.3 The IT infrastructure

In devising an information technology infrastructure strategy for CIS, the following business objectives had been considered:

- To provide a general purpose 'office systems' facility which would include word processing, shared printing, etc. In the near future an electronic mail system may also be implemented.
- To facilitate the electronic exchange of information with entities outside the Hospital Trust. Specific exchanges would be with the purchasers for managing contracts, various authorisations and referrals. This is going to evolve into a key function, since the Hospital Trust serves a large number of purchasers throughout the UK and is a specialist provider in certain disciplines.
- To send medical statistics to the Department of Health.
- To continue supporting existing systems.
- To ensure that new systems can be supported from a central location.
- To provide an adequate level of security so as to protect:
  - The Hospital Trust IT systems from intruders within the Trust premises.

- The Hospital Trust IT systems from unauthorised access by those outside the Trust.
- Other NHS networks from unauthorised access from within the Hospital Trust.

These requirements are being met by developing an integrated information system that is supported by Sun's 600 MP series UNIX server running Solaris 2.0 operating system as a technical core. This model was chosen after considering the processing requirements and minimum memory and storage necessary to support CIS running an Oracle relational database in a client-server mode. In order to facilitate effective communication, the infrastructure includes local area networks (Ethernet) at each hospital[3]. These will connect to the CIS database server with fibre optic links where appropriate. It is expected that some workstations will reside at community based sites and will have a facility to dial-in into CIS across normal telephone lines or via an ISDN link.

The Hospital Trust does not experience any 'legacy system' problems. The organisation did not have an integrated system to support its operations, though some work was done on stand-alone Apple Macintosh workstations, especially in the planning department. The personnel payroll system and the finance system were however run by McDonnell Douglas and GL Millennium (ICL mainframe) respectively. The clinical functions made minimal use of these systems and there was a wide variance in their use of computer based systems. Although the administrators wanted to build upon their existing knowledge of Macintosh products, they recognised the need to provide compatibility with IBM PCs. It was envisaged that the local area network needs of CIS would be met by an Ethernet LAN running at 10 Mbps. A local UNIX host at the sites would act as a file server for each LAN. TCP/IP protocol would be used with support from SQL*Net. Though CIS would not be available for access from external systems immediate-ly, the Novell/Network Designers X.25 gateway was considered to meet the future needs.

A fully operational CIS will have three servers which will hold a database of clients at each of the three hospitals[4]. The Unix server at one of the hospitals would hold data on clients of community service points. If there is a workstation connected to a local area network, all the data will be held on a Unix database server rather than on the workstation. In case a workstation is not connected to a LAN, but the connection is via a dial-up link, the local data will be held in an Oracle database on the workstation's hard disk.

Security

CIS is designed to process data of varying degrees of sensitivity. Though some of the information will be available publicly, most is extremely sensitive. This includes medical conditions of clients, drug prescriptions, their offences, convictions and other special needs. A breach in security could not only result in extreme embarrassment to the Trust and the individual but also have detrimental effect on the treatment plans. A typical unauthorised access could result in loss in integrity of the data or even its misinterpretation. Depending upon the level of reliance on the system by staff, incorrect information could even lead to the death of an individual.

Based on the risk assessment done for the CIS system, the administrators and the system developers found five areas of particular concern[5]:

- unavailability of essential client-care information, particularly for clients receiving acute services.
- loss of integrity of critical client-care information.
- loss or damage to critical components, including the threat of arson.
- theft of hardware containing sensitive client information in the community.
- errors by staff (operators, system administrators, etc.) could affect the security of the system.

A threat that could lead to any of the above is considered as 'high risk' for CIS. Based on these risks the systems designers proposed a risk assessment grid which would facilitate them in their systems analysis and design process (table 4.1). Accordingly, risks are classified into three categories: high, medium and low. These categories determine the criticality of a particular threat or vulnerability around which countermeasures are built.

In developing a secure CIS, countermeasures are split into two categories: technical and non-technical. The method of selection of countermeasures in these two categories is based on the level of risk. An appropriate level of risk is identified by calculating the value of information, software and hardware. A method for assessing the value of information is however not detailed. The technical countermeasures for CIS include logical access controls, resource controls, audit trails, database security, input/output controls and communication security. Logical access control operates at two levels, one for the PCs and the second for the network. The PC and network access control requirements comply with the recommendations of the NHS Information Management Group. These include procedures for establishing and changing passwords, the use of one-way encryption algorithms, mechanisms for updating user identities, time stamping, restricting the number of log-ons, automatic 'locking' of the PCs if left unattended and the use of dumb terminals. Having ensured the access of authorised users into CIS, there are the resource controls. Such controls restrict each user only to the programs, data, and system resources that are strictly required for the job function. Resource controls operate at the level of the PCs, network and individual applications. One very important issue in controlling resources is that of negotiating access levels, rights and obligations. Although there is a policy for the traditional paper based systems, its use has been determined by the prevalent norm structures in the organisation. Since CIS development is based on SSADM, the existing policy and procedures are being automated. The Hospital Trust administrators and the system designers have not however given this issue serious thought[6].

Table. 4.1 Summary of threat categories considered when assessing the security of CIS

	Confidentiality	Integrity	Availability
Acts of God	Low risk	Low risk	High risk
Deliberate threats from outsiders	High risk of hackers and theft	High risk of client's data being modified	High risk of wilful damage; Medium risk because of unauthorised access
Deliberate threats from staff	Low risk of unauthorised access	Medium risk of data being modified	Low risk of wilful damage
IT equipment failures	Low risk	Low risk	Medium risk because of equipment failure
Errors by staff	Low risk of accidental disclosure	Medium risk	Medium risk

Controls such as user validation, limit and range checking are used at the level of inputting and outputting data. All output reports show data changes and control totals for each transaction. In addition, controlled reorganisation and logical restructuring facilities for the database help in maintaining database integrity. Similarly, adequate protection is built into the LANs. Resource control, access management and input/output controls can only restrict access and monitor the users. In case a security breach occurs, there is a need for an audit trail that will help in the investigations. CIS has such audit capabilities, both at the PC operating system level as well as the application and database level.

The non-technical controls for CIS have not been clearly specified. The security documents and the analysis done by outside consultants presents extended lists of possible security organisations. The need for a security policy and a security awareness programme is stressed. Personnel and physical security issues are also touched upon. The Hospital Trust management has not taken adequate steps in this regard. This supports the contention (see section 3.3.3) that the Hospital Trust managers believe that security can be incorporated into CIS by considering the technical controls alone. In the following section, the detailed findings of the empirical study show that this may not be the case. Since the 'softer' issues have largely been ignored, the probability of occurrence of adverse events is great.

4.3 The case study

The previous section of this chapter specified the wider context in which the Hospital Trust was operating. The management operations and the IT infrastructure were also explained. This section uses the framework developed in chapter 3 to analyse the operations at the Hospital Trust. The focus of the analysis is on interpreting the management of information system security. The analysis is based on table 3.1 and takes us through the most generic human and cultural aspects to the more specific issues related to form and means. This allows us to comment on the implications for the security of information systems in organisations.

4.3.1 Analysis of the 'business world'

The analysis of the 'business world' allows us to comment on the high level issues relevant to an organisation, viz. the relationship of the purpose of the organisation to the manner in which information technology is used. This sheds light on the implications for the security of information systems. In analysing the business world of the Hospital Trust, three distinct stakeholders can be identified: the clinicians, the nurses and the administrators.

Organisation of the three groups

The Hospital Trust has experienced significant changes in the way in which the three 'specialist' groups are organised. Traditionally, in the pre-internal market era, the doctors were a dominating force. This was by virtue of their clinical expertise, and practically nothing used to happen without the consent of the Consultant Doctors. Major hospital decisions were generally initiated and executed by them. The doctors' expertise prevailed because of their professional attainment. There-fore they drew power from the formal authority vested in the same role. At a formal level, however, there existed a 'triumvirate' arrangement where a senior consultant doctor, a senior nurse and a senior administrator took formal responsibility. However, the senior doctor invariably would exercise influence over the other two members of the team. Consequently the doctor, generally of a consultant level, emerged as clear top decision maker.

Besides the system of expertise, the doctors dominated because of two other factors. First was the system of authority, which gave legitimate power (or formal power) to the role. Second was the system of politics. The system of politics generally operates to displace legitimate power (Mintzberg 1983a). However, since authority and expertise lay with the same role, the system of politics further strengthened it. Thus, because of the operation of all these systems, the role exerted tremendous influence. With the changes at the national level, hospitals were amalgamated into Trusts, being headed by a chief executive. This was also the situation at the Hospital Trust. In the Trust a senior doctor has now assumed the role of a medical director and a senior nurse that of a nursing director. The role of the directors is to advise the chief executive on the various top management decisions, but the ultimate authority rests with the chief executive (figure 4.2).

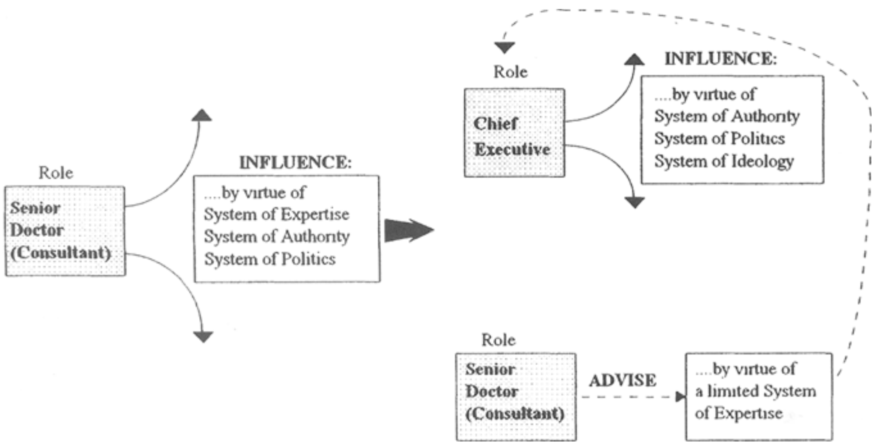


Figure 4.2 Top management and the changing role

The Hospital Trust doctors today experience increased pressure on their authority and expertise within the Trust environment. Traditionally, because they were experts in their fields, they were allowed considerable discretion in performing their tasks. This meant that most hospital work came under their direct control. Though an administrative hierarchy existed in the hospital, it had to surrender a lot of power to this elite group. The hospital functions were conducted more by mutual adjustment and less by formal bureaucratic rules. Work was carried out in small teams, members of which used to change over a period of time[7]. Different Consultants were in charge of different wards, their work being co-ordinated informally.

In the new set-up, the former authority and power of the doctors has now formally been placed in the hands of the Chief Executives. They also hold all the budget strings. Consequently, the system of expertise that gave tremendous power to the doctors is also diminishing. A concerted effort is being made by the Hospital Trust administrators to minimise the role of doctors even in the health care delivery process. The formation of multidisciplinary teams and attempts to capture the knowledge of doctors in the integrated computer based information systems are steps in that direction. The success or failure of these efforts is subject to debate, but such actions mark a trend towards a situation where the chief executive wields a lot of power and authority and is able to promote his ideologies in the Hospital Trust. Such political considerations will be discussed later in section 4.3.2.

Expectations, obligations and the value system

In this period where structural changes have been induced into the management of the Hospital Trust, the expectations and obligations of various groups have dramatically changed. The present chief executive used to be a hospital manager in his earlier days. His duties were more administrative than managerial. Although he used to be a member of the triumvirate that took major decisions, his role was limited. Now, in his present position as a chief executive he has developed a system of influence around himself. This gives him informal and formal power, bureaucratic control and legitimate authority. Evidently the structures of power have shifted. These have also affected the structures of authority and responsibility. Discussions with different people in the organisation revealed patterns of behaviour that were in tune with the chief executive's system of ideology. As one consultant doctor put it "...he does not like people driving big cars", so most of his close associates do not. Being at the top of the organisation has given the chief executive a unique opportunity to practise and promote his own belief system. This system is rooted in his social services background. Another doctor observed that people from the social services do not pay much attention to the way they dress. This is in contrast to the prevalent norms in the medical profession. Thus it becomes evident that the new hierarchical system in the Hospital Trust has dramatically changed the expectations and obligations of the former administrators and other stakeholders. Most look up to the value system promoted by the Chief Executive. The gap between the clinicians and the administrators has also widened. The doctors still consider themselves to be an elite group, culturally dissimilar to the managers. Managers on the other hand no longer consider themselves to be doing petty administrative jobs, but call themselves thinkers, planners and symbolic workers. Their level of expectation has also risen, morale has increased and their obligations have changed. They no longer expected themselves to provide support to the core business of providing health care. Rather they consider themselves to be key players who strive to maintain the efficiency in providing such services.

The nurses took a very different stance from that of the doctors and the managers. Discussions with them revealed significant detachment from the organisation's corporate goals and objectives as compared to top and middle level managers. One nurse, a ward manager, was no doubt concerned with the actual survival and growth of the organisation but was less worried regarding factors such as cost justification of CIS, content of management information generated, competitive advantage of the Hospital Trust as a result of CIS, the benefits realisation of the project and the power and politics involved. Such an attitude can be analysed in relation to Maslow's motivational theory and studies on managerial motivation by Cummings and ElSalmi (1968). Both these researchers feel that the higher the manager in the organisational hierarchy, the stronger is the commitment to the goals and objectives and eventually the survival of the organisation. A person moving up the hierarchy, who has been appropriately rewarded and sees more rewards with each promotion, has a vested interest in seeing the survival of the organisation. Cummings and ElSalmi also note that:

> high-level managers ... express more satisfaction in their jobs and greater fulfilment of their needs for autonomy and self-actualisation than do those at lower levels; the jobs of the latter tend to focus on the security and social needs.

Some level of commitment exists at the lower managerial level as well. Lower level managers feel satisfied in leaving behind some operational tasks to achieve a new status. Individuals at this level seem to have a weak identification with the organisation. Nurses in one of the Wards in the Hospital Trust typically belong to this category. It became evident from discussions with the ward manager and other nurses that there was a conflict in the value system as compared to that of the middle level managers. The middle level managers were just concerned with the success of CIS, the Hospital Trust and the organisational mission. Organisational ideology is not a strong force among the nurses; however, professional ideology – the belief in the profession and its norms – certainly is. The only usefulness of CIS for the nurses was to cut down paper-work, remove duplication and therefore save time. They felt that the time saved could be used in professional development of the nurses and in providing better care to the patients[8]. This level of detachment of the nurses can be explained in terms of the high intrinsic satisfaction that the nurses obtain in serving the patients. Thus a conflict between organisational goals and professional ethics has crept in.

Consequences for the information system and security

The analysis so far has revealed conflicting ideologies, preconceptions and objectives of the dominant players within the Hospital Trust. It is interesting to evaluate the consequences of top level policy and the mission statement on the different levels of the organisation. The success of an information system and of efforts to maintain its security are largely dependent on the policy and the vision of the organisation. Any viable organisation needs a vision, a purpose, so as to compete in a hostile world. The need for such a vision is all the more greater for the Hospital Trust since it operates in a highly volatile environment. Besides a corporate vision, the Trust also needs an information systems policy, since it aspires to make information technology central to all its tasks. A concurrent need for a security policy is also obvious from the discussion in section 4.2.3.

At a business level a corporate policy and a statement of purpose did exist in the Hospital Trust. The statement of purpose clearly states that the Trust is in the business of providing services to people with learning disabilities. On the basis of its corporate vision, the Trust has established other objectives which guide the organisation in its operations (figure 4.3). In order to implement successfully its objectives, the Trust has established the role of a planning manager whose main task is to realise the business objectives. The planning manager recognises the importance of the availability of timely and correct information as the key success factor. Therefore, the development of a computer based information system was considered to be crucial in achieving the corporate objectives.

Drawing on the work by Pettigrew (1985) and Walsham (1993), corporate strategies and organisational purposes can be analysed on the basis of the content, the context and the process of change. The major element of the Trust's corporate strategy is the 'vision for change'. Interviews with top management revealed that they had expectations of CIS (which is also considered as a tactical device) to produce an improvement in the way in which administrative and clinical work was done. This improvement ranged from increasing the efficiency and effectiveness of patient administration functions to providing clinical decision support and management control. With new legislation in place, the wider contextual factors of the Trust had considerably changed and the management saw the new information system as a means to succeed in the changed environment. The content of this broad vision appears to make sense, but problems emerge when the management's attitude, the norms of management control and the process of change are considered.

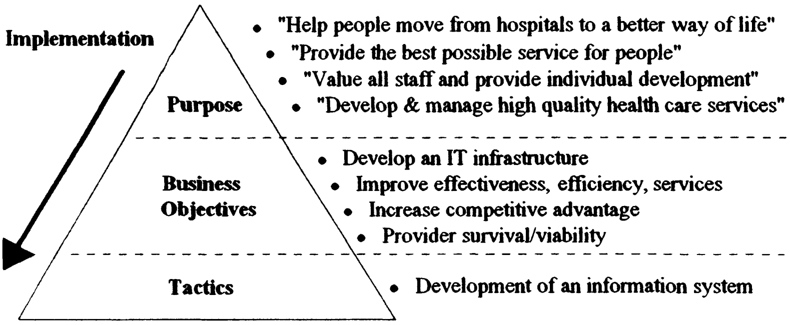

Implementation
Purpose
• "Help people move from hospitals to a better way of life"
• "Provide the best possible service for people"
• "Value all staff and provide individual development"
• "Develop & manage high quality health care services"
Business Objectives
• Develop an IT infrastructure
• Improve effectiveness, efficiency, services
• Increase competitive advantage
• Provider survival/viability
Tactics
• Development of an information system

Figure 4.3 From corporate purpose to tactics in the Hospital Trust: the management's model

The top management of the Hospital Trust has solely focused on achieving its business objectives. They saw their objectives being achieved through the development of an IT infrastructure. The 'efficiency' and 'effectiveness' objectives were coupled with increased management control. This has major consequences. It is a narrow view limiting the scope of autonomous action at all levels. By using the information system for exercising management control and making the work environment transparent, the management was creating resistance to change. These actions go against the primary business objectives of increasing efficiency. Such outcomes have also been noted elsewhere (see Walsham 1993). Similar to the observations made by Han (1991), the NHS Trust faces problems of deskilling work and decreased effectiveness owing to a move towards increasing control.

The computer based information system may have been considered as a tactical ploy, but its objectives should complement the vision and the business objectives. CIS is being sold in the organisation as a tool to help in improving effectiveness and efficiency of the health care delivery process. It is perceived as a means to reduce paper-work, decrease duplication and offer competitive advantage in a highly market oriented health service. However, the basic architecture of CIS supports neither the IT infrastructure objectives nor the corporate purpose. The planning manager and the information manager consider the computerised 'individual care plans' as the unique selling points of CIS. It may be recalled here that there are two kinds of individual care plans: one for long stay patients and the other for short stay ones. Since the needs of these two classes of patients are very different, so are the individual care plans. CIS is solely concerned with individual care plans for the long stay patients. This would have been fine had the Trust been operating in the early 1980s. The needs of today have changed because of internal market mechanisms. Although the corporate philosophy of the Trust seems to be in tune with the changes[9], the strategic objectives of CIS are in direct conflict. The CIS project has been modelled around one particular ward. Interestingly, this was a long stay ward due to be closed permanently. Thus it can be said that the design of CIS is out of tune with the real world situation. Even if it is presumed that CIS would function properly in the years to come, the security aspects have not been considered at all. The Hospital Trust not only lacks a proper IT policy but there is no information systems security policy. The outside consultants have however used the NHS Information Management Group's guidelines for security as a given set to work from.

In an ideal situation, corporate objectives, information system strategy and security planning should complement each other. However, in the case of the Hospital Trust, the security planning issues have not been stated explicitly (except generic recommendations by outside consultants – see section 4.2.3). The Hospital Trust case presents a situation where not only is there a lack of integrity between the business objectives and the way in which technology was introduced, but also there is no strategy for preventing the occurrence of negative events.

Although the literature recognises the importance of security policies, the manner in which these are developed is rather restrictive. In light of the Burrell and Morgan categorisation (chapter 2), such policy initiatives cannot only be categorised as functionalist, but also as highly technology oriented. The NHS Information Management Group security policy guidelines, for example, presume that the corporate objectives exist and that they adequately support the information systems strategy. Hence it is believed that security can be achieved if certain logically discrete steps are taken. It can be interpreted from the discussion in the previous pages that since there is rancour and discordance in the expectations and obligations of different roles, the presumptions with respect to developing security policies are flawed.

Another issue worth mentioning here relates to the commitment of the top management. Most security policy documents (including those of the NHS-Management Executive) stress that top management commitment should be gained while designing and developing security policies. At least in the case of the Hospital Trust this was not achieved. Whatever rudimentary guidelines that existed, came from the system analysts. Discussions with top management revealed that either they were not aware of the consequences of adverse events or they did not regard the issue to be important. Even though the top management (the Chief Executive and the other Directors) were not involved with the security issues of CIS, they should be aware of the directors' fiduciary duties (for details see Ardis and Comer 1989).

The next section considers, in addition to some of the issues raised above, the cultural and political significance of the CIS project. In doing so it considers the importance of looking at the security of the whole organisational edifice, rather than of just the technical infrastructure.

4.3.2 Analysis of the pragmatic aspects

In implementing the integrated information system, the Hospital Trust has regarded information technology as the main catalyst for change. It has relied on IT for successful implementation of the concepts which add value to the health care delivery process and consequently which change the culture of the organisation. Little consideration has been given to the existing ways of doing work. Thus there has been an over-reliance on the functionality of the system in order to reap information technology benefits. As a result the Trust has seen a massive reorganisation of its ways of working. The adoption of new management, new structures and new styles of teamwork have come to the forefront. In achieving its objectives the management of the Trust has emphasised developing hybrid staff members who know something of everyone's job. This change process has evidently affected the organisational norm structures and also has consequences for the manner in which the security of information systems is considered. These elements are elaborated and discussed in this section.

The security culture

The Hospital Trust has relied on information technology to implement the organisational changes. It is very easy for a technologist to forget the social context which justifies the very use of technology. It is often the case that problem domains are isolated from the context and solutions are developed without consideration of any environmental influences. This has consequences at two levels: one, computer based information systems do not serve their original objectives and two, there are implications for the security of such systems. The second point needs some clarification. Computer systems do not become vulnerable only because adequate technical controls have not been implemented, but because there is a discordance between the organisational vision, its policy, the formal systems and the technical structures. A computer scientist would only consider security after a system has been implemented, whereas such concerns have to be addressed even before a system has been conceived. Most of the existing literature on security takes the former stance. Even the underlying principles of the Orange Book consider security of systems as a purely technical matter. The TCSEC ignore the informal aspects of the evaluation process. Even when considering 'verified protection' (class A1), the emphasis is to verify security controls against the formal model of the security policy. The whole process is an 'afterthought'. Baskerville (1988) recognised the shortcomings and suggested that security should be considered at the logical design phase. Similar suggestion have come from elsewhere as well, where it has been suggested that there should be a class in TCSEC which goes beyond A1 verified designs (Chokhani 1992). This again is a highly structured way of looking at security. What in fact is needed is to consider security at the requirements analysis stage of a computer based information systems development process. By doing so we tend to address the integrity concerns of an organisation which help in maintaining consistency and coherence between different organisational functions. This can only be achieved if an organisation facilitates the development of a security culture. In considering security of systems from this point of view we are implicitly linking security design with the quality of information systems developmental activities and good requirements analysis for the design of information systems.

Security culture is the totality of patterns of behaviour in an organisation that contribute to the protection of information of all kinds. The prevalence of a security culture acts as a glue that binds together the actions of different stakeholders in an organisation. If such a culture does not exist, there may be problems of not only maintaining the integrity of the whole organisation but also the protection mechanisms of the technical systems would be threatened. It is after all the people who make the control mechanisms operational. Security failures, more often than not, can be explained by the breakdown of communications. Because we tend to view communication as only when we speak to different people, writing reports, holding meetings, etc., we ignore the non-verbal aspects of the communication. Analysis of the culture and our concerted efforts to inculcate a sub-culture for security is the first step in the remedial process.

Culture is shared and facilitates mutual understanding, but can only be understood in terms of many subtle and silent messages. Therefore culture can be studied by analysing the communication processes. This also means that culturally determined patterns of behaviour are messages that can be communicated. Hall (1959) regards culture as communication and communication as culture. Consequently, culture is concerned more with messages than with the manner in which they are controlled.

Implications for information system security

The Hospital Trust's CIS is a typical example where the computer based system has acted as a message system signifying the underlying patterns of behaviour of different groups. To illustrate this let us take the issue of controlling a staff member session schedule. Controlling such a schedule poses a complex managerial situation, especially when a computer based system is used to carry out the task. The staff scheduling module is not just another duty rostering mechanism within CIS, it gives a graphical display of the 'free' and 'busy' times of each staff member thus allowing the service point manager to plan the use of staff effectively.

Prior to CIS, a nurse would typically allocate (book) time for a particular activity such as a therapy session. Subsequently, this role would be held responsible for the successful conduct and delivery of the service. However, with the implementation of a computer based information system the situation has changed. Not only would the nurse be held responsible for the tasks, but the time allocations, free times, number of sessions per day/week, etc., would all be monitored. The computer has indeed emerged as a new supervisor.

The system analysts and the designers have failed to recognise the subtleties in the behavioural patterns of the nurses. Consequently the formally designated procedures and structures for the technical system do not signify the meanings and intentions of the users and the staff who are being controlled. Reasons for this can be attributed to poor system specification. Ideally, it should be the endeavour of the system analyst to relate the syntactic domain (i.e. the formalisable aspects of the problem) to the semantic domain (i.e. to ask the question: what would it mean in the real world?) giving due pragmatic considerations (i.e. to consider the cultural setting of the different roles). In other words, the analysts have just considered the *form* of the problem and not to the *content*. Such a design, which concentrates on the superficial aspects alone, not only leads to the development of systems that cause problems (e.g. decreased staff morale) but also lacks vigour. Therefore such projects are seldom abandoned.

The implementation of such a system has different communicative contents. In figure 4.4, the solid line represents the transmission of the actual signal from Role 'A' to Role 'B', allocating a specific task to the nurse. The transmission of the signal is an indication of a communication having taken place between the two roles. With the computer based information system in place, the communication takes place through the computer. Thus in net effect Role 'A' gets things done through the computer.

The transmission of the signal from Role 'A' to 'B' influences the attitude of Role 'B'. The complex situation posed by controlling a staff member session schedule through the use of a computer can only be understood in terms of differences between the formal communication used by machines and the natural language used by peopl. At this point it is interesting to consider the different modes in which people communicate. Ordinary communication between people (written or spoken) operates in any of the four modes: 'affective', 'denotative', 'ritual' and 'formal' (Morris 1964). The affective communication conveys judgements of value and thus plays upon a recipient's feelings while the denotative communication is based on facts and evidence. The ritual communication is used in our everyday discourse and uses words without reference. The formal communication employs signs as objects and is not intended to trigger any behavioural responses. All modes of communication operate simultaneously.

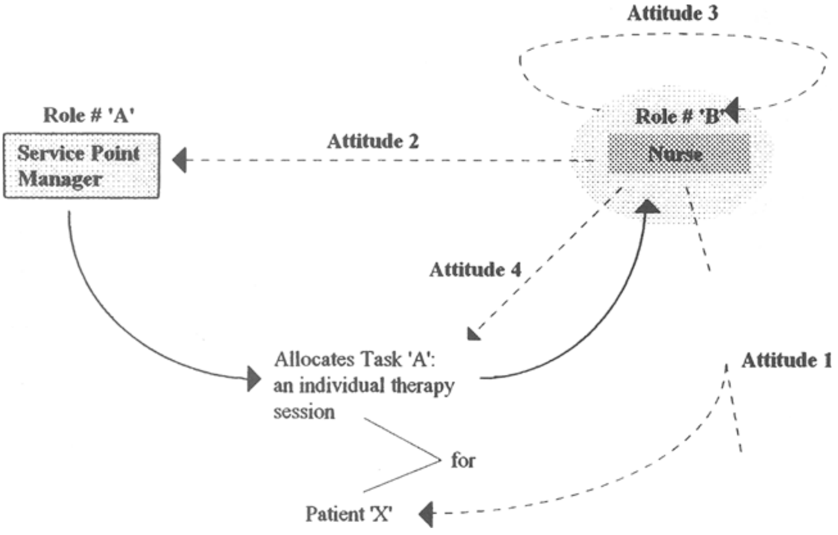


Figure 4.4 Emergent messages: attitudes signified by CIS

A distinction between the modes of communication is useful to evaluate the attitudes of Role 'B' towards 'A'. These attitudes can be classified as follows:

Attitude 1: By allocating a particular task, Role 'A' can influence Role 'B's attitude towards the subject being referred. Since in this context we are not considering mechanical tasks, the implication of this influence could be serious. The situation becomes far more complex when the incumbent of Role 'B' knows that the time spent with the patient would be closely monitored. This could adversely affect the very content of the therapy session. Thus in providing an 'effective' and an 'efficient' service, the management would in fact be sacrificing the quality.

Attitude 2: The attitude of Role 'B' towards Role 'A' would also be influenced. Role 'B' will have to adjust his attitude towards Role 'A'. This is especially so when a machine is used to control and co-ordinate the work and performance of Role 'B'. Such a situation is typical of superior–subordinate relationships.

Attitude 3: Less consciously, the whole context would influence the attitude of the persons themselves holding Role 'B'. Again the consequences could be serious. There would be problems with the self-confidence and morale of the individual. Rather than providing therapy to the patient, the Role 'B' incumbent would require some kind of help to cope with the situation.

Attitude 4: The attitude of Role 'B' towards the message itself is very interesting in the context of organisational change. Role 'A' perhaps unintentionally, but often deliberately, may convey some measure of confidence that should be placed in what is said. This communication act becomes far more complex when Role 'B' sees a computer as performing a supervisory task.

It becomes apparent that with the use of a computer based information system, the affective and the ritual modes of communication are marginalised. This has serious implications. A service point manager who does not achieve an emotional rapport with the nurse will be left with neat time allocations but may fail in motivating the nurse. This may eventually lead to potential negative events. On the contrary, a manager who establishes a rapport, can promote enthusiastic activity, however, this could be significantly curtailed because of the structure imposed by the computer system.

Analysis of the silent messages and the related security concerns

We have seen the manner in which the introduction of a computer based system affects the attitudes of different players in an organisation. In fact these are silent messages which help us in analysing the culture of an organisation and assess the implications for security of the organisations and their information systems. Based on the various categories of silent messages drawn from Hall (1959), table 4.2 summarises the interpretations from the silent messages (see appendix for a description of Hall's culture map).

When considering the implementation of CIS in the Hospital Trust, not all elements of Hall's culture map are of significance. Hence 'bisexuality' and 'play' streams are excluded. Analysis is conducted by considering actions within each cultural stream identified by Hall (1st column in table 4.2). Then the actions are analysed by considering their significance in other cultural areas of the organisation (2nd column in table 4.2). Finally, implications for security are interpreted (3rd column in table 4.2). Analysis is done by closely considering areas where the system has had a direct impact. Interpretations for security are drawn out by reflexive thinking and other material provided by different stakeholders within the Hospital Trust. An evaluation of each of the streams is described below. The complete analysis is presented in table 4.2.

Interaction. The introduction of CIS has introduced new communication patterns between junior nurses and managers. The computer has emerged as a supervisor. This has affected the patterns of interaction between different roles within the organisation – typically between doctors, nurses and managers. A change in the status and role of the nurses can also be observed. The introduction of CIS has taken away from the nurses the responsibility to manage their own time. Furthermore, since the individual care planning process has been computerised, the formal and the technical system tends to marginalise the role of doctors in needs assessment (in practice, however, this is not true). Hence the system is imposing new ways of doing work. The inability of the organisation to develop a shared vision and consensus about the shared patterns of behaviour has led to communication breakdowns. Employees are extremely unhappy and show resentment. Although the Hospital Trust has not experienced any serious negative events as yet, there is a high probability of such adversities in the future.

Association. CIS has changed the associations of individuals and groups within the organisation. The system has been introduced in a very authoritative manner. All concerned have to use it. This has severe 'organisational' and 'territoriality' implications. Typically managers are forcing a set of objectives on to the nurses and doctors who have to reconsider and align their ideas with the 'authoritarian' corporate objectives. Because of CIS and the aforementioned organisational implications, organisational culture is being fragmented – nurses and doctors show more allegiance to their professions than to the organisation. The mismatch between corporate objectives and professional practices is leading to divergent viewpoints. Hence there are concerns about developing and sustaining a security culture. It is important that the organisation has a vision for security, otherwise corporate policies and procedures become difficult to be realised.

Subsistence. CIS is adversely affecting the subsistence issues related to different groups. The introduction of the concept of a multidisciplinary team and its being formalised and automated raises concerns among different groups. There is a feeling in the organisation – among some nurses and managers – that

Table 4.2 Examples of silent messages conveyed at the Hospital Trust: interpreting the implication for security
(The categorisation is based on E.T. Hall's Primary Message Systems. Only relevant streams are shown, represented by numbers in the 1st column – the primary impacts. Numbers in the 2nd column are the cell numbers from the culture map – the secondary impacts.)

Direct organisational intervention through CIS	**Significance in other cultural areas of E T Hall's map**	**Implications for security**
(0) New communication pattern between junior nurses and managers for managing their time.	(00) Patterns of interaction between doctors, nurses and managers change. (01) Change in status and role of the nurses; their time is managed rather than their being made responsible.	Inability for an organisation to develop a shared vision and a consensus about the shared patterns of behaviour. This leads to communication breakdown. Employees are unhappy and show resentment: a security issue.
Computerised Individual Care Plans as the means of needs assessment.	(09) Imposition of a new way of doing work.	
(1) Introduction of an integrated system where all groups *have to* use the same system.	(11) Managers announce the purpose and objectives of the Trust. Other groups reconsider their own objectives in the light of the corporate objectives.	A mismatch between corporate objectives and professional codes of different groups leads to conflicting viewpoints. Therefore there are problems with having a *shared vision* and developing a security culture.
All activities will be monitored by the planning department.	(14) Different groups show allegiance to their professions rather than the organisation.	
(2) Hospital information more readily available – typically for budgeting.	(21) Consultants considered as an expensive resource. (22) More focus on costing 'activities'.	At the level of subsistence, a system should address the basic physical needs. Over-formalisation has led to incoherent objectives of different groups, leading to alienation. Business processes do not support overall vision.
The introduction of the concept of multidisciplinary teams and its being formalised and automated.	(21) 'Consultant is no longer a dictator.' (26) There is a feeling that nurses can do most of the doctors' work.	

(4) Systems are located at the point of service delivery. A WAN is to be installed spanning three hospitals and other out-reach service points.	(46) The learning process in service delivery encourages ownership of the system. (48) Ownership leads to responsibility structures that give protection to systems. (49) Rationalising of services.	The notion of ownership of systems and information reflects problems of authority and responsibility – a major security concern. Also a problem of having consistent territoriality (areas of operation) objectives.
(5) CIS provides comprehensive management information. Computerises the paper based system and is very structured.	(52) Misconceptions about well being of different groups. (54) Rigidity of CIS and inflexibility of planners hinders further developments; therefore new associations have emerged.	The purpose of an integrated system and of maintaining integrity and security is defeated when user's needs are not met. Some groups have considered independent advice on IT use. Defeats security policy objectives.
(6) CIS provides good interfaces and a training module.	(62) Reduces the learning time for user. (64) Learning is location independent.	Trade-off needed between ease of use and easy access into modules.
(8) Security provided at the level of password control and rudimentary risk analysis.	(81) Disruption of power structures. (88) Influence of varied interest groups perceived.	Only technical controls exist; no rules, training and awareness programme.
(9) CIS is to communicate with national systems. It is addressing new organisational forms.	(90) There are concerns for 'trusted' communications. (91) New skills depend on new professional and organisational networks.	Major security concern is of a hierarchical structure imposed by CIS (as well as the security structure) on to a very organic organisation.

a multidisciplinary team can limit the dictatorial role of the consultant doctor. However, in reality there are many expert decisions that only a qualified consultant doctor can make. Such a situation can potentially lead to rancour and conflict within an organisation. This may lead to a situation where a complex interplay among different factors may lead to the occurrence of some adverse consequences.

Territoriality/Location. CIS has created many artificial boundaries within the Hospital Trust. Such boundaries do not necessarily map on to the organisational structures. In such a situation there are concerns about the ownership of information and privacy of personal data. Problems with the ownership of systems and information reflects concerns about structures of authority and responsibility. Hence there are problems of having consistent territory objectives (i.e. areas of operation). Failure to come to grips with the territory issues can be detrimental to the organisation since there can be no accountability in the case of an incident.

Temporality/Time. CIS provides comprehensive management information and has computerised the paper-based system. Technically, the system is very sound in performing basic administrative tasks. However, with respect to clinical activities it is fairly restrictive and inappropriate. Hence it does not serve the needs of many users. In this regard the users have sought independent advice on information technology use. This defeats the core objective of any security policy.

Learning. CIS provides good training to someone who is unfamiliar with the core operations of the organisation. The users who feel that their needs have been met through CIS have to establish a trade-off between ease of use and access. The management of the Hospital Trust has not as yet resolved this issue. Although the system has been developed, access rights are *ad hoc* and largely based on an outdated paper-based system.

Defence/Security. CIS has identified different levels where password control needs to be established. However, since access rights among different roles have not been established, there are concerns about influences of different interest groups and disruption of power structures. This is an extremely important security issue and cannot be resolved on its own. Unless various operational, organisational and cultural issues are resolved, it may not be possible to come up with a solution.

Exploitation. CIS aspires to communicate with the national systems and address the needs of emergent organisational forms. As of now it appears that the organisation does not have the competence to manage such a complex task. More specifically, the structure of CIS is hierarchical, while the Hospital Trust and the national health services are evolving into a very organic form. This raises a number of security concerns – especially if a negative event takes place.

Discussion

An analysis of the silent messages conveyed when a new computer based information system is implemented allows us to predict the consequences for security. This means that many aspects of security are predominantly social in nature and care should be taken when cultural changes are introduced. This does not mean that all new systems should fit into the culture of an organisation, but a better understanding would facilitate a smoother implementation. It would also decrease the chances of adverse reactions on the part of the users that could possibly lead to security problems.

A review of the impact of direct organisational interventions (column 2) allows us to learn and adopt appropriate means for communicating intentions to people in an organisation. Only if a proper mode of communication is adopted and maintained can the chances of a weak security be minimised (column 3). There are three ways of communicating to people how to behave (Hall 1959). First is the formal mode, where no reasons are given and a person is told to do certain things under a certain set of circumstances. Formal statements direct a person's behaviour. The formal communication and learning process is supported by explicit rewards and punishments. However, too much formalism may be inappropriate when the environment is volatile and people have to react to changing conditions. This is a typical situation at the Hospital Trust where the environment is changing constantly and one set of rule structures becomes outdated very quickly. The structure of the health services within UK is at the present time being transformed from a highly hierarchical organisation to a predominantly organic one (see for example Loveridge 1992)[10]. CIS on the other hand imposes a strict structure. The security rules are also based on the notion of 'ownership of data', a concept that presupposes a strict hierarchical, bureaucratic and a mechanistic organisation. Hence there are problems of consistency between what is perceived to be the responsibility structure and what actually exists. This is discussed in detail in the following sections.

The second mode of communication is by informal example. It may never be possible to make explicit the communication of certain cultural patterns. In bringing about direct interventions into the management systems or in the introduction of new computer based systems, managers and systems analysts should appreciate many subtleties of behaviour. Failing to do so may result in non-conformity of purpose to the group norms, which may breed resentment. A disillusioned employee is a potential threat to an organisation. Some degree of support can be brought about by offering rewards and punishments. Only if the system designers of CIS understand the informal behavioural aspects of the various groups can they avoid the potential hazard of alienation and loss of trust of the employees.

The third form communication is technical. Here a reasoned and an analysed description of things is given. As a prerequisite, technical communication requires highly aware individuals who understand the content of the communication. In the case of the Hospital Trust, although most of the employees using CIS are highly educated, they are not aware of the benefits and drawbacks of using a computer based system. So, it can be concluded that the system developers and the planning department have not marketed the system properly to its employees. Moreover, it is not just the problem of good marketing; a 'product' can only be sold if it has been designed properly and fulfils the needs and wants of its customers. CIS fails on both these counts.

The next section analyses the Hospital Trust and CIS from a semantic point of view. It considers the semantic content of the communications and the structures of responsibility and draws out consequences for the security of the organisation.

4.3.3 Analysis of the semantic aspects

One of the common denominators in the successful management of computer based information systems has been the analysis of stakeholder[11] requirements. This is an important activity since it helps the analyst to develop a common consensus regarding the meaning of different activities. The relevance of doing so is further augmented when information and communication technologies are used to transmit information over wide and local area networks. Typically such networks attempt to link a wide range of stakeholders (e.g. General Practitioners, Hospitals, Pharmacies, Social Services) in different organisational settings (Dhillon and Backhouse 1996). Health informatic professionals have struggled with varying degrees of success to build systems which not only allow a free flow of information but also bring about a consensus in the meanings and intentions of different groups.

Organisational actions and emergent reactions

At this point it is interesting to evaluate the Hospital Trust's strategies from the perspective of the changing social context. The context may offer opportunities or threats. The UK NHS, however, is faced more with threats than opportunities. In recent years the Hospital Trust has seen an increased demand for health care. This has been a consequence of medical advances, demographic changes, new service developments and increased expectations. This increased demand has put pressure on the limited UK NHS resources. The problem has been further complicated because of tightening public expenditure constraints and privatisation. For the Hospital Trust there were many other threats as well. The financial position was not very healthy. It was even doubtful if full financial support could be given to the information system development project in the years to come. There were problems with the morale of the work force. The Trust was closing down a few hospitals and there was uncertainty among the junior nursing staff. The senior nurses and doctors were also displeased with the recent changes, both at the national and the Trust level. Within the Regional Health Authority (of which this Trust was a part), between 1990 and 1991 there was an eight-fold increase in the managerial staff. The national figures for 1989/90 and 1991/92 showed a 109% increase in the NHS expenditure on salaries for general and senior managers. As a result of this, the clinicians were not only unhappy with the dominance of the managerial cadres but also with the manner in which they were managing different aspects of the hospitals.

Discussions with professionals at different levels revealed that there was rancour and distrust towards the administrators. Commenting on the information systems infrastructure, the Hospital Trust pharmacy manager raised her voice and asked what use were computer systems that resulted in lowering the quality of their work. Ironically, the Hospital Trust pharmacy had a stand-alone computer based pharmacy system that was in operation since early 1980s. The system was totally scrapped by the planning department to make way for the new CIS. System development of CIS has been delayed and the Trust pharmacy had to revert back to the manual system dating back to the late 1970s. Such a sequence of events is a typical example of poor planning and co-ordination on the part of the planning department. These organisational actions have however been interpreted in different ways at different levels. The pharmacists, for example, resent having accepted the advice to scrap their earlier system. But on the other hand they had no choice. The information systems plan and the resultant changes were forced on them and as a result they had to get rid of their old system, revert to manual working and await the arrival of CIS. As a consequence of this, the pharmacists regard the administrators and managers as authoritarian and attempting to do too much in areas which are beyond their comprehension.

On the clinical front it is interesting to evaluate the relationship between the business objectives, established predominantly by the managers, and the clinical objectives. The comparison appears in table 4.3. The two sets of objectives are indicative of a dichotomy at the level of the inner organisational context and the process of implementation.

This dichotomy can be explained by considering the manner in which the Hospital Trust business objectives are being implemented. CIS is considered as a means to achieve their implementation. The realisation of the business objectives is a significant change in itself, and regarding CIS as a means of achieving them adds to the complexity. Table 4.3 matches the relevant clinical objectives with specific business strategies. A superficial comparison reveals that the cultural issues and the processes of cultural changes have been neglected in formulating the business objectives. There is a complete mismatch between the strategic vision as postulated by the management and the focus of the clinicians. This is partly because consideration has been given only to the formal benefits of the new management system. Therefore, new ways of doing things have been designed, keeping in view the formal computer based information system. Although the managers contend that CIS maps the existing manual system, it is not entirely the case. This has resulted in new ways of working that have introduced significant cultural changes. Interviews with the top management revealed that they in fact wanted to "change the culture of the organisation". Although bringing about cultural changes may be in the best interests of the Trust, managers need to take into account the various existing management practices. This was especially relevant in the case of the Trust, because there were different work constellations that lacked commonality in their goals. Moreover, a lack of coherence of purpose and the changing roles and responsibilities of individuals were alienating various members of the organisation.

Table 4.3 Matching business with clinical objectives

Business Strategy	Clinical Objectives
Develop an IT infrastructure	None
Improve efficiency, effectiveness and service quality	'Services should be based on individual client need' 'Services should not be designed around a hospital or bed based service'
Increase competitive advantage	'As far as possible services should be developed within the local Districts' 'Health expertise should be available as and when it is required and not as a constant element of people's lives'
Provider survival/viability	'There should be a mixed provider economy'

The analysis of the corporate strategy and its relationship to the management systems of the Hospital Trust reveals that the vision of tangible benefits was an important contributing factor in the introduction of information systems in the Trust. The decision to implement systems at the hospital and Trust level gave inadequate importance to the contextual aspects of the environment. Nevertheless the process of system implementation received much attention. Most of the managerial thrust has been on the content of the change. Such inferences have also been drawn in other case studies (e.g. Walsham 1993; Madon 1992; Dent 1992; Coombs and Cooper 1992). In relation to the new information system there has also been significant thrust on the content of the decision support system, which aids clinical decision making, and on monitoring the health care delivery process. Since a new system of this kind changes the way in which people work and interact, the analysis of the processual aspects becomes important. Furthermore, the whole change process takes place within the current organisational context which cuts across various sub-cultures. This draws attention to the study of various organisational contextual features. Failing to understand all these factors leads to the development of inappropriate management systems, requiring further development of new computer based information systems.

Various organisational sub-groups interpret such actions in different ways. The clinicians were the most sceptical. One consultant psychiatrist interpreted the management actions as part of an overall 'antipsychiatry movement'. He labelled the planning manager as being one of the proponents of this movement. In fact during the 1960s antipsychiatry became a popular cause. Books such as Szasz's *The myth of mental illness*, and films such as *One flew over the Cuckoo 's nest* appeared to challenge the concept of mental illness. He went on to say that the very design of CIS and the lack of importance being given to acute services for the mentally ill is a blatant example of the manager's attempts to undermine the utility of psychiatry. Citing examples related to the architecture of CIS, he stated that not one module of the system gives due importance to the clinical aspects of treating the mentally ill. Indeed the system places a lop-sided emphasis on providing services such as art therapy, music therapy, physiotherapy, speech therapy, etc. It is contended that the planners of CIS are out of tune with the developments in genetics, neurophysiology and neuropharmacology. Modern techniques such as brain imaging have actually brought psychiatry to the centre stage. There is now a greater understanding of the contributions of biological, psychological and sociological factors in the management of mental illness. One clinical director of the Hospital Trust felt that the managers were behaving as they were, more out of fear than because of their ideology. He said, "Managers do not want a total medical takeover." The Medical Director went a step further and considered "...human service organisations as organised anarchy". Therefore, according to him guidelines are needed that address the lack of governance. Compliance with such guidelines can only be instituted if there is a "lead medical figure on each side,.....with a manager's hat on". A resultant common theme emerging from the discussions with doctors is that problems of bad management, incoherent objectives and general inconsistency arise from a basic lack of knowledge and awareness of the clinical trade on the part of the managers.

The doctors considered all managerial actions to be seriously affecting the flow of information. They visualised a typical scenario relating to the consequences of misinterpretation of data. Consultants were worried because CIS did not go into the details that the doctors needed. Although they were responsible for the wards and the patients, increasingly they had less control over the manner in which the treatment was being provided. A doctor's diagnosis and case notes are stored on CIS. Traditionally the interpretation of these is made by individuals who have the knowledge and expertise to do so (i.e. the doctors). In the present climate, CIS encourages the non-medical staff (i.e. the nurses) to draw conclusions 'logically' from the system. There is a clear-cut threat of misinterpretation of data. Even though CIS incorporates all data integrity controls, their utility is jeopardised by the inherent threat of misinterpretation. Misinterpretation of data or the misapplication of rules could potentially lead to some negative event.

The nurses were divided in their opinion about the organisational actions. Clearly the senior nurses are set to benefit from the management plans. This is for two reasons. First, there was no power struggle between them and the managers, rather they were being given increased responsibility in providing Hospital Trust services. Second, they had an axe to grind with the doctors. As the nursing director put it, formerly "nurses were subservient to doctors". Now "CIS is forcing a structure"; it is prescriptive and doctors are being forced to give up power. She agreed that as a result of management's actions, doctors are being alienated, but "we do not want that to happen", she said. For her the root of the problem regarding the power of the doctors was their authority to assign beds in hospitals. Therefore, a simple solution for her is to close the hospitals which would result in diminishing their power. On the basis of this she justifies the new management system at the Hospital Trust which focuses on closing the hospitals, moving people out into the community or into nursing homes and thereby dispersing the power.

A similar viewpoint is expressed by some 'forward-looking' ward managers. One particular ward manager considers that doctors should have nothing to do with the health care delivery process. He went on to say, "doctors should do what they are supposed to do". Indeed one wonders what else is the role of doctors but to provide health services to the patients. Slightly conservative ward managers however thought that it was really impossible to replace the role of a doctor. They felt that CIS was fine so far as administrative support was concerned, but beyond that it was the domain of doctors. Such people represent a minority, at least within the Hospital Trust. Middle ranking nurses looked at CIS and the managers to give them certain opportunities. It seemed that they tend to thrive on the inherent conflict between the doctors and the managers. One service development manager for example was happy that CIS was "legitimising a structure". She considered the focus of the new management system to be more on using the consultants efficiently since they were an expensive resource. At the same time she felt that the role of consultants was not being marginalised, rather that their expertise was being used appropriately.

The divergent viewpoints held by the nurses can be attributed to their position in the management hierarchy. Three definitive categories can be identified. First are the 'foot-soldiers', the nurses providing the actual mental health care at the ward level. These nurses were more concerned with their professional attainment rather than the political aspects of systems development. With respect to providing health care services, they regarded the role of doctors as supreme. Second are those nurses who aspire to be involved more in management rather than nursing. They were quite critical about the role of doctors in treating the mentally ill. This group gave importance to the logical functionality of CIS for their decision making. Third are the nurses who have reached the top of the hierarchy. They represent a cadre of nursing which has good deal of managerial responsibility. The Medical Director also envisages a similar role for the doctors. Such nurses focused more on controlling the clinical profession than on the intricacies of the practice itself. This group considered CIS in terms of providing business information and fulfilling business needs.

It becomes apparent from the organisational actions and the related responses of different groups that the existing structures of responsibility and authority are being questioned and changed. It does not mean necessarily that the change is for the good. The appropriateness of the change is a subjective issue but the changes are certainly affecting the norm structures of different groups and the way in which they relate to each other. In such situations the intentions and meanings of one group or individual can often be misinterpreted. Furthermore the different sets of rule structures that determine preferred behaviour can also be misunderstood and misapplied. This essentially means that there are systems analysis and design problems with CIS. Since the design of the system is being used to legitimate various structures and fulfil hidden agendas of different groups, it means that the analysis process of CIS was skewed towards particular groups with vested interests. Such systems place at risk the entirety of the organisation and its purpose and always run the risk of either being abandoned or misused in some form. These risks may be referred to as operational risks and as having nothing to do with information system security, but they certainly have their origin in the systems analysis and design process.

Problems with the management system

The Hospital Trust presents a typical scenario of inconsistency and incoherence in its objectives. This can be observed not only at the strategy formulation stage but also at the level of organisational structures which are a means for strategy implementation. The emergent environment presents a split hierarchical structure, the managerial and clinical. As has been argued elsewhere (Loveridge 1992), this has changed the roles and responsibilities of the key players. The changing responsibilities has left wide gaps in the management systems. This also raises potential problems for the security of information systems. Backhouse and Dhillon (1996) demonstrate how responsibility is a key element in the design of secure systems. They stress the importance of understanding the informal environment first, before designing a formal system. This aspect is discussed in detail in the sub-sections below.

In spite of the new formal management systems that have come into place within the Hospital Trust, the informal organisational norms are very weak. This indicates the prevalence of an informal environment where the clinical and business objectives do not support each other. This has resulted in a remarkable difference in roles created by the formal system and as they actually exist. Taking the example of a consultant doctor, the formal system views him/her as part of the multidisciplinary team. The multidisciplinary team is constituted of nurses, physiotherapists, dieticians, etc. This team assumes the responsibility of assessing the needs of an incoming patient, developing an individual care plan and subsequently monitoring the health needs. All these activities will be carried out with the help of a computer based information system. There is no mention of the key player, i.e. the consultant doctor, in diagnosing any medical illness. At the most, the role is restricted to that of an advisor. Most clinical decisions are now taken by a multidisciplinary team, which is part of the Trust. The Trust is also made up of roles, and holders of these roles are, under the new arrangements, *ex-officio* members of the team.

In reality, however, a consultant doctor performs very important tasks. He is assigned a specific clinical role to assess the mentally handicapped. Besides, he assumes all responsibilities for the medico-legal, liaison, outpatient and audit work. The role is also responsible for planning services for specific health care needs and in this capacity advises the Chief Executive on specific areas. Moreover, although a consultant is formally just another member of the multidisciplinary team, he takes all important clinical decisions and is held responsible for them. CIS tries to negate this 'influencer' role. As one consultant observed, the managers are involved in a childish play and are in fact losing out in the game. He observed that these petty things are motivating him to consider seriously the option of going private full-time. Doing this would reduce his NHS association to just a few sessions. The Hospital Trust is seeing this trend even more than ever before. This has serious consequences for the skill level within the Hospital Trust. Though it may not become apparent straight away, in the long term all the good doctors are going to concentrate on their private practices while the 'not so good' doctors are going to be left doing full-time NHS jobs. Obviously, this would mean that the quality, efficiency and effectiveness – buzz words of the managers – would not have any meaning. This also increases the scope for errors being committed, not only in the diagnosis of illnesses but also in health care delivery and in interpreting various issues. The reasons for such errors may not be attributed directly to CIS, but their origin can certainly be traced to the analysis, design and implementation of CIS.

The above example illustrates the extent to which there is a mismatch between the actual practices and the formally designed management system. The reason for the incoherence of the system can be linked to the analysis of content, context and processes of strategies. These show an over-reliance on the business vision and less on the clinical side. Unless there is a good match between the business strategy and the clinical objectives, system vulnerability cannot be avoided. This is because the responsibility for implementing business strategies resides with the clinicians. The mismatch leaves large areas where there are no clearly defined responsible agents, thus making it difficult to identify the structures of responsibility. Since responsibility has been understood as a key element in the security of information systems (Backhouse and Dhillon 1996; Strens and Dobson 1993; Lane 1985), it becomes evident that the management systems in place are highly vulnerable and problematic. As the information system is based entirely on the formal management system, it is also equally vulnerable. This raises serious questions about information security.

CIS and the relevance of employee activities

CIS is changing the basic symbolic code of the actions of the employees. A typical example of this is when managers refer to 'patients' as 'clients' as part of the attempt to change the way in which doctors and nurses 'see' their own work. These symbolic codes have been institutionalised to a substantial degree by the top-level managers and the middle-ranking administrators. However, the operational staff (e.g. the nurses) were more concerned in providing care to the patients and in their own professional development. CIS is also affecting the structure of various actions. A number of activities have been combined and different roles now allow the role holders to exert influence by virtue of their expertise. The extent to which these changes will be internalised still remains to be seen, but there is certainly a marked conflict between different interest groups that hinder a smooth transition and the intellectual growth of the Hospital Trust. This is clearly demonstrated by the activities of the Administration Manager of the Hospital Trust.

One of the key responsibilities of the Administration Manager is to check compliance and administer the Mental Health Act. Over the years she has gained a significant level of expertise in this activity. It seems that the role has become quite dear to her. She clearly expressed the feeling that she will not delegate this function to anyone, since it is very important to get the compliance right. Such is the power exercised by the MHA Administrator that all the details of MHA and its compliance are kept in her office. The staff have no physical access to these details. Even though CIS does have a MHA administration module, she still intends retaining her small index card based manual system.

Further discussions with Administration Manager revealed that besides MHA administration, she was also in charge of certain other activities. These were concerned with liaising with external organisations (the purchasers of the services), the Trust departments, the carers, the wards, the families of the clients and the clients themselves. MHA administration as a responsibility was given to this particular manager entirely because of convenience. It made sense to do so since she had the expertise in managing the MHA. However, in the design of CIS, a system of politics was in operation. By virtue of her expertise in MHA administration, the Administration Manager convinced the design team that the Mental Health Act aspect be integrated into her other normal activities. This gave her a straight advantage that saved her from being made redundant. This was so because the constituent hospital, where she was initially based, is due to be closed and all services are to be rationalised.

Within the Hospital Trust, the role of an Administration Manager draws authority from the Hospital Manager who in turn draws authority from the Chief Executive of the Trust. By virtue of a person having expertise, it places the individual in a privileged position. Being in such a position allows the person to exert influence on other roles. In this example, the Administration Manager by virtue of having expertise in the designated area, exerts influence on the Chief

Executive of the Trust to act in a predetermined manner. The social phenomenon of influence is a very complicated notion. According to Lukes (1974) an agent exerts influence either because of a conflict of interests or otherwise. Here the Administration Manager has no conflict of interest with the Chief Executive, but because of the expertise in the person, there is a 'system of inducement' in operation. This leads to exerting influence on the Chief Executive and by that gaining more authority. Since the computer based information system formalises the authority and subsequently the responsibility structure, it leads to reinforcement of power. The behaviour of this particular middle manager is in line with what management policy researchers call 'the power and means of influence of the line managers' (Mintzberg 1983a). According to Mintzberg:

> the lower in the hierarchy the manager, the greater his incentive to deflect orders and technocratic standards downwards and to withhold information from flowing upwards or else to exploit it, as well as the expertise contained in his unit.

Given the foregoing, we can see the manner in which a new information system changes the character of an organisation. The example not only illustrates the manner in which the middle-ranking managers can have influence but also the problems facing the analysts in eliciting user requirements. It is sheer common-sense that the design of systems should not be person-specific. If it is, then there are problems with the usability of computer based systems once that individual leaves the organisation. This aspect is related to the choice and use of a systems analysis and design method, an issue that will be dealt within the next section.

Significance of responsibility and accountability factors

The Hospital Trust computer based system holds information of varying kinds: patient case histories, medication reports, pharmacy details, etc. This information is highly sensitive and personal. It is important that a high level of security be maintained. It will be very embarrassing to the organisation if personal information about patients gets into the wrong hands[12]. However, the task of maintaining a secure environment is not straightforward. There are problems with various power groups in the Hospital Trust. The most obvious conflicts are between the doctors, nurses and the managers. The uncertainty created by governmental regulations imposes another dimension. In such an environment it is extremely difficult to negotiate access to relevant data, establish accountabilities and identify structures of responsibility. Consider a typical example where a patient is referred to the Admissions and Assessment Service at the Hospital Trust by the Home Manager of the Community Home where the patient resided. In this case the agents capable of taking responsibility are: Hospital Trust and Person (probably a consultant doctor). These agents realise affordances through their roles. For instance, the affordance of treating a patient can be realised through the role of a 'Registrar' (a junior doctor).

At this stage we must identify the norms associated with the agents. The 'Hospital Trust' which realises its behaviour through the roles of a 'Registrar' and the 'Consultant' doctor must take responsibility on part of these positions. In our example, although the Consultant is responsible for the patient, it is a norm that the Registrar will be looking after the day-to-day affairs. This is a typical example of a 'cognitive norm' characterised by standardised beliefs and knowledge within a group. Identifying such norms is extremely important since they play an important role in negotiating access into personal files (of the patient in this case). It must be noted that though the 'Registrar' may not have formal clearance to access certain files, nevertheless the prevalent norm system in the organisation determines the privilege level. This has important implications for security since a rigid rule-based structure of the formal system (the computer based information systems) is imposed on to a predominantly informal norm based environment. This is especially so in an organisation which is characterised by distinct groupings, each with a very strong sub-culture (the doctors, managers and the nurses in this case). Thus the identification of agents, their roles and the associated communication acts help us to understand and evaluate the environment better. Furthermore, we are able to identify more precisely the structures of responsibility and authority.

Summary and discussion

Findings so far have revealed that CIS has been perceived differently by the various groups within the Hospital Trust. The reactions of these groups stem from the meaning structures expressed by CIS. The relevance of these meanings is linked with the dissimilarities in intentions within the organisation. Such dissimilarities form the basis of the conflicts related to CIS and the problems of acceptability. The risks of system misuse or of any other security concern are also ontologically dependent on the diverse meaning systems in an organisation. As mentioned earlier the problems can be linked to faulty product design (i.e. CIS).

Such design problems can be summarised and discussed by considering the prevalent 'sign' functions within the Hospital Trust. We refer to sign functions because most organisational activities attempt to signify events and then communicate them. This is the property of 'signs' (Eco 1976). Most sign functions within the Hospital Trust are fixed because organisational structures, technology, roles, tasks and interpretations have been stabilised, at least for a given period of time. There are however 'loose connections' between the need for CIS, its implementation and the emergent reaction. When considering developing secure environments, it is these 'loose connections' that need to be studied, evaluated and understood. As will become evident by the end of this chapter, whatever means that are used for controlling access, for bringing about conformance to expected patterns of behaviour or for maintaining integrity become meaningless if the subtleties of behaviour, structures of meanings and intentions of key players are not understood and interpreted. These are the loose connections in an organisation.

Table 4.4 categorises the expressive content of CIS and considers its significance within specific domains. Denotative expressions refer to what CIS stands for within the Hospital Trust. In this case CIS is a sign function which refers to a set of objects or actions. Connotative expressions refer to the underlying meaning structures, typically with respect to CIS. These expressions consider the implication of what CIS refers to within a given domain.

Table 4.4 Summary of the meaning structures expressed and represented by CIS

Expression given by CIS	**Significance in the Domain**		
	Medical	Nursing	Administrative
Denotative	instruction	plans; policies	plans; policies; evidence; facts; value judgements
Connotative	coercion	rewards; inducement	rewards; inducement

Considering the significance of CIS within each of the Hospital Trust domains, it becomes evident that superficially the medical profession considers CIS to be purely instructive. The doctors consider this to be a completely prescriptive tendency on part of the managers. Prescriptive strategies work well in cases where the domain is highly standardised and practices are routinised. A typical example is in financial and accounting activities. The process of health care delivery is a highly descriptive, evaluative and an iterative one. There is only a small fraction of the tasks which can be routinised; most of the others are highly subjective and greatly dependent on the personal style of a doctor. CIS seems to impose a very rigid structure on the doctors. This is the reason why, deep down, they are having coercive feelings. These are the feelings of restraint and compulsion to do things in a particular way. Such actions could have a number of consequences. The most adverse is that the complete information system is not used by the doctors. In other cases, because of malicious feeling, the system may be misused. Doctors may also possibly adopt different routes to do their work. There are indications of this within the Hospital Trust. In a typical instance the Clinical Director asked the Planning Manager to consider some aspect of his functionality in the design of CIS. This was blatantly refused by the manager on the grounds that it was beyond the scope of CIS. He went on to say that even if he did consider the request, it would take two years before the directorate could get the deliverable. On seeing this attitude, the Clinical Director independently sought the solution to his problem from an outside vendor. Currently a stand-alone system is being run in the Clinical Director's office. Other consequences could range from alienating doctors, thus 'creating' disgruntled employees, to serious inputting and outputting errors being committed.

The nursing staff on the other hand consider CIS to be part of the strategic plans and policies. For most nursing staff CIS promises to bring in new hope and enrich their job functions. Consequently, deep within them CIS gives them a lot of inducement and holds potential rewards. This does not mean that nurses are a happy lot, in fact they may suffer the most because of the rationalisation drive of the Hospital Trust. Many nurses may be made redundant or may have to move out into the community. The feeling prevails that CIS would usher in significant rewards. It negates the role of the doctor and gives medical responsibilities to the nurses. There is a general feeling that doctors will come to accept this situation and that needs assessment and implementation of care will fall into the hands of the nurses. As one nurse pointed out, "we prepare all the Individual Care Plans ....", thereby questioning the role of the doctors. Such wishful thinking may not take form. There are serious consequences of this attitude. In one sense CIS has been 'over-sold' to the nurses. This group has been promised benefits which may actually not accrue. If that happens, which is highly likely, the nursing group may be disillusioned. This would mean that the nurses are not only going to feel alienated, but also cheated, betrayed and used. In this situation the Hospital Trust would have at its hand a group of people who can cause a lot of harm at the point-of-service delivery. The risks of intentional human errors and intentional misinterpretation of data cannot be ruled out. Whatever technical controls a system may have, ultimately it is people who execute the controls. The Hospital Trust is moving towards a situation where most employees are going to be very angry.

CIS represents a very different meaning structure for the managers. At a surface level for them CIS stands for their strategic plans, their overall policies. They are of the view that it is based on facts and hard-core evidence for a need. They legitimise their actions by saying that nothing has been changed, the computer system is just automating all the manual tasks. However, they have forgotten *en route* that there are many tasks which remain best unautomated. Deep inside, they feel that the system is going to produce many rewards. They will be able to quantify most of the activities and produce reports showing their efficiency levels and cost savings. The managers are actually not serious about security. The Planning Manager, when confronted with a question regarding the consequences of a security breach, fumbled with his words. Obviously, the issue had not been given serious thought. However, eventually he said that nothing disastrous is going to happen; at most it is going to cause embarrassment!

In conclusion, this section has reviewed various organisational actions and the manner in which different groups have reacted to these actions. The reactions of the various stakeholders has consequences for the success of CIS and also hold a key to the prevention of misuse. Positive reactions will determine correct use of the information system. Therefore, the intentionalities of different groups and the relevance of the information systems infrastructure to the user needs are to be analysed. It is hoped that a better understanding of the structures of meaning will help in developing appropriate computer based applications such that there is very little opportunity to misuse. The next section looks into the manner in which meaning structures come into being.

4.3.4 Analysis of the syntactic and empiric aspects

The health care delivery process, although visible, is known to most people at the service delivery level. Some of the elements of service delivery are highly norm based, while others follow strict rule structures and are therefore procedure oriented. Within an organisation these rules and procedures act as symbolisms producing images and narratives about different events. An interplay of rule and norm based structures determines the patterns of behaviour in any given context. In the previous sections we have noted the cultural significance and the meaning content of these rule and norm structures. This section analyses the form and the means in which these rules have been implemented. Ideally, the rules specified for the IT infrastructure should adequately represent the real world of the organisation (Checkland 1981). If this does not happen then the computer based information systems run a high risk of being misused. Security concerns are therefore paramount when considering the implementation or viability of rule structures.

Logical service specifications at the Hospital Trust

In the particular case of CIS, the system developers and the project team regarded the Hospital Trust activities as an input–output process. Therefore, they considered the health care process in terms of patients coming into the hospital, being treated and then discharged into the community (also depicted in figure 4.1). This conception helped in modelling the systems development tasks by using the Structured Systems Analysis and Design Methodology (SSADM). The first phase of SSADM, analysis of the current system, identified eleven subsystems within the hospital environment. These sub-systems interact with each other to transform patients so as to improve their learning skills. The eleven sub-systems are: Admit client; Provide care; Client administration; Resettle client; Contract management; Staff deployment and duty rostering; Pharmacy; Monitor service quality; Provide staff training and development; Budget management; Manage ward. In conducting the analysis of the current system, SSADM requires an analyst to investigate problems, bottlenecks or dissatisfaction among users. This is an important stage since the very success of the final product may depend upon correct requirement assessment. The analysts for CIS were supposedly directed by the Planning Manager to key personnel in each of the functional areas. Discussions with different people revealed that these personnel were not appropriately identified to provide the required information to the analysts. Two interesting issues emerge. First, the project team failed to identify various stakeholders in the Hospital Trust, thus resulting in an inadequate analysis. Second, the analysts (who were outside consultants) should have taken the initiative to define the problem domain adequately. The result of this is that though various processes had been identified, there was no consideration given to user reactions. A careful interpretation of such reactions helps in the development of a rich picture and assesses the pragmatic and semantic aspects appropriately.

The second stage of SSADM provides a logical view of the required system. CIS analysts identified five core activities, viz.: Administer client; Provide care; Administer trust; Resettle client; Manage staff deployment. The logical structure was again based on the input-output model. The underlying presumption in this case is that if the needs of individual sub-systems are being met, then the needs of the overall system are also being fulfilled. The logical view of the system has problems at two levels. First, it is based on an inadequate systems requirements, which is an output of the first stage. Second, the control transforms introduced in the Data Flow Diagrams do not represent the real operations. The reason for this is also related to the problems in requirements analysis. Implementation of controls at this stage is a very sensitive issue. These become apparent once the system is automated. Because the nature of logical controls does not match the prevalent structures, there are problems of incoherence. This becomes clear from the structure of the 'Provide Care' sub-system of CIS. The module is central to the health care delivery process and its successful operation depends on the construction of an Individual Care Plan (ICP). However, the analysts do not consider the relatedness of ICPs and the organisational functions. The formal model for developing an ICP is based on the notion of choosing dishes from a hospital menu, a concept which does not consider the needs of the doctors. This is because of an ongoing disagreement among professionals as to the relative importance of ICPs and ward rounds. Such a discordance becomes more obvious in a hospital that provides care to the mentally ill. ICPs work well in residential wards, but those wards are being closed by the management. What will be left will be the acute wards. Consultants within the Hospital Trust are of the opinion that in this new setting, primacy cannot be given to ICPs. Judgements about care plans are largely dependent on ward rounds. In fact they proposed the merger of ward rounds and ICPs when considering health care provision for acute wards. The logical model of CIS simply considers the existence of an ICP and bases the controls (error handling routines) and security mechanisms around them. The 'Provide Care' module typically comprises six processes: assess needs; construct ICP; plan care delivery; review care; monitor care; implement care. Each of the processes gets constant input from the ICPs for the purpose of monitoring and control. The quality of the logical model is questionable because it is based on the ICPs which necessarily do not represent the real world situation.

The second stage of SSADM also looks into the new requirements of the users. These are then included into the logical models. However because of requirements analysis problems such new needs have not been met. In one particular case the requirements of some doctors have simply been ignored. The Hospital Trust is a centre of postgraduate training of psychiatrists. The Medical Federation provides funding to the Trust to organise the training schemes. The Dean had requested the consultants of the Hospital Trust to develop an IT infrastructure to manage the training function better. The consultants approached the CIS project team in this regard but the planning manager declined to provide any system support in the short term. The consultants could not wait for years for such a system to be developed, so they bought some custom software from a vendor. Such a requirement should not have been ignored by the planning department for a number of reasons. First, since it is a user requirement it should have been considered adequately. This would have also prevented independent system development activities at the unit or departmental level. Second, inadequate management of the training schemes would affect the quality of the training process which in turn means that the Medical Federation may withdraw its funding. This could result in losing accreditation for the training programs resulting in the loss of manpower. Had the system analysts been aware of the consequences, they would probably have considered this new requirement more sympathetically.

Other stages of SSADM have had problems as well. The final set of formalisms selected by the users does not represent the real environment. A feasibility study of various options for implementation was carried out and later presented to the users. Two interesting issues emerged. First, the users selected do not represent the real setting of the Hospital Trust. The ward managers involved in the study specialise in long stay residential care and non-acute illnesses. Consequently the focus of CIS is skewed in that direction. Second, the residential non-acute specialisms are being relocated from hospitals to a community setting. The requirements in the new environment will be substantially different from what they are at present. The system developers have not considered this aspect. The reason is that none of the users from the acute mental illness units has been involved in selecting options for CIS. The underlying intentions for such a situation reflect the political motives of different groups. Had the system analysts been aware, consideration would have been given to such issues. The remaining stages of SSADM, though having been carried out adequately, are insufficient because of inconsistency problems highlighted above.

Logical security measures

It is a well documented fact that prior to system development, designers should achieve a deep understanding of the application problem domain (Baskerville 1993; Avison and Wood-Harper 1991). In terms of developing secure systems, it is important that security features are considered along with the system design process (Baskerville 1988). Accordingly, Baskerville identifies three distinct stages. First, the emphasis should be to produce the right kind of security rather than implement security correctly. If the latter is the case, then security is being considered as an afterthought to systems development. Second, security design in itself should be characterised by either logical or transformational models[13]. Third, rather than emphasising cost-benefit risk analysis, the focus should be on the usage of abstract models. Though there is a limited effort in using these concepts, the SSADM-CRAMM interface offers some opportunities.

The CIS system development team which used both SSADM and CRAMM has however failed to capitalise of the benefits of the SSADM-CRAMM interface. As of now CRAMM is the only risk analysis method that has been integrated into the overall information systems design and development. The method comprises three stages, each being supported by the CRAMM software (Farquhar 1991). Stage 1 sets up the scope and boundary of the analysis. Owners of the data are identified and interviews conducted. Stage 2 groups the organisational assets logically by using a database of generic threats. Stage 3 suggests countermeasures on basis of asset groups, risk levels, etc. (see figure 4.5). The main difficulty of using CRAMM is the level of expertise expected from the analysts in carrying out stages 1 and 2 (Polson 1995). Used properly, CRAMM accepts inputs from different stages of SSADM. Stage 1 of CRAMM proposes a set of countermeasures based on the initial system specifications. The second review stage produces a set of countermeasures based on the initial view of data and the business options as conceived by the analysis and requirements specification stages of SSADM. The third stage identifies countermeasures on the basis of the technical decisions taken while using SSADM. A final list of countermeasures is generated which is later used in the physical design of the system.

In CIS, the emphasis on generating countermeasures has been skewed towards stage 3 of CRAMM. Rather than using inputs from SSADM to identify countermeasures at stages 1 and 2 of CRAMM, the system developers have used the NHS Management Executive documentation to identify broad categories of threats. A typical example of this generic classification appears in table 4.1. An important step in stage 1 of a CRAMM review is the identifying of 'data owners' and then conducting qualitative interviews with them for asset evaluation. This has not been done. Interviews were conducted only with the Chief Executive, the Planning Manager, the IS Manager, Director of Finance, the Administration Manager in one of the constituent hospitals and the Medical Audit Manager. A few members of the CIS user group who did participate gave information more suitable for system development activities than for asset evaluation. Moreover the interviewees were not necessarily the 'data owners'.

The notion of identifying 'data owners' is complex in itself. This concept is based on the presumption that almost "everything in existence on the earth 'belongs' to some individual or organisation" (Dorey 1991). Therefore an owner of an asset has authority over it and has responsibility for its safekeeping. This assumption facilitates the implementation of control mechanisms in a strictly hierarchical manner. The origins of such a notion can probably be traced to the military sector, where there is a prevalence of strict hierarchies and it is relatively easy to delineate data into concrete physical entities. However, in a civilian environment identifying responsible agents may not be all that easy. This is more so in a hospital setting which is gradually evolving into an organismic form (i.e. is developing strong external relationships and weak internal structures).

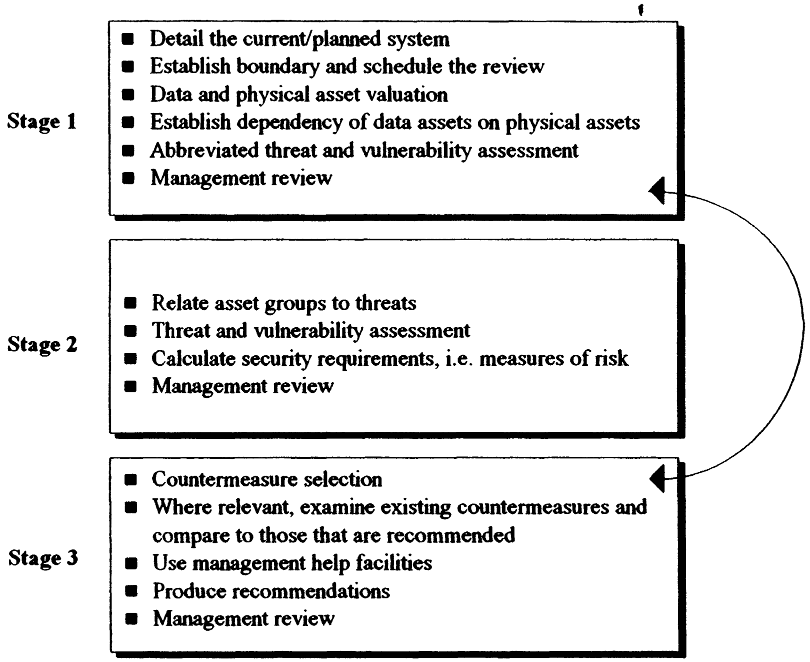

Stage 1
Detail the current/planned system
Establish boundary and schedule the review
Data and physical asset valuation
Establish dependency of data assets on physical assets
Abbreviated threat and vulnerability assessment
Management review
Stage 2
Relate asset groups to threats
Threat and vulnerability assessment
Calculate security requirements, i.e. measures of risk
Management review
Stage 3
Countermeasure selection
Where relevant, examine existing countermeasures and compare to those that are recommended
Use management help facilities
Produce recommendations
Management review

Figure 4.5 Overview of CRAMM

In the Hospital Trust, although the analysts used CRAMM to identify possible countermeasures to establish relevant controls in the physical design phase, they did not carry out the tasks suggested in stages 1 and 2. The complexities, problems and shortcomings in identifying 'data owners' and valuing assets are marginalised when CRAMM itself is not used correctly.

Logical structure of the controls

The means of implementing security controls are as dubious as the form of the controls. This becomes clear on analysing the existing control mechanisms at the Hospital Trust's CIS. The analysis can be performed by looking at processes and the related modulators[14]. A simple example is the process of recording someone's finger print. An impression must be left on a greasy surface, glass or special paper before being observed by the human system. In this case modulation concerns the manner in which a signal is given some physical representation before being observed. This interpretation is a two-way process. Not only can an object leave an impression (finger print – a sign) for interpretation, but also a number of signs can be translated into a physical object. Control is instituted through a feedback process, the emphasis being on having a minimal level of departure from desired performance. An adequate control therefore is the one in which the 'modulator' retains the meaning of the final outcome (for more details see Stamper 1973).

The controls in CIS can be analysed by looking at the characteristics of the modulation process. Consider the Client Care module of CIS. Doctors diagnose and analyse the patients' requirements through a complex set of signals, even though they are observing a single modulation process. The meaning of their final prognosis depends heavily on the relationship with patterns formed with other signals. The module however is 'straight-jacketed' and does not allow subjective interpretations. Typically, it permits a doctor/nurse to enter the goal of the treatment, expected outcome and the desired outcome. Additionally, there is a facility to prioritise the goals. The controls emphasise the efficiency of service delivery, giving no consideration to outside influences. The controls are implemented with the assumption that inputs and outputs of the modulator (the rule structure of CIS) can adequately be captured and assessed. Furthermore it is assumed that the primary source of given data will go in as input to CIS and that the output is a result of a convenient recording operation. The doctor or a nurse can then see the deviations in performance which can subsequently be rectified. The mechanisms are represented diagrammatically in figure 4.6.

If we take a real life example of a patient coming into hospital for treatment, the simplistic control structures of the module become obvious. An initial review of the patient may indicate symptoms of some kind of *Schizophrenic psychosis* but it may require considerable effort to pinpoint the class of schizophrenia. Since the goal, expected outcome and desired outcome cannot be stated as clearly as the system expects us to do, the very use of the module becomes questionable. In terms of modulation the origins of the problem can be traced to the influences of other signals onto the modulator. In the particular instance of diagnosing *Heberphrenia*, a class of *Schizophrenic psychosis*, the other signals take the form of symptoms such as 'shallow mood accompanied by giggling', 'self absorbing smile', 'hypochondriacal complaints', etc. The final interpretation of a doctor may therefore be very different from the perceived outcomes. The system attempts to impose a strict formal control of comparing the output to the input without considering the complexity of the task. The existence of such controls is very problematic and raises concerns for security – particularly that of misinterpretation of data. This is, in our definition, a serious security concern.

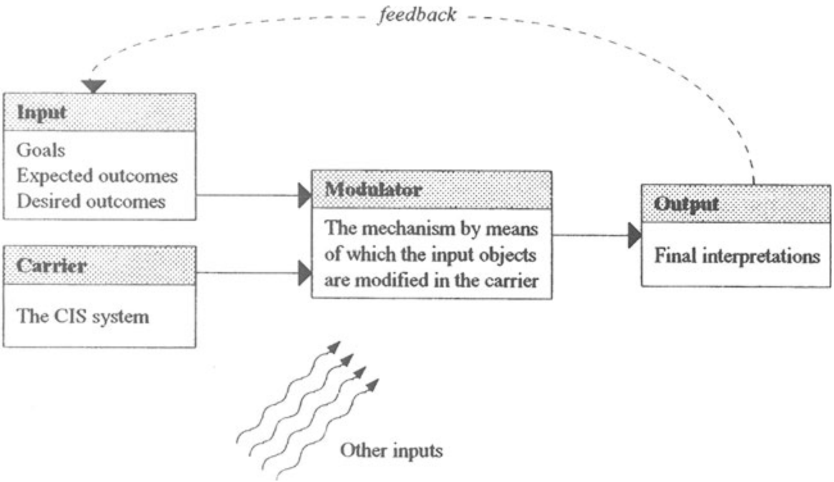


Figure 4.6 The control feedback loop and the emergent concerns

Summary and discussion

The health care delivery process as conceived and conceptualised by the managers of the Hospital Trust (see section 4.2) has subsequently been translated into a computer based information system. Ideally, the computer based system should link the understanding and expression of ideas to the formal systems (Liebenau and Backhouse 1990). This should form the basis for generic solutions around which specific applications can be built. Liebenau and Backhouse (1990) identify the notion of 'usage' and 'reference' as fundamental to establishing a link between the intentions and meanings (i.e. semantic considerations) and the formal representations (i.e. syntactical issues). 'Usage' refers to the ways in which formalisms are created and the concept of 'reference' links the formalisms to actual actions. Considering the computer based systems development activities, the various modules of CIS represent the formalisms which encompass the elements of health care delivery process. The actual delivery of services is related to functionality of the modules. In a good systems development activity, the correct use of 'usage' and 'reference' concepts is very important since it allows us to relate meanings of our actions in the real world to actual physical, social and legal operations.

Table 4.5 summarises the security concerns for each module of CIS. These are linked to an inadequate understanding of the 'usage' and 'reference' issues by the system analysts. Part of the problem related to imperfect representation lies with the kind of methodology chosen for systems development, i.e. SSADM. No doubt SSADM helps in mapping requirements of the manual system, but it is rather difficult to generate a 'rich picture' of an organisation. Consequently, the rules and procedures of the information system do not consider the power, politics, intentionality and beliefs of different individuals and groups (i.e. the semantic components). The system developers lack a clear understanding of the 'real world' resulting in the development of a defective system, which runs a high risk of under utilisation, complete abandonment or even misuse.

Table 4.5 Summary of the form of CIS and related security concerns

CIS sub-systems	**Issues regarding**		**Security concerns**
	nature of the formalisms ('usage')	**relationship of formalism to actions ('reference')**	
Administer Client	Translates the whole manual operation into a computer based one	The module relates to the actual practices	Though primary concern is for privacy that can be maintained by password protection, there are however implementation problems
Provide Care	Presumes that patient needs can easily be categorised and hence imposes predetermined classes of activities	Computer based classes do not adequately represent the 'real world' actions	Problem of validity of perceived actions. Because of such inconsistency problems even simple control mechanisms run the risk of being misused/not used
Manage Pharmacy	Translates pharmacy record maintenance onto the computer	Falls short of fulfilling the basic objective of pharmacy costing and drug utilisation reviews	Threats of vulnerability to competitors and integrity problems of the pharmacy processes
Administer Trust	Formal structures of this module presume that all other modules are being used adequately	Logically the module would generate relevant management information	Because this module draws information from 'provide care' and 'resettle client' modules, its success depends on those modules
Resettle Client	Module based on the premise: *minimise patient stay in the hospital*	A worrying trend because it questions the very existence of a managers job. This has prompted managers to reassess their objective	CIS attempts to be a medical decision support system. Validity of such systems is questionable. Raises problems of power and conflict
Manage Staff Deploy-ment	Computerises the personnel aspects: wages, salaries, duty rostering etc	No emphasis on training and development – a real requirement	Excessive personnel controls result in alienating employees

4.4 Emergent issues

The purpose of this section is reflect on the key findings from the Hospital Trust case study. These are then related to the problem of managing information system security. Information system security is considered as a state of caution and safety with respect to the information handling activities of an organisation. In terms of the definitions presented in chapter 1, security can be achieved through the maintenance of consistency and coherence of the information systems.

It is interesting to note that within the Hospital Trust, security has been viewed very narrowly. Although the possibilities for the occurrence of adverse events have been explored, the countermeasures have been restricted to access control mechanisms. The wider contextual issues with respect to the information system have largely been ignored. Hence there is a strong likelihood that the computer based information system at the Hospital Trust will neither contribute towards enhancing the productivity nor the effectiveness of the organisation, but rather it may make the organisation highly vulnerable. This is because there is a mis-match between the actual practices and the formally designed computer based information system. There are two contributing reasons. First, since the organisation represents a split hierarchical structure (i.e. between clinicians and managers), the informal organisational norms are very weak. Furthermore the clinical and business objectives do not support each other. The combination of these factors has resulted in a remarkable difference between the roles created by the formal system and how they actually exist in practice. Second, although all stakeholders (doctors, nurses and managers) agreed that ideally the system would be a boon to the organisation, there was disagreement on the manner in which it was developed and implemented. The organisational work practices were technology driven, i.e. it was the computer system that was determining the formal reporting and authority structures. Moreover, it was also forcing unrealistic informal social groupings on to the members of the organisation. Since the key players were unhappy with the change process, there is a risk of system misuse.

In such an environment, however extensive the control mechanisms for preventing the occurrence of adverse events, there is a strong likelihood that most controls may either be ignored or be inappropriate to the real needs of the organisation. In order to make the controls effective, what is needed is coherence between the technical computer based information system, and the environment in which it is embedded. In the case of the Hospital Trust, it is contended that the computer based system is largely based on the formal rule based manual system. In that case a careful analysis is necessary so as to assess whether it is appropriate to computerise everything. At face value this may not seem to have any security implications. However, the inability to understand such aspects leads to incoherence and inconsistencies in the operations of the organisation. Although the analysts may consider the system to be technically foolproof, because the people using it are unhappy or discontented, there are strong chances of the controls being subverted.

Another emergent issue relates to the manner in which the system was conceived and planned. It is clear from the empirical study analysis presented in the previous section, that the motivations for developing the system were more political in nature, rather that the real need. Consequently, the whole policy planning process is quite *ad hoc* in nature. With respect to information system security, there has been practically no emphasis on developing a policy. Within the organisation it is believed that a very generic policy statement developed by the NHS management executive would be sufficient. This further demonstrates complacency on part of the CIS project team.

Table 4.6 Résumé of major issues

Emergent issue	Interpretations from the Hospital Trust case
Planning and security policy	Reasons for developing an information system are more political than otherwise. Information systems planning is ill-conceived. Security planning and policy is not considered as an issue.
Evaluation of security	No strategic importance was attached to the evaluation of security. CRAMM was used to assess the risks. Risk analysis was conducted in a very *ad hoc* manner. Environmental factors have not been adequately considered.
Design considerations for security	Proper requirements analysis has not been carried out. A very narrow technical perspective has been adopted – thus ignoring the human element. Security, if at all considered, has been an after-thought.
Implementing information system security	Implementation of various controls has been arbitrary. No consideration has been given to the beliefs and expectations the stakeholders. There was a major security risk through the 'creation' of a disgruntled employee.

Based on the analysis of the Hospital Trust case presented so far, four key themes pertaining to the management of information system security can be identified: the planning and security policy issues, the evaluation of security, information systems design consideration in security and the implementation of security. A résumé of the major issues is summarised in table 4.6 and discussed at length in chapter 6.

4.5 Conclusion

This chapter has attempted to describe how the computer based information system within the Hospital Trust was conceived, analysed, designed and subsequently implemented. By using the conceptual framework proposed in chapter 3, the analysis of the case revealed inconsistencies in the design and management of the information system. Discussion in this chapter has also revealed that with respect to information system security, the CIS project team has considered the syntactic and the empiric issues only. The pragmatic and semantic aspects have largely been ignored. It also becomes clear that indeed the deep-seated pragmatic aspects of the Hospital Trust have a significant bearing on the security of information systems. This contention supports the main argument of this book. The key themes identified in this chapter form the basis for developing a synthesised perspective later in the book.

[1] Syndicalism is a form of occupational power in which workers attempt to regulate their own work. With origins in the medieval guilds, the thrust is on introducing extended periods of subordination and initiation. Once trained, individuals gained considerable occupational autonomy.

[2] The concept of a medical product is increasingly being used by the managers. A typical pre-reform hospital provided a wide range of clinical services. For the purpose of administration and accountancy, these services are referred to as products. Since some products prove to be more profitable than others, a 'rational post-reform hospital' may choose to discontinue the production of less profitable ones (Whynes 1993).

[3] It may be noted here that the IT infrastructure is (and has been planned) on the presumption that there are three hospitals within the Hospital Trust and that there will be significant electronic communication between them. However, the management has made concrete plans to rationalise the services as a result of which two of the hospitals are being closed completely. This decision had been taken by the Trust long before commissioning the CIS project. These facts have been completely overlooked by the CIS project team. The Trust administration and the software development consultants have not considered this in their plans. Rather, three separate feasibility studies for developing a networked environment have been conducted.

[4] *ibid.*

[5] CIS risk assessment was done by using CRAMM. CRAMM complements the systems analysis and design methodology, SSADM, which was used for development. There are however problems in using CRAMM, since it requires a significant level of expertise and an understanding of the organisational environment (Polson, 1995). Risk assessment and systems development for CIS was commissioned from outside consultants. Considering the nature and quality of risk assessment done, there are doubts regarding the competence of the staff (see section 4.3.4).

[6] This judgement is based on the interviews conducted by the author.

[7] This is especially true of junior doctors (Registrars), who generally come on a teaching rotation of one year duration.

[8] It should be noted that while the middle and top level managers refer to patients as 'clients', the nurses still call them 'patients'.

[9] Politically this may be subject to some debate.

[10] Loveridge (1992) does not use the term 'organic'. However, it can be interpreted that indeed the structure of the NHS, abetted by the medical profession, is changing. Loveridge notes that "the nature of medical control over the delivery process and over deployment of clinical knowledge is ... eroding" p218. When considering the Hospital

Trust case, there are clear indications of such a trend. This has resulted in many consultant doctors 'diluting' their relationship with the main place of work. In the Hospital Trust more than half of the consultant doctors had strong professional interests outside the hospital. This signifies a move towards the creation of organic structures.

[11] The term stakeholder is used in a commonsensical manner and connotes any person or organisation that has interest in a given activity.

[12] Not only are there a number of organisations which would be interested in such information but disclosure of information about behavioural patterns of a patient could be deleterious to the treatment.

[13] Logical models consider the needs of a system in a data-oriented (functional) manner. The transformational models emphasise more on the organisational and behavioural needs. System development for CIS is based on logical modelling.

[14] The basic ideas of modulation are rooted in Shannon's Mathematical Theory of Communication. The notion assumes that when a message is communicated it gets translated while moving from one medium to another. In doing so it carries a set of patterns from one medium and imposes them on to another.

5 The case of managing IS and security in a Local Council

5.1 Introduction

The case study described in this chapter concerns the management of information systems and their security within a Local Government Council. In order to develop an insight into the systems in place, the Public Services and Works department, the biggest unit within the Council, was sampled out. At the time of the study there was an initiative within the Council to introduce a 'federal' IT infrastructure. This was happening amidst increased socio-political and economic pressures. Indeed the case study was selected because of the ongoing change programme.

This chapter discusses the various contextual influences within the organisation. Section 5.2 describes the nature and orientation of the Local Council, especially with respect to changes initiated at the national level. Section 5.3 presents an analysis of the case study. It uses the conceptual framework developed in chapter 3 to examine the management of information system security. Section 5.4 identifies the emergent themes for discussion. These form the basis for developing a synthesised perspective in chapter 6. Section 5.5 concludes the interpretation of information system security in the Local Council.

5.2 Organisational background

Organisational processes, management structures and information systems are largely influenced by the wider contextual changes within an organisation. This section therefore evaluates the context of organisational events and actions relevant to the Local Council. The first part of this section focuses on the broader sectoral context and sketches the post-war history of changes in local authorities. The second part describes the setting of the case in question, followed by a discussion of the IT infrastructure in place.

5.2.1 Local Government in the UK

The years between 1945 and 1975 have often been termed as the 'golden age' of British local government. This period represented a time when spending in this area rose and new responsibilities were added incrementally. This trend seemed to make local government an important pillar of the British political system. However, there were concerns about providing community support on the one hand and the need to ration the 'offerings' on the other. Having recognised the pitfalls, there were attempts in the 1960s to modernise services. These efforts focused on providing a clear well defined set of services (e.g. education, housing and social services) at a local level, with reasonable efficiency and local democratic accountability. The changes resulted in the creation of the Greater London Council and a set of new London Boroughs.

The beginning of the changes

1974 saw major changes in local administration with the introduction of a two-tier system of Counties and Districts throughout England and Wales. This was followed in 1975 by a new system of Regions and Districts in Scotland. The first tier included County Councils in England and Wales and Regional Councils in Scotland. The thrust here was to provide services that were most suitable to administer on a large scale – for example the highways, transportation, police and fire. The second tier comprised the District Authorities. The focus being on the provision of local services, for example, housing, refuse collection and recreational facilities.

The intention of this reorganisation was not to redefine administrative boundaries and allocate service functions between different types of Authority, but only to increase the efficiency of local government. A 'corporate planning' model was adopted as a means of achieving this purpose, and a typical structure constituted of a Chief Executive, a Management Team of departmental Chief Officers and expanded central support functions such as personnel and management services.

Towards a market driven authority

There is widespread agreement that the functioning of local government has changed significantly since the 1980s. This has primarily been because of the Local Government Planning and Land Act of 1980. The Act introduced controls that resulted in penalising councils that spent more than a previously determined limit. 'Hit-list' councils, that had 'excessive and unreasonable expenditure', were identified. First steps in this direction were taken in Scotland in 1982-83. This was followed by legislation on 'rate-capping' in England and Wales in 1984, making it possible for the central government to set a maximum level of local taxation for particular councils.

The thrust at that time had been on efficiency and the trend was towards introducing a market ideology. There were two claims which formed the basis of this orientation. First, that market orientation in the delivery of services would increase the efficiency with a dominant stress on 'value for money'. Second, that direct accountability to 'consumers' would increase as a result, thus shifting the emphasis from local governments being responsible to citizens (through political pressures and elections) towards being responsible instead to consumers (because of forms of market pressures) (Cochrane 1993).

The orientation towards 'consumerism' should not be interpreted as local government being replaced by central direction, or by the market. Yet it should be recognised that substantial change has taken place. This change, as the Audit Commission puts it, is in relation to understanding citizens as 'customers', rather than 'clients'. This means that role of the Councils should be to encourage a "diversity of provision from a range of agencies" rather than seeking to deliver directly (Audit Commission 1989). In a similar vein Brooke (1989) considers that in the future there would be a range of single service agencies with a strong and a coherent political, professional and managerial leadership based around a central core of strategic planners and regulators. A second, and managerially inclined cadre would run the services. This vision fits well with the overall government programme since the late 1980s.

Because of the changes resulting from governmental polices and legislative measures, the final outcome has been to mimic a relationship that exists in the private sector. This was formalised in the resultant Citizens' Charter[1]. The emphasis of local government therefore has shifted towards 'customer service'. In fact at the present time terms such as 'customer service', 'customer care', 'closeness to the customer', 'public service orientation' are all being widely used in local government circles. Based on the private sector model, the use of the word 'customer' implies a two-way relationship, in which customers can make choices, have appropriate information to make those choices, have access to goods and services if they are willing to pay and gain redress if they are not satisfied.

With an increased orientation towards the customer, local government is striving to get closer to the public. This involves looking into six different issues. First, there is a need to find out what the public wants. The CBI's document, *Working for Customers* translates this as follows: "Working for customers means just that. Finding them, listening to them, thinking like them, anticipating their needs and solving their problems" (Confederation of British Industry 1983). Second, judgement needs to be made about the extent to which an authority is meeting the needs and wants of the customers. This can be effectively done by the customers themselves. The National Consumer Council argues that local authorities can become more consumer oriented by setting targets for performance, measuring and reporting achievements and giving consumers the information to question performance. Third, the level of communication with the public needs to be increased. This pertains to providing information about local government activities and services. Fourth, public access to information needs to be improved. It involves making it easy for those interested to take an active part in the local government. Fifth, new ways of thinking about customers and often new ways of behaving towards them should be inculcated. This entails developing a customer culture. Sixth, the service should be organised in such a way that those structures and procedures are adopted that are convenient for the public. The methods employed to develop such a customer orientation gave a considerable boost to the use of information technology within the local governments.

Initiatives in the local government and computer based systems

The complex organisational environment, new organisational forms of the local government, and pressures from the changing economic and social contexts have indeed brought quality issues to the forefront. The extensive use of information technology is further heightening the situation. Today, information technology is considered not only as the cause of many changes, but also a consequence.

Though the change in orientation of local governments and the use of information technology to support the changes are a recent phenomenon, the history of the growth of computing within the local government can be traced to the 1960s and early 1970s. During that period the use of computers was largely determined by expenditure and employment levels and was hence restricted to a few support areas. Today, information technology is not just confined to the expanded central support functions, such as personnel and management services, but is playing a crucial role as a catalyst enabling the changes to take place (Land 1990).

The current profile of use of information technology within local government has evolved from large mainframe applications focusing on efficiency to a networked environment where the impetus is largely political. In this transition the control over information technology has shifted from a centralised information technology department to the users. Information technology is no longer considered as a central resource that is based on mainframes and is hardware driven. Rather the focus today is on distributed technology where most developments are software driven. There is also an increased tendency towards outsourcing.

Advances in the technology have encouraged the formation of small and medium sized enterprises and the break-up or the decentralisation of large organisations. Sanderson (1992) notes that within the local government vertical control hierarchies are being replaced by lateral structures that have a devolved control. Furthermore, there is a new emphasis on 'organisational culture'. This is leading to a networked form of an organisation where there is a small 'core' workforce that is supported by a large 'peripheral' low-skilled, part-time or subcontract labour force.

The development and use of information technology applications within local government can be classified loosely into two groups. First, there is a range of systems oriented towards providing and handling information for management and administration. Examples of such systems can be found within the payroll, personnel, budgeting and accounting functions. Second, there are systems concerned primarily with the services provided by the Authorities. Systems within this category can either be for providing information regarding day to day activities or may be aimed at providing information for monitoring and policy planning purposes. It is this last group of systems that has attracted most attention in terms of "providing mechanisms for improving the human condition" (Barras and Swann 1985; p61). The case study presented in this chapter focuses on such systems. Typical examples of these systems within local government are as follows (some of the examples are based on Barrett and Masters 1985):

- Systems that monitor the changing size and structure of the population in an area, thus helping in identifying particular subgroups – school age population, elderly, etc.
- Systems that help identify and delineate problem areas such as level and dynamics of unemployment.
- Systems monitoring the pattern of residential and commercial development, thereby facilitating planning and development of infrastructure (e.g. schools, libraries, etc).
- Housing systems which provide support for allocating council housing.
- Systems that monitor public transport provision.
- Systems that monitor refuse collection.

The use of such systems has predominantly been for policy planning. Since the 1960s there have been major initiatives to develop integrated information systems that could support functions such as payroll, budgeting, transport modelling, etc. The development of such integrated systems was encouraged by the General Information Systems for Planning report in 1972 and the McKinsey report in 1975, which were commissioned to assess the information needs of local authorities. However, there is a widespread belief in developing small, dispersed and operational systems (Barrett and Masters 1985). In practice this intent has not been realised. Increasingly there are political pressures to link and integrate widely dispersed systems, typically referred to as 'federal IT infrastructures'. The basic principle behind the linking of numerous small independently developed and managed systems into a loose network is valid, but problems arise when the application domains are significantly diverse. This is discussed at length in section 5.3 below. Furthermore, many of the integrated systems developed in the 1970s were not entirely successful. Failure has generally been attributed to the inadequate scale of resources, the timescale and remoteness of systems from the users. Examples of some of the integrated systems of that period are: Local Authority Management Information System; National Gazetteer Pilot Study; Spatial Analysis and Retrieval System; Local Authority Financial Information System.

At the present time, falling costs and improved technology have made large systems feasible and cost effective. As a consequence many large integrated systems have been developed, although the extent of their use still remains questionable. The often cited success stories are the big systems, such as SOSCIS – a system to record social service clients, and HMIS – a system to manage housing provision. There is a trend also for software houses to develop custom software to undertake particular tasks. The role of integrated systems, however, is bound to change, especially when there is an increased tendency towards decentralisation and empowerment.

The Local Council, which is the focus of this study, operated in such an environment, characterised by changing national policies, new technologies and a lack of a consistent vision. Differing political motives further complicate the situation. Section 5.2.2 discusses the organisational setting of the Local Council. Next the core business activities and the implications of the wider contextual changes are highlighted.

5.2.2 The Local Government Council

The Council is a typical Government Council with wide-ranging activities. The spread of activities can be gauged from the Council's involvement in Public Services and Works, Housing, Social Services, Transportation and Refuse Collection.

Organisational structures

The Local Council is headed by a Chief Executive and supported by Directors who are in charge of particular departments. The 'Chief Executive's Office' provides strategic support to the functioning of the Chief Executive and the Council. Each of the Departments has a number of Assistant Directors who are responsible for their own specific divisions. They are in turn supported by Principal Officers, Managers and Assistants.

Within the Council there is a growing trend to decentralise activities and consequently departments vary considerably in respect of hierarchical structures. In the housing department for example, there is a top management emphasis on developing professional teams. It is believed that such teams ought to be constituted of "commercial and slick" managers who respond to customers' needs. The thrust therefore is to create a flexible environment that encourages enterpreneurship – although within a framework of uniformity.

In spite of a growing trend towards decentralisation and delayering, some departments have been slow to take up the new ideas. The reasons for this can be attributed to the very nature of the work. The Public Services and Works Department, for example, still operates in a fairly hierarchical manner, although initiatives by the Chief Executives' Office are fast transforming this mode of working (discussed in detail in the following sections). The Social Services Department also has a traditional approach towards its clients. Some employees feel that they were significantly constrained by their job descriptions and departmental boundaries.

The service care delivery process

Whatever the organisational forms and the mode of working, there is a common focus, across all departments, on service delivery. There are three main drivers for this orientation. First, the emergent governmental regulatory framework because of the Citizens' Charter. Second, the increased awareness on part of the citizens thus leading to greater expectations. Third, the "economy, efficiency and effectiveness" drive of the Audit Commission. As a result, the Local Council lays significant emphasis on measuring service performance as a means of improving service delivery.

Service delivery within the Local Council is a dynamic process with the customer being the focus of attention. The customers of local government often do not conform to the private sector model, where they actively decide their own needs and wants. The idea of a customers[2] is far more complex, with people having different status and varying degrees of control over the services they receive.

In providing services, the Local Council focuses attention on the needs and views of customers. The underlying purpose is to be more helpful, thus making it easier and more pleasant for the public to use the service. In doing so service delivery is envisaged as an input–output process (figure 5.1). A concerted effort is made to assure the quality of service delivery. In line with the Audit Commission requirements importance is given to economising on the nature, scope and orientation of the service. Data is constantly gathered from the public to assess and monitor service utilisation. Furthermore, because of the current trend towards outsourcing, extra effort is made to manage the contracts effectively. All these activities require the timely availability of the right kind of information. Consequently, there has been a renewed emphasis to develop computer based information systems that can best serve the purpose.

A greater need for precise information, coupled with increased customer orientation, is making the Local Council more results oriented. This contrasts with the earlier emphasis on methods and procedures for delivering services. Because of this new orientation, the pattern of use of information contained in systems is very different from the previous, more administratively oriented systems. The differences arise at three levels:

1. The usefulness of the systems is not limited to standard predefined reports. Instead, the systems are expected to respond to *ad hoc* requests.

2. Although predefined monitoring systems have been established and adequate information is generated for that purpose, there is an emergent need to provide information for short-term decisions. Increasingly, systems are expected to fulfil this need.

3. With an increased emphasis at present on customers, the heavy users are the professional and technical staff as opposed to the administrative departments.

This has resulted in 'patchy' systems developmental activities that have centred on specific subject areas and particular end users. Such efforts raise many interesting questions about system risks and infrastructural security. These are discussed in the following sub-sections.

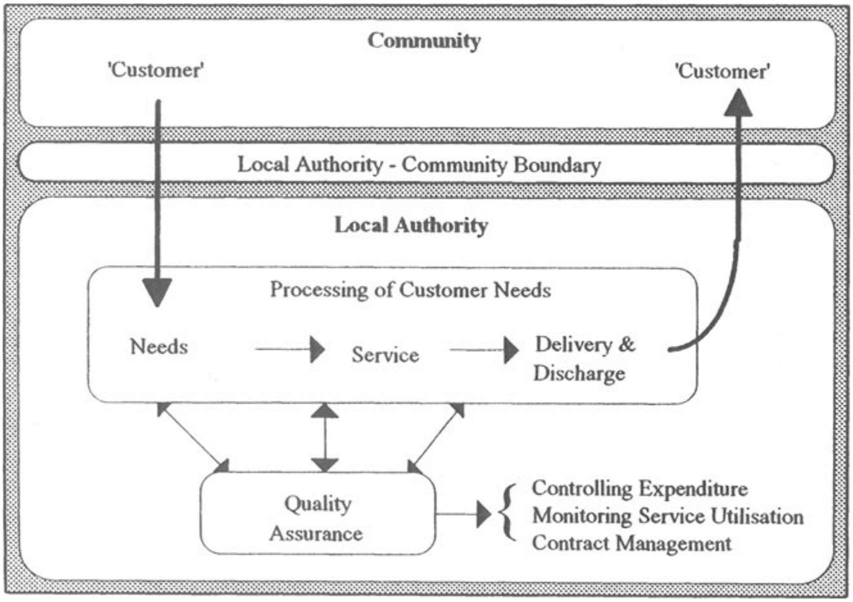


Figure 5.1 ***The service delivery process at the Local Council as envisaged by the management***

5.2.3 The IT infrastructure

The Local Council spends over one million pounds on the acquisition of personal computers and software each year. There are a number of Local Area Network servers within the Council. The Public Service and Works department, which was the focus of empirical study analysis, spends over £200,000 per year on information technology, in terms of hardware and software acquisition, on services from the IT department, or on direct charges.

Some of the key computer based systems within the Local Council are listed below:

- The *Electoral Register System* that is housed in the Council Secretary's department.
- The *Works Orders Processing System* for managing Council owned properties that is used by the Building and Architectural Services.
- The *Careers System*, the *School Administration* and the *Education Awards System* operate within the Education department. The functions range from basic school administration processing, calculation and payment of awards for school children and students in further education and to maintaining records of clients, vacancies and employer list.
- The *Housing Benefits System* processes Housing Benefits and issues payments and rebates. The system interfaces with numerous other systems within the council. There is also the *Housing Applications System* that holds applications for Council accommodation and transfers in priority order to reflect the Council's allocation policy.
- The Finance Department has a number of small systems dedicated to specific tasks. These include, the Centralised Cash System, Mortgages System, Sundry Debtors System, Sundry Income System, Commercial Rents System, Council Tax System, Non-Domestic Rates System, Creditors System, Benefits Cheque Reconciliation System, Payroll/ Personnel System, General Ledger System.
- The *Corporate Payments System* within the Personnel and Management Services department is used to enquire about payments made by the Creditors System.
- The *Planning Applications System* of the Planning and Transportation department processes Planning and Building Control Regulations applications throughout their life history. There is also the *Planning Decisions Analysis System* that provides statistical analysis of floor space, etc., and other changes arising from planning applications.
- The *Homecare System* within the Social Services maintains details of Home Helps and Clients, scheduling of visits to clients and payment processing for Home Helps.
- The *Excess Charges System* that processes car parking fines, including payments, reminders and court case details is used by the Public Services and Works department. The system interfaces with the Centralised Cash System and DVLA.

- The *Trade Refuse System* within the Public Services and Works department monitors the collection of trade refuse.

The above list is not exhaustive, but gives a flavour of the various applications within the Council. Each of the departments of the Local Council comprises a number of sections. These sections in turn have in place very specialist computer based systems. For example, the Public Services and Works department is constituted of 14 sections. Each has a dedicated system in place.

The computer based systems in the Local Council are based on ICL hardware. The main networked infrastructure within the Local Council comprises one Novell connected device, one live ICL OSLAN backbone (plus one reserve), one short backbone for the SUN Digital workstations, one in reserve for contingencies. There is also a thin Ethernet network linking the four text processing centres at the main location.

Security

Systems within the Local Council process information of varying degrees of sensitivity. It is of utmost importance that existing controls are not subverted, the systems are not misused and access is granted in accordance with the stated policy. The responsibility for checking compliance and auditing information system security resides with the Computer Audit Manager, who is placed within the Local Council Audit Services.

With respect to the networked infrastructure, security at present is largely restricted to managing access rights. The computer audit findings have, however, identified some interesting gaps. These shall be discussed at length in section 5.3. In terms of access control, the network supervisor access profiles are held by the Information Centre analysts (the Information Centre is part of the IT department). These analysts are responsible for the maintenance and installation of some thirty Novell Netware servers, as well as the network backbone infrastructure including mainframe and external links. This access allows full read, write, amend and delete access to client data to take place without the knowledge of, or control by, the user department. The current Netware version allows network supervisors to do anything with the data without leaving any audit trail. Furthermore the security of the network is managed by the analysts on a `quick-fix' approach. Problems are tackled as and when they appear and the analysts set their own priorities.

In evaluating and analysing the security requirements, the Audit department uses a four-stage approach:

Table 5.1 The security review method at the Local Council

Stage	Description	Activities performed and techniques used
I: Interviewing	Interviews are conducted with Computer Liaison Officers[3] within various departments.	Location, environment and maintenance is assessed; access control is assessed; acquisition of h/w and s/w is assessed; Data Protection Act compliance is assessed.
II: Exploration	Documentation, testing and analysis of preliminary findings.	The above situation is matched with extensive checklists. The checklists present all possible controls within a specific environment.
III: Detailed examination	Further examination of areas of concern.	A qualitative judgement of potential problems is carried out by the Computer Auditors.
IV: Reporting	Findings are reported to the departmental heads.	A descriptive report with recommendations is prepared by the Computer Audit Manager.

The security reviews at the Local Council have a very qualitative character. Questionnaires, observations and audit software are used to assess the potential vulnerabilities. The actual implementation of the technical controls is carried out by the analysts within the IT department. With respect to the non-technical organisational measures, recommendations are made to the respective departments. It is not the responsibility of the computer auditors to see through the implementation of the controls.

5.3 The case study

The previous section of this chapter described the contextual aspects of the Local Council. The social, economic and political environment of local government was described. The management operations and the IT infrastructure were also explained. This section critically analyses the various aspects of the Local Council. The framework developed in chapter 3 is used to analyse critically various aspects of the organisation. The main focus is on interpreting the management of information system security. The analysis is based on table 3.1 and considers the most generic human and cultural aspects as well as the more specific issues related to form and means. This gives a rich picture for comment on the implications for the security of information system within organisations.

5.3.1 Analysis of the 'business world'

The analysis of the 'business world' of the Local Council helps in reviewing the organisational purpose and its relationship to the use of information technology. This allows us to interpret the implications for security of information systems. With respect to the management of information systems, three distinct stakeholder groups can be identified. These are the Chief Executive and his advisers, the auditors and the user departments. The following paragraphs discuss the business world issues in relation to these three groups of stakeholders.

Organisation of the three groups

For the purpose of this analysis, the Chief Executive and his advisers would be called the 'Strategy Group'. This is because this group of people had a broader vision than that of the departmental users or even the auditors. The Strategy Group is largely the Chief Executive himself, the support staff from the Executive Office, and some key people from the IT department[4]. The orientation of this group has significantly changed over the past few years. This has largely been in line with the contextual trends discussed in the previous section. Interviews with members of the Strategy Group revealed three distinct phases in evolution of the management style within the Council. These are: 'corporatism', 'professionalism', and 'federalism'[5] (figure 5.2). The use of information technology within the Local Council has also matured accordingly.

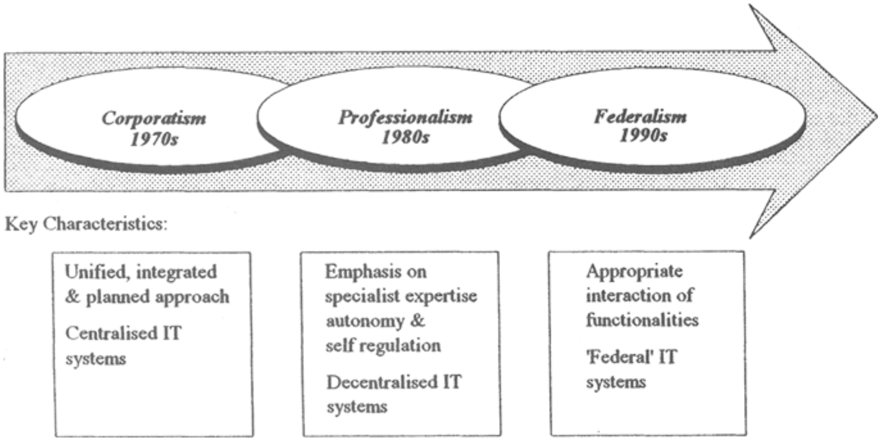

Corporatism
1970s
Professionalism
1980s
Federalism
1990s
Key Characteristics:
Unified, integrated & planned approach
Centralised IT systems
Emphasis on specialist expertise autonomy & self regulation
Decentralised IT systems
Appropriate interaction of functionalities
'Federal' IT systems

Figure 5.2 Trends in the Local Council

In the mid-1970s, the Local Council was passing though a 'corporatism' phase. This was the time when all managerial problems were considered to be interrelated. Hence a unified, integrated and a planned approach was considered appropriate. This period saw a concerted effort towards centralised information technology systems. The Local Council focused on providing a number of discrete services, each connected to a distinct environment. In later years, typically until the mid-1980s, the dominant notion among top managers in the Local Council was 'professionalism'. The emphasis then was on specialist expertise with a consequential stress on autonomy and self regulation. Therefore the thrust was on effectiveness of the services provided. By this time information technology infrastructures had also become significantly decentralised. In recent years however, there has been a growing trend towards 'federalism'. Federalism connotes the appropriate interaction of various functionalities. Though the organisation as a whole remains united, the individual departments retain significant independence. Such a situation has significantly been aided by the development and use of computer networks within the Local Council. The aim of the senior management in the Local Council today is also to develop a 'federal IT infrastructure'[6].

In spite of the changes in the immediate environment, the user departments have largely remained unchanged. They have inherited a traditional hierarchical structure. However, the extensive use of information technology and networking is flattening organisational structures. The departments no longer have strong internal coalitions. There is a growing trend towards making strong links with external parties. The IT department for example has largely been outsourced. The situation is further complicated by increased competition. Because of pressure afforded by an ever-changing environment and imposition of federal structures, the departments feel that they have little strategic control over their operations. This has resulted in a strong criticism of top down standardisation drives. For them the onus is on being more responsive to business needs. The Strategy Group on the other hand considers this environment to create 'non-standardised islets of service expertise' that are incompatible with the rest of the organisation. Furthermore, it feels that there is no central control on overheads with an imbalance in scales of economy, and no critical mass of skills. The conflicting objectives of different stakeholders are represented in figure 5.3.

The Strategy Group recognised these differences and hence started considering a more federal structure in its management. In terms of use of information technology, the Strategy Group objectives have largely been based on a mainframe culture, whereas the user department objectives show a resemblance to decentralised end user computing environments. It is envisaged by the top managers within the Local Council that needs of the networked environments of the future would be appropriately addressed by the 'federal objectives'. The changing orientation and adoption of new technological infrastructures have posed a complex set of problems for the third group of stakeholders – the auditors. Their main concern is with respect to their competence to address the changing needs. The implication of these changes and their responses are examined in detail in the sections that follow.

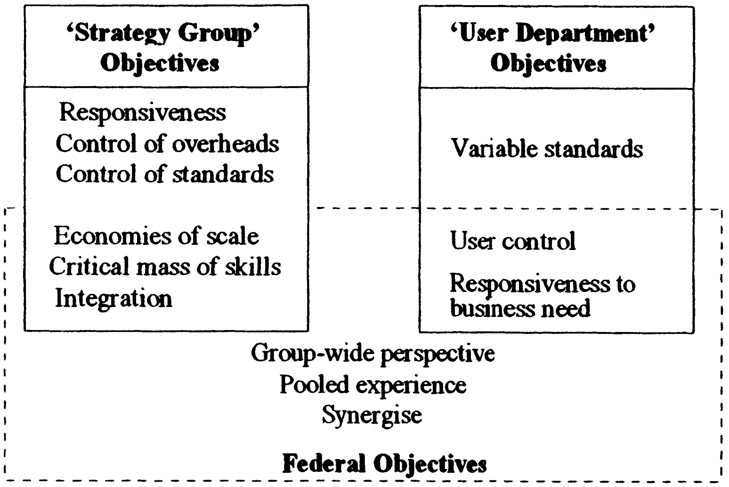


Figure 5.3 Differing objectives of the stakeholders

Differing expectations, obligations and the value system

The structural changes within the Local Council have fostered significant transformations in the expectations, obligations and value systems of the different stakeholders. The present Chief Executive is an information technology enthusiast. In his current job he has a vision to change the culture and attitude of the people within the Local Council. This, he thinks, is possible if everybody in the organisation can communicate freely. With this conception in mind, an 'Electronic Communication Initiative' was launched in 1994. Underlying this vision is a more pragmatic need. Since the context is becoming market oriented, the Chief Executive views the Local Council as a network of service purchasers and providers. In such an environment information and communication are a key to enabling the links between a diverse range of services. This belief also ties in with the federal structures and infrastructure espoused by the Strategy Group.

The users on the other hand consider these strategies to be of no use. As one section manager in Public Services and Works put it, "...what's the use, they do not understand our needs". In this case reference was being made to the organisation wide networking initiatives. Another manager, stationed at one of the Depots, went on to say that there was a clear communication gap between what is planned and what actually happens at the front end. This is an indication of a mismatch between the corporate agenda and the development of information technology infrastructures (this issue is discussed in detail in the next subsection).

Further investigations into the beliefs and values of the users revealed two distinct groups: a group that believed in the ideals of 'federalism' as presented by the Strategy Group, and one that was more traditional in orientation and believed in autonomy and self-regulation. Those in the latter category were mostly based in the sections and had little or no contact with those in the Strategy Group. In this regard there appears to be a core concern about the manner in which the Strategy Group conceives and enforces its ideas. No doubt there are arguments in the literature (e.g. Cooke 1992) that encourage management changes for maintaining the quality of service provision, but there is also a clear mention of involving the front-line people. Taylor (1988), for example, notes that:

> Most of the best ideas for improvement on the ground will come from individual members of staff. Regular job consultation and/or performance appraisal schemes might be considered, along with finding other imaginative ways of further unlocking and unleashing the drive, energy and enthusiasm of the workforce. (p2027)

In the case of the Local Council there is a mismatch between the perceptions of different groups and little effort has been made to involve the front-line staff. Part of the blame can be attributed to the differing obligations of the people concerned. One front-line manager pointed out that most people are interested in getting on with their job rather than being held back to fill another form or download data on to the main computer system.

In such an environment the auditors are faced with a tough job. Their main concern has been with the 'loss of reference'. The constantly changing structures and management thrust mean that auditors have to rely on formal systems of control. These are far detached from reality, hence auditors often end up checking the integrity of the systems and processes. As Brunsson (1990) points out, the auditing function in itself is becoming a means to formalise the allocation of responsibility without interpreting the cultural consequences. Computer auditors in the Local Council have indeed been looking at the physical and logical control issues, ignoring the deep-seated pragmatic aspects.

Consequences for the information system and security

It has been noted in the previous section that different groups within the Local Council had conflicting objectives and expectations. This section analyses the implications of these divergent premises for the information systems in place. It is important that corporate vision of an organisation is reflected adequately at the level of service delivery. Not only should there be a proper system of communication between the top echelons of the organisation and the bottom rung, but also a common consensus with respect to the implementation process. This means that everybody in the organisation interprets the corporate philosophy in the same manner. Any shortcomings in this regard would reflect inadequacies on the part of the management.

Though the underlying ethos of the Local Council's management philosophy is 'customer care', the corporate vision centres around developing a networked authority (see figure 5.4). This vision is reflected in the corporate strategy and even the information technology strategy. The corporate vision is rooted in three fundamentals. First, that responsibility for service delivery and control should be devolved to the lowest levels. In many cases this may lead to certain services being outsourced. Second, that an intelligent infrastructure should be developed such that services are linked with the customers and corporate policy. Third, that within the Local Council information should be managed as a resource. For the IT department this involves developing an attitude to share along with the technical capability and access to computer directories across the organisation.

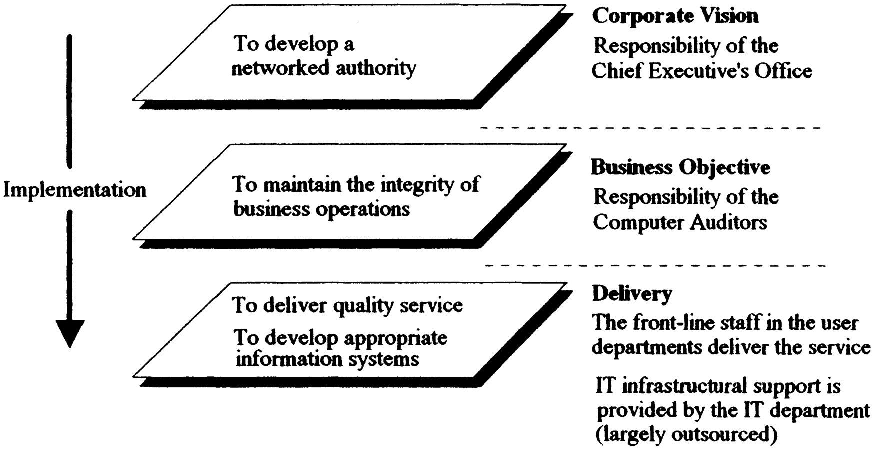

To develop a networked authority
Corporate Vision
Responsibility of the Chief Executive's Office
Implementation
To maintain the integrity of business operations
Business Objective
Responsibility of the Computer Auditors
To deliver quality service
To develop appropriate information systems
Delivery
The front-line staff in the user departments deliver the service
IT infrastructural support is provided by the IT department (largely outsourced)

Figure 5.4 Levels in the Local Council's corporate strategy

The current corporate vision of the Local Council has emerged from the changing role of information technology. The Strategy Group recognises that change is sweeping the authority, and hence the corporate objectives need to be aligned to the new needs. As the Executive Adviser to the Chief Executive writes in one of the internal circulars, "new ways of working and new relationships open up as information and communication technologies converge. True partnership of business understanding and technical understanding leads to opportunities for redesigning the organisation". He went on to say that in line with the federal information technology strategy espoused by the Strategy Group, information and communication technologies are set to become a vehicle of empowerment in the Local Council. Powerful small machines and communication networks mean that users can obtain and manipulate locally the information that they require. In due course these networks are destined to become a means to link purchasers and providers, thus facilitating an integrated delivery of local services. It is envisaged that this will facilitate the provision of quality services to the Council customers.

However grandiose the vision might appear, there are real concerns at the level of service delivery. The front-line staff in the user departments within the Council are typically asking three sets of questions:

1. **Why is it that the Strategy Group does not understand our needs?** Because of this, the communication gap between different stakeholders is ever increasing. This is reflected in the manner in which the corporate strategies are operationalised. For instance, the user departments were given a substantial amount of freedom to purchase information technology services, but with the adoption of new infrastructures this is changing. Having encouraged a decentralised infrastructure, the top management began enforcing a new vision, the vision for a networked authority. In many ways this relates to the top management desire to curtail the powers of the user departments – though under the banner of federalism[7].

2. **Why are we not getting value for money?** The user departments have become more cost conscious, especially after the introduction of compulsory competitive tendering and service level agreements. The purchaser/provider split has raised the expectations of the user departments. This issue has been further complicated by the continued orientation towards distributed computing.

3. **Why are the promised projects not being delivered on time?** The concern with user departments is not to see the realisation of the corporate vision, but something more immediate. Since they are paying for most information technology projects, they are interested in knowing why the IT department fails to deliver the 'goodies' on time.

The failure of the top management to address the immediate needs of the user departments and the growing trend towards outsourcing are threatening the core objective of the Council, i.e. provision of quality service. This synthesis does not indicate that corporate policies have not been developed properly. Rather the converse is true. The changes introduced are indeed in line with the contextual demands, but the means adopted in implementing changes have been rather myopic.

The developments at the corporate and service delivery level have further raised questions about the medium term strategic objectives of the organisation. It is extremely important for the Local Council to maintain the integrity of its operations. This is so because the strategic vision and the operational objectives depend so heavily upon information for their success. The availability of information not only helps an organisation to co-ordinate and control its internal and external relationships, but also influence the effectiveness of an enterprise. Therefore, any disruption in the information and communication systems or in the organisational operations has a detrimental effect on the entirety of the concern and the systems that support it. In the Local Council, the function of maintaining integrity has been the responsibility of the auditors. Because of a mismatch between the immediate service delivery objectives and the corporate vision, the computer auditors have had a narrow focus on 'system based audits'. Power (1994) explains such audits as those that "can easily become a kind of ritual, concerned with process rather than substance, and governed by a 'compliance mentality' which draws organisations away from their primary purpose" (p19-20).

In light of the theoretical orientation of information systems and security approaches, security audits at the Local Council can be termed as functionalist in nature. One of the key characteristics of such approaches, identified in section 2.3.1, is that management of information systems and security is considered to be processual in nature. Hence a typical auditor tends to ignore (or overlook) the context in which information is being processed. This forces the auditor to compartmentalise the problem domain and concentrate attention on the technical edifice. As Power (1994) notes:

> Rather than examining large quantities of transactions, auditors focus on the control systems governing those transactions ... the truth is that they are rationalising a shift away from direct contact with practices which has been primarily driven by cost (p19).

Such an orientation raises concerns about the prevention of the occurrence of adverse events. Since the auditors seem to be less concerned with the integrity of the organisational purpose and are focusing more on the procedural controls, the antecedents to potential negative events are not being evaluated.

The next section elaborates some of the issues and conflicts identified so far. The cultural and political aspects related to the information technology infrastructure are highlighted. It stresses the importance of maintaining the integrity of the whole organisation, rather than of just the information technology infrastructure. In doing so it points towards management considerations for maintaining information system security.

5.3.2 Analysis of the pragmatic aspects

The previous sections highlighted the growing trend within the Local Council towards federalism and federal information technology infrastructures. This section elaborates the federal information technology architecture within the Council and specifies the consequences for information system security.

Characteristics of the federal information technology infrastructure

The federal systems environment, as it exists in the Local Council, comprises a general ledger, its feeder systems (e.g. payroll and creditors) and the personnel systems that are linked to the departmental and sectional systems. Initially these systems started as mainframe applications, but with improved technology the departments have been given substantial control. Federal architectures have been imposed on the departments. These have however been 'afterthoughts'. In order to operationalise the structures, the departments are required to input relevant information into the central information systems. Figure 5.5 takes the example of the Public Services and Works department to depict the architecture. Though initially it was thought that links would be established with the existing systems and only marginal new systems development activity would be undertaken, in reality the federal IT infrastructure is taking the form of a parallel council wide integrated information system. This results in duplication of work since in many instances the staff have to input data twice, first into the departmental and sectional computers and second into the council-wide systems. This observation was made within the Public Services and Works department.

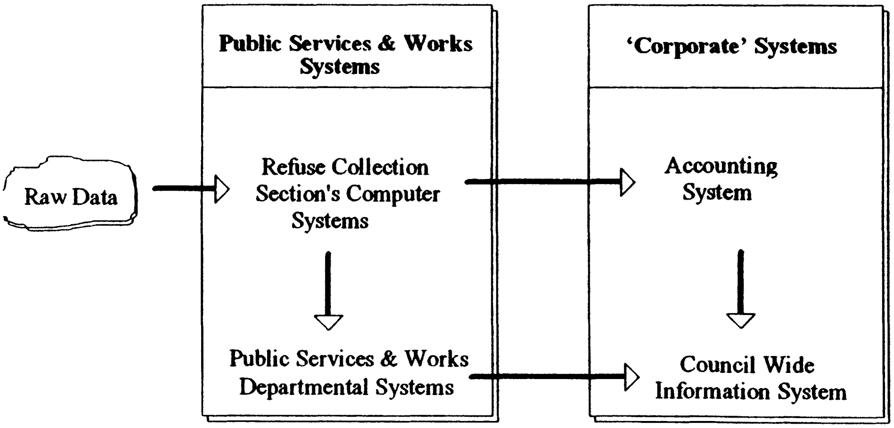

Public Services & Works Systems
'Corporate' Systems
Raw Data
Refuse Collection Section's Computer Systems
Accounting System
Public Services & Works Departmental Systems
Council Wide Information System

Figure 5.5 Towards a federal information technology infrastructure at the Local Council

The Local Council uses another buzz word for its federal information technology infrastructure – the 'intelligent infrastructure'. It is envisaged that at the heart of an intelligent infrastructure is the capability to share. Although some of the aspects of the intelligent infrastructure have actually been operationalised, a few are still in the conceptualisation and developmental stages. Typically an 'intelligent infrastructure' consists of an organisation-wide electronic communication infrastructure. It is believed that paper will be largely replaced by electronic means of exchanging information. Communication between locations, between different aspects of a service, across services and with the community will be developed. There will also be a new architecture that will integrate voice, images, text, sound, video and graphics. Typically a single device could be used by staff 'in the field' for voice/data communication with the centre and others. There will be a library of software and information 'components', which will enable new systems to be created and customised to specific needs through the use of software tools. Narrating the benefits of such efforts the manager responsible for the Geographical Information Systems explained how useful such systems would be to "extract new information from existing data by providing a new way of looking at data". He went on to emphasise the success of text retrieval systems within the Local Council and the ease with which it is possible to extract information from existing sources. Within the overall effort to develop a federal IT infrastructure, the Public Services and Works department has been chosen as a pilot site.

However rational and useful the federal information system architectures may appear, there are inherent problems. The information systems requirements are constantly shifting because of changes in organisational procedures, in systems in place and because of incompatibility of data. A particular case in point is the introduction of compulsory competitive tendering. Furthermore, the constantly changing environment has significant cultural implications. Although in the beginning the cultural issues may not appear to be important, they have a substantial bearing on the security and integrity of the business processes. The next part of this section considers this issue and interprets the consequences for information system security.

Cultural implications for information system security

It has been argued that if analysts and business managers do not take a holistic view of the organisations, technology driven information systems invariably fail (Ambaye and Hayman 1995). Furthermore, a mismatch between the needs and goals of the organisation could potentially be detrimental to the health of an organisation and to the information systems in place (Dhillon and Backhouse 1996). This indicates that organisational processes such as communications, decision making, change and power are culturally ingrained and failure to comprehend these could lead to problems in the security of information systems. This has been recognised in the previous chapters, hence emphasising that security should not only be considered in terms of physical access controls and data integrity, but the deep-seated culturally ingrained issues should also be addressed.

In understanding the role of information systems within organisations, it has been argued that emphasis should not be on how people comprehend and use technology, but on how groups of people within an organisation behave and interact with information (Boynton and Zmud 1987). This indicates that basic human attributes such as behaviour, attitudes, values, management expectations are a key to interpreting the use and misuse of information. In fact the totality of such attributes represents the security culture of an organisation and contributes to the protection of information of all kinds (also refer to section 4.3.2.).

The Local Council, where a federal information technology infrastructure is being implemented, is a good case in point of the technological edifice affecting the manner in which people work and relate to each other. These patterns of behaviour are generally shared among different individuals and groups of people and their totality constitutes the culture of the enterprise. Within the Council, over a period of time different members of the organisation have shared various work patterns and it is believed that any disruption in these would be a cause for concern. To illustrate this contention, let us take the issue of monitoring service performance. It has been observed that beliefs and values of people have indeed been significantly affected. With increased decentralisation of services within the Council, individual departments and sections have been largely responsible for judging the level and adequacy of service provision. However, with a strategic thrust towards federal structures a 'superstructure' is being imposed on to the existing architecture. In the Public Services and Works department for example, the monitoring of Refuse Collection has been the responsibility of the sectional head. Interviews with various people within this sub-group revealed that there have been absolutely no problems with the either the function of refuse collection or with service performance. However, the Strategy Group is operationalising a 'federated' structure whereby it will be the responsibility of the refuse collection Scheduling Manager not only to update and judge his own performance but also to provide data to the corporate system in a format determined by the Executive Adviser. This is not only leading to the development of a parallel IT infrastructure, but also doubling the workload of the people in the Refuse Collection section (refer to figures 5.5 and 5.6).

Because of the changing roles and expectations of members of the organisation, largely triggered by the demands of the Strategy Group (the Executive Adviser being the responsible person), there are certain attitudes expressed by the Scheduling Manager in the Refuse Collection section. The net outcome of the attitudes is difficult to determine; however, some judgements can be made by determining the degree of assertiveness on the part of the Executive Adviser. If we consider the Executive Adviser's (Role 'X') demand as a communication act, then the Scheduling Manager (Role 'Y') could possibly express four kinds of attitude (figure 5.6). These attitudes are with particular reference to 'what is spoken about' and 'what is said'. In our example the reference relationship is with 'customer service provision' monitoring as distinct from the normal reporting practices.

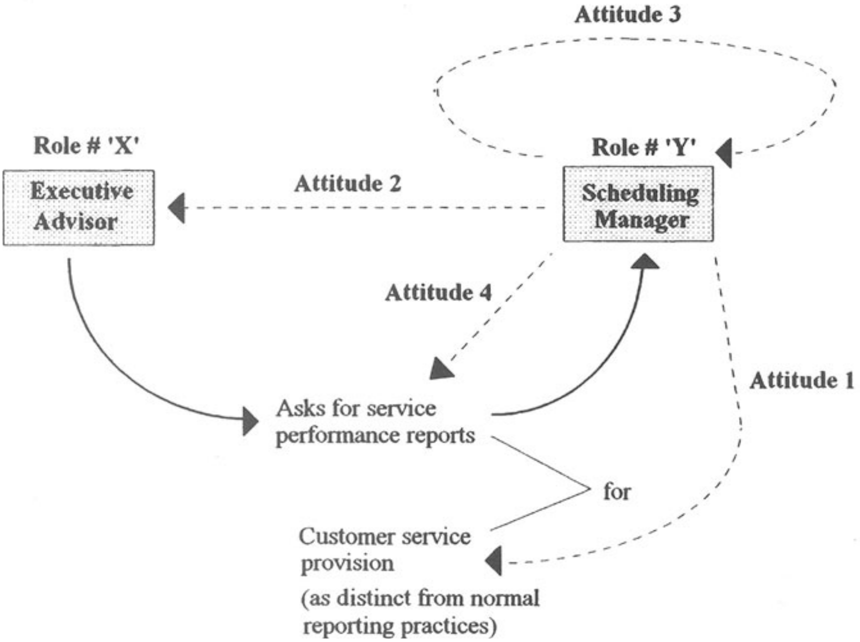

Attitude 3
Role # 'X'
Executive Advisor
Attitude 2
Role # 'Y'
Scheduling Manager
Attitude 4
Attitude 1
Asks for service performance reports
for
Customer service provision
(as distinct from normal reporting practices)

Figure 5.6 Emergent messages: attitudes signified by top management IT initiative

The attitudes of Role 'Y' towards 'X' in our example are as follows:

Attitude 1: With respect to demanding performance reports, the incumbent in Role 'X' significantly influences the attitude of Role 'Y'. These reports relate to the performance of a particular individual or a group, judged against criteria identified by Role 'X'. The reports are required over the network in electronic form, creating a parallel infrastructure to what already exists. This can cause a lot of discontentment, disillusion and alienation for Role 'Y'. Since the attitude of Role 'Y' towards the subject being referred to will be uncooperative, a possible future outcome could be circumvention of controls and inputting misleading or false data into the system. This could result in various negative outcomes.

Attitude 2: By imposing certain structures, Role 'X' actually engages in a communication act that leads to influencing Role 'Y's attitude such that it affects Role 'X'. Since the position of Role 'X' within the management hierarchy is advisory in nature (a typical staff function), it significantly influences power relationships between sectional heads, departmental heads and those in the Chief Executive Office. Traditionally, all monitoring and service performance reports passed through a hierarchical structure (sectional head through to departmental heads and then to the Chief Executive Office). Now the use of information technology and direct mode of communication between two very different levels is actually leading to much talked about notions of 'delayering' and 'flattening out'. In such an environment, if the attitudes of key players are not managed properly, at some stage these very people may end up as 'disgruntled employees' and are therefore potential sources of negative events.

Attitude 3: At a less conscious level, a combination of all the contextual issues may lead to a significant change in attitude of Role 'Y' towards itself. A possible outcome could be loss in morale, self esteem and confidence. Again the very purpose of bringing about the changes will be defeated. Rather than enhancing the level of customer service provision, in real terms it will actually decrease.

Attitude 4: The attitude of Role 'Y' towards the message itself is interesting. There would be different outcomes if the communication is human or if it is computer mediated. In the latter case there is a possibility of Role 'Y's morale being boosted, since personal communication with members of the Chief Executive Office gives a significant amount of power and legitimisation to the activities. However, in the former case, the consequences could be adverse since a computer may be seen as a new 'boss'.

It becomes clear from the above analysis that if the context is not carefully examined, top management may end up having a neat set of figures for productivity levels and customer satisfaction, but may not achieve a satisfactory rapport with the staff. On the other hand if the attitudes are analysed and managed adequately, there could be a good working relationship among different parts of the organisation. This will lead to an organisation having human resources that are trustworthy, responsible and of high integrity – virtues that are extremely important for developing secure environments.

Analysis of the silent messages and the related security concerns

The previous section illustrated how computer based systems affect the attitudes of people in organisations. Such implementations are in fact silent messages being communicated and can help us in understanding the patterns of behaviour and the culture of the organisation. If not managed properly, intentional changes in the culture can lead to significant security concerns. This section draws out the underlying silent messages and their implications for information system security. These are based on the various categories of silent messages drawn from Hall (1959), table 5.2 summarises the interpretations from the silent messages (see appendix for a description of Hall's culture map).

When interpreting the implications for security through Hall's culture map, not all elements are of equal significance (a similar situation existed in the case of CIS in the Hospital Trust). In table 5.2, 'bisexuality' and 'play' streams are excluded. Analysis is done by considering the direct actions taken within the organisation (1st column of table 5.2). Then significance of the actions in other parts of the organisation is assessed (2nd column of table 5.2). Finally, interpretations for security are drawn; these link the effect of actions to the negative events (3rd column of table 5.2). In many cases various possible scenarios are sketched. The interpretations are based on a combination of reflexive thinking and critical analysis of comments made by different stakeholders. Analysis of each of the culture streams is described below. The complete analysis is presented in table 5.2.

Interaction. The introduction of a federal information technology infrastructure has established new communication patterns between departments/ sections and the Strategy Group. The new IT infrastructure has been used to introduce a service performance monitoring system. This has implications on the patterns of interaction between different stakeholders. The front-line staff, who are immediately affected, are seeing a change in their status and role. Furthermore, the time of interaction has significantly changed the working patterns. Such direct organisational interventions have significant implications for security. Foremost, the stable and cohesive group structures are being threatened. This has led to the organisation striving to develop a shared vision. If such changes are not managed properly, there is a high potential of communication breakdowns and the 'creation' of disgruntled employees – thereby increasing the risk of negative events.

Association. The federal information technology infrastructure is evolving into a environment of cybernetic control. Since the Audit Commission considers customer service as a top priority, the Strategy Group within the Local Council wants to control and monitor the service delivery process. Thus in many ways the top management is imposing a corporate vision on to the departments. Consequently, different groups are reassessing their own position in the light of the corporate agenda. Such organisational actions do not help in developing a common culture. An organisation that is 'culturally fragmented' has difficulty in dealing with eventualities.

Subsistence. Pressures from the Audit Commission to be more customer oriented have increased the information needs of the Council. Hence the traditional reporting structures are being questioned and the organisation is being 'flattened' and delayered. Since there are financial pressures as well, the Council is becoming more cost conscious. This has brought the auditing function to the centre stage. The complex interplay between these contextual factors has resulted in the federal information technology infrastructure, whose sole purpose is monitoring. This has resulted in formalisation of predominantly informal activities. At the present time there is an increased risk of misuse and abuse of

Table 5.2 Examples of silent messages conveyed at the Local Council: interpreting the implication for security ***(The categorisation is based on E T Hall's Primary Message Systems. Only relevant streams are shown, represented by numbers in the 1st column – the primary impacts. Numbers in the 2nd column are the cell numbers from the culture map – the secondary impacts.)***

Direct organisational intervention through IT	**Significance in other cultural areas of E T Hall's map**	**Implications for security**
(0) New communication pattern between the departments/sections and policy group. Introduction of a new work concept - monitoring service performance. A new IT based system is implemented.	(00) Patterns of interaction between different stakeholders change. (01) Possible status change for front line staff. (05 & 09) Complex interplay between times of interaction between individuals and imposition of a new way of working.	Fairly stable and cohesive group structures are threatened. The organisation strives to develop a shared vision. If not managed properly, there is a high potential for communication breakdowns, and 'creation' of disgruntled employees
(1) Introduction of a federal information technology infrastructure that the whole organisation has to adopt. All customer service issues shall be monitored by the Executive Office.	(11) Top management imposes its corporate vision on to the departments, different groups reassess their own position vis-à-vis the corporate agenda. (14) Individuals and groups feel threatened in terms of encroachment on their 'territory'.	Problems in developing a corporate vision and a security culture because of a 'them and us' attitude. This is because of conflicting objectives within the organisation.
(2) Increased need by the Local Council for information – typically because of audit commission requirements and guidelines in the Citizens' Charter. Information has become a basic physical need necessary for subsistence.	(21) Traditional reporting structures are being questioned – trends towards 'flattening out' and 'delayering'. (22) Cost effectiveness has become the primary criteria for evaluation. (24 & 25) There is an increased focus on auditing.	Introduction of a system whose sole purpose is monitoring tends to formalise the traditionally informal activities. The existing business processes do not support the overall vision, thus introducing far greater risks.
(4) The computer system is located at the service delivery level. In the ultimate networked environment the system will bypass departmental hierarchies.	(46) Empowerment of the front-line staff will encourage ownership of their tasks. (48) Ownership leads to responsibility structures that give protection to systems. (49) There will be the rationalising of services with an increased role for system integrity and auditing.	'Empowerment' and 'ownership' objectives raise questions about power, responsibility and authority. This is a major security concern. There will also be problems of defining territoriality objectives.

(5) New information technology architectures introduce new conventions about time and scope of the activities.	(54) Rigidity of the new architectures and predetermined performance criteria hinders further development; this changes the nature and scope of the groupings.	The imposition of a kind of integrated system results in the parallel development of two IT infrastructures. This raises serious policy and strategy questions. The result is the loss in integrity of the systems with business processes becoming vulnerable.
(6) The new infrastructures induce an increased orientation towards customer care.	(62) The service monitoring criteria may have an educative content. (64) Learning is location independent.	Though the federal structures have potential benefits, planning needs to be done properly. Programme needs to be marketed properly.
(8) In the light of new systems being introduced, the use of security audits have been stepped up.	(81) Power and authority structures are questioned since auditors take on the role of 'policing' the organisation. (88) Security auditors mostly explicate the technical defences, with little or no concern for formal and informal.	Only technical controls are recommended. Some advice on rules and structures is also given. Little consideration is given to the development of security culture, awareness and training.
(9) The Local Council aspires to be a networked authority where no paper is used.	(90) There are concerns for 'trusted' communications. (91) There are concerns for developing future organisational competencies.	Major security concern emerges from a sudden change in breaking up hierarchical structures and delayering of the organisation.

the computer based systems, because the existing business processes do not support the overall vision. In this environment the computer based systems seem to have a dubious role.

Territoriality. The introduction of a federal information technology raises some serious concerns about devolving departmental hierarchies resulting in empowerment of the staff. As a result, increasingly the employees will have to take responsibility for their tasks. Coupled with the rationalisation of services, in the future the organisation will have to have an increased focus on system integrity and auditing. Since such federal systems question the traditional notions of territoriality, the organisation will have to make explicit the structures of responsibility, authority and accountability. Failure to do so will affect the management of information system security.

Temporality. The information technology architectures at the Local Council introduces new conventions about time and scope of the activities. The federal structures have largely been imposed on to the user departments, thus forcing the front-line staff to reorient their activities. Furthermore, the new information technology infrastructure is developing as a parallel system, thereby raising serious policy and strategy issues. This calls for a renewed effort for information systems and security planning.

Learning. Although the new federal infrastructure has potential benefits, it needs to be planned properly. Typically, such an infrastructure forces people to think about their performance and educates them about customer care. However, over-formalisation has resulted in dissatisfaction and rancour at different levels of the Council. Such an attitude has severe implications for the occurrence of adverse events.

Defense. Having recognised the importance of security, the Council uses auditors to identify the vulnerabilities and make recommendations about instituting controls. Although the auditors tend to question the power and authority structures, the focus has been the technical control systems. Very little has been done with respect to developing a security culture and establishing awareness and training programs.

Exploitation. The Local Council aspires to be a networked authority. Hence it is important that needs of the emergent organisational form are addressed appropriately. As of now it appears that the organisation does not have the competence to manage such a complex environment. The break up of hierarchical structures and delayering can potentially lead to a number of negative events. This necessitates the importance of proper planning, both at the corporate level and for security.

Discussion

It is clear that when a new computer based infrastructure is introduced into an organisation, significant cultural changes take place. These have inherent implications for the security of the computer based infrastructure and for the organisation as a whole. Analysts often consider their systems to be secure if necessary password protections have been put in place. However our analysis of the silent messages within the Council reveals that there are many aspects of security that are not technical in nature. It is therefore important also to address these other social and organisational issues.

An important issue emerging from the analysis so far relates to the communication of the intentions of different actors. Considering the implications of direct interventions with respect to the information technology infrastructure, it becomes clear that only if the intentions are communicated properly could the security risks be minimised. This can be done by using Hall's (1959) threefold classification[8]. Within the Council, at a formal level the new IT infrastructure is imposing a totally different set of rules. The traditional organisational structure is extremely hierarchical where IT infrastructures are extremely decentralised. The new infrastructure imposes rules that advocate delayering and integration of the IT infrastructures. Consequently, there are problems of consistency between the overall purpose and operational practices. The second mode of communication is informal. It may not be possible to explicate and formalise such communications. However their understanding leads to the interpretation of many subtleties of behaviour. This is extremely important when our primary concern is with developing secure environments. Research has shown that it is generally the established employee who is the major cause of internal breaches (Audit Commission 1994; Backhouse and Dhillon 1995b). Understanding of informal modes of communication helps in 'nipping the evil in the bud'. The third form of communication is technical. In the context of the Local Council, though a federal IT infrastructure may be the best option, the users need to understand the rationale behind it. In spite of the fact that most users are highly aware of IT infrastructural issues, the ideas need to be sold properly.

The next section considers the semantic aspects of the IT infrastructure within the Local Council. Particular attention is give to the meanings associated with different communications and the related structures of responsibility. In a final synthesis implications for security are drawn out.

5.3.3 Analysis of the semantic aspects

The usefulness of understanding the meanings of our actions has been well researched into (Backhouse and Dhillon 1995a; Manning and Cullum-Swan 1994; Donnellon *et al.* 1986). The findings of the previous chapter also bring home this aspect. In the case of the Local Council and its efforts to introduce a federal IT infrastructure, the issue of understanding the content and meaning of different organisational actions gains prominence. This section analyses these meanings and relates them to varying patterns of behaviour. Since these meaning structures underscore the entirety of organisational functions, interpretations for information system security can be drawn.

Organisational actions and emergent reactions

Organisational actions within the Local Council have largely been context driven. Over the last two to three years, a series of changes and rationalisations have been considered within the Council and many of these have been implemented. Information technology has played an important role in this change process. Managers within the Local Council feel that in future IT based systems are going to be of strategic importance to the Council. The Deputy Director of Public Services and Works department considered the particular usefulness of such systems to be in the area of "progressive and planned introduction of competition". He felt that immediate future developments would take place in the areas of customer care, parking enforcement and performance review. People from different parts of the organisation seemed to agree that the net outcome of all the changes would be a further increase in the use of computer based information systems.

While discussing the contextual changes and the related organisational responses, one of the managers in the Public Services and Works department compared the situation to a jigsaw. He said, "there are a lot of brightly coloured pieces around – citizens' charter, customer contracts, total quality...". And the current emphasis of the Strategy Group is to "wedge together a bunch of pieces", without any consideration to whether they fit. In a separate discussion with the Computer Audit Manager, this viewpoint was endorsed. In fact the Strategy Group at the Local Council was involved in 'fitting together incompatible pieces of the jigsaw'. However bright the ideas and initiatives might be, unless they are placed into a coherent whole, organisational efforts are dissipated.

In the case of the Local Council, the scenario presented above becomes clear. Since the council is characterised by a highly decentralised IT infrastructure, the work patterns are such that they are not technology led. This can be illustrated by considering the issue of customer care. For years the sections and departments have had manual complaint monitoring systems in place. With the advent of specialist software packages used by departments and sections, complaint monitoring systems have been built into them. Thus the quality of service provided is regularly monitored at the departmental/section level. For instance, the Waste Management section uses an off-the-shelf package to monitor waste collection in the Council. The computer system, which has been well accepted by the section, helps in penalising contractors for their infringements. Managers of the section see this as customer care at the operational level. When the Strategy Group attempts to introduce an information system that will presumably facilitate customer care, the individuals at the departmental level do not see the utility. Rather than considering computing and communication technologies to enhance customer care, they are getting the feeling of a 'big brother watching them'. Over a period of time the organisation has developed potent norm structures and so there are fears that these structures and social groupings would be broken. Consequently, at the departmental/sectional level, where the use of technology has been incidental to the normal functioning of the organisation, implementation of any 'technology-led formal systems' faces strong resistance. Resistance at the departmental level is indicative of poor management rather than inappropriateness of the changes.

The Strategy Group however views the changes differently. In line with the general beliefs of the CEO, it aspires to make the Council a 'networked authority'. The rationale behind this is twofold. First, it wants to breed a culture of informality (the Chief Executive's office defines *informality* as "everybody talking to anybody at any time"). It is assumed that this would facilitate effective communication and thereby bring in efficiency in the work practices. This will result in the provision of better customer care (though the experiences in Public Services and Works department are rather different). Second, it visualises the council as a 'paper-less office'. The rationale put forward is that every year the Council uses nearly 25 million sheets of plain paper. Since the costs for printing, storing, distributing and disposing paper are enormous, "the Council is determined to tackle this problem ... and electronic communication and networking are set to provide one of the most effective and exciting solutions". This means that there is a lack of consensus on the purpose, form and means of IT usage among different groups. There is a mismatch between the Council's policy and the practices at the sectional level which raises questions about integrity of information systems and organisational practices.

At a policy planning level the Local Council executives recognise the need for a purposeful strategy for information and communication technologies to grow and ensure an optimal use of the resources. As the Executive Adviser to the Chief Executive commented, "a central focus for organisational change is required". He went on to say that role of the Chief Executive's Office is to translate political aspirations across a diverse range of services by providing links with resource allocation processes and implementation practices. He also felt that increasingly there was a need to balance the pressure for change and to facilitate internal change. In relation to the issue of operationalising change, there appears to be a lack of depth in the approach. This becomes clear from the statement made by a personnel from the IT department: "Computer based systems are central to transforming an organisation". This essentially means that information technology is considered as a means of bringing about change. The notion of change incorporates the transformation of not only business processes and activities, but also of the organisational and group culture. This does not mean that culture should not be changed. In fact, often organisational contexts demand that patterns of behaviour are 'fine-tuned' and adjusted. However, the concept of using information technology to institute a change in working patterns and culture seems inappropriate.

Discussions with the information technology and security auditors revealed an interesting interpretation of the changes. One auditor commenting on the top management initiative said, "to them, if it is big, it has to be effective". Implicitly, this meant that large and complicated projects seem to get commissioned without careful consideration. Within the Local Council, the federal IT infrastructure project was a clear example. Further investigations into the possible scope of the federal IT infrastructural project revealed a complex array of political objectives. Although the need for such an infrastructure came from the top management, the actual proposals were prepared by the IT department. The genuineness of intentions behind the initiative cannot be questioned; however, there is doubt about the hidden agenda of the IT professionals.

At the present time, most of the IT function has been outsourced. As part of the agreement, most of the IT staff have been taken over by the vendor company, however, there are still a few people on the council payroll. It is apparent that they are 'creating' work tō prove their worth. This emerged after discussions with the auditors. "There is a lot of manoeuvring going on," said one auditor. He made positive indications of how certain individuals within the IT department were teaming up with persons in the Chief Executive's Office. These 'partnerships' were rolling out what were termed 'flagship projects'.

Three such projects have actually taken shape. The first relates to setting up an electronic mail network. It has been sold to the top management on the basis that it is an excellent vehicle for raising IT awareness and literacy. Moreover, it is contended that the initiative to introduce electronic mail for chief officers provides an opportunity to highlight IT and point to new ways of working. The second project deals with providing business information services. The underlying intention is to link external and internal customers. At the present time there is already an infrastructure in place that links parts of the Local Council to its external customers. The new project proposes to extend this network to cover all departments within the council. A pilot of this project has been set up within Public Services and Works. The third project is concerned with setting up an executive information system. Different kinds of such systems are already in place, but it is proposed that certain common features be identified and a common architecture for executive systems be put in place. It is argued that this will make 'executive' information more accessible to those who are responsible for developing and implementing corporate policy, and to other members of the Council.

In the discussion so far it is apparent that whatever steps are taken, there are emergent reactions by different individuals and groups of people within the organisation. This means that a careful analysis of the proposed actions is needed. Indeed top management should be selective in choosing the initiatives. The real test is not only how the individual initiatives themselves work, but whether they are appropriate, and how they fit together in the organisation.

Problems with the management system

The previous sections have focused on eliciting issues from a macro organisational perspective. It is the intention with this section to draw examples from a particular Local Council department – the Public Services and Works, and relate them to the corporate initiative. This will allow us to make interpretations about the problems and concerns with the management systems in place.

With respect to the management systems within Public Services and Works department, the overall responsibility to develop and maintain IT based applications rests with the department rather than the Chief Executive's Office. So far as the day-to-day operational issues are concerned, responsibility has been further devolved to the individual sections within the department. Assessment of current and future IT requirements is also done at a sectional level. Recommendations regarding possible strategic options are later made to the Chief Executive's Office. These ways of working have evolved over a period of time. However, not all procedures and functions are necessarily sufficient and adequate. There is a need to redesign and formalise some of the processes. For instance, no specific responsibilities have been assigned for the management and housekeeping of the networks that operate within the department. Nevertheless some officers, on their own accord, have taken responsibility for some of these aspects. This situation is typical of most departments across the Council.

Discussions with different people within the Public Services and Works department showed satisfaction with the existing ways of doing work. One of the Assistant Engineers said, "the systems may not be perfect, but they work". Indeed the systems were far from being perfect. However, the existing ways of doing things have been well accepted by the staff and they do not seem to have any serious problems with them. At a departmental level there was definitely a need to develop an IT strategy. Such a strategy would be of use on three counts: in developing a statement of critical success factors, in identifying key issues and opportunities, with particular attention being given to management information and the quality of existing systems, and in defining objectives, scope, resources and timing for future actions. Since December 1993 initiatives had been underway to develop an IT strategy. By the end of 1994, it had been developed and put in place.

Because the current ways of doing things have been around for so long, they have become a part of the behavioural norms. In carrying out the day to day functions, it has become difficult for different roles to delineate formal job requirements from the institutionalised norms. In order to illustrate this point, let us take the example of an Assistant Engineer responsible for giving IT support. This role is placed within the Traffic and Highways section of the Public Services and Works department. As per the job description, responsibilities of this role fall into four categories. First, to apply accepted techniques in the preparation and implementation of traffic management schemes, including traffic surveys, traffic capacity calculations, detailed design, liaison with police etc. and on-site supervision. Second, to use computer technology to interrogate the Central Research Centre accident database system for investigation and statistical purposes. Third, to maintain and develop aspects of the section's computer network system with specific responsibilities for security back-up and virus monitoring procedures. Fourth, to maintain and develop the section's computer applications including the Graphic Information System, word processing, database and Computer Aided Design packages. This involves liaison with the suppliers and other agencies.

In reality however there are a lot of other functions that are performed by this role. Since the over-arching responsibility of the role is to provide IT support, the incumbent actually makes a concerted effort to check and maintain the integrity of the operations. Discussions with the individual in this role revealed that at all times his intention was to identify the business processes and match them with current IT infrastructural capabilities. This he did in association with the front-line staff. By doing this he made sure that the current infrastructure met the requirements of the front-line staff and the related business processes. Thus he was able to make assessments of future requirements and present them to responsible people within the department. Commenting on the functions and responsibilities of this Assistant Engineer and others within the department, the Assistant Director of Public Services and Works department said that this was a means "to provide improvement in the efficiency of existing services ... leading to improvement in quality". This was extremely important for the Assistant Director since he accepted the fact that the future was in taking the use of information technology out of the departments and into service points, where it may be accessed directly by the public. In such a situation incumbents in the role of the Assistant Engineer become increasingly important, for they are pivotal in providing system integrity.

The scenario presented so far indicates a fairly stable environment. However, potential problems in the business processes cannot be discounted. Top management initiatives to introduce a federal IT infrastructure increase the risk of misuse and abuse of the current infrastructure. In the present form the top management initiative is considered by different people, within the departments and sections, as an exercise in 'recentralisation'. As one Service Co-ordinator within the Waste Management section said, "we are going back to where we started". The federal infrastructure is not perceived as federal at all. In fact staff at sectional level view it as a game of power and control. In net terms, the new initiative is not only creating a dual IT infrastructure, but is also breaking apart the existing consistent, coherent and integral management system. In this new environment different roles not only have to input the required information into the new system, but also to reassess their job functions. In the case of the Assistant Engineer (from the example cited above), the new infrastructure is really taking him away from what he has always been doing. At present he can no longer concentrate on maintaining the integrity of the operations. This is because the top management wants to judge his performance on certain set criteria, which have been drawn from his job specification. Consequently, the majority of the Assistant Engineer's effort goes into 'getting his performance right'. This has two implications: first, the engineer's efforts to maintain system integrity have been dissipated, second, rather than the changes having enriched his job content, they have had a negative impact.

Discussions with the Auditors reaffirmed these findings. It became apparent that one particular member of the top management team was a business redesign enthusiast. Hence he wanted to change the processes in which service performance data was collected. Rather than conducting a detailed analysis of current work practices, he introduced a system that was at present being used within the Public Services and Works department, and in due course it is to be introduced into other departments as well. Such a system will actually question many of the current roles within the departments. It is not the contention here that such attempts invariably lead to chaotic consequences; in fact, the usefulness of such efforts has been well received in the literature. The business process re-engineering community is striving to introduce the concept of 'radical change' and the associated benefits. Proponents of process redesign argue that only radical change holds out a promise of potential benefits (Hammer and Champy 1993). In bringing about such a change, it is necessary to adopt an integrative approach that considers the contextual aspects with specific emphasis on the degree of change (i.e. whether it is incremental or radical). This allows us to optimise the use of information technology once a process has been identified as a candidate for change. Some advantages of doing this are enhanced productivity and effectiveness of the operations. However this is not happening in the Local Council. The change being introduced by the top management is neither incremental nor radical, it is 'piecemeal'. Since such change initiatives do not take a holistic view, they invariably result in a loss of integrity of the business operations. This results in conflicting demands and expectations on the part of the members of the organisation.

The manner in which the above system (which is a component of the federal information technology infrastructure) is being introduced is a typical example of an ill-conceived change initiative that results in the introduction of 'broken' processes (Hammer and Champy 1993). It also illustrates how a relatively stable management system can be transformed into a volatile and an incoherent one.

Significance of responsibility

The review of management systems in the previous section shows that the stability of existing systems has been disturbed. The principle reason was the implementation of an extremely formal rule based structure on to a predominantly informal, loosely configured structure. Prior to the changes, responsibility for maintaining system integrity and security had been adopted by different roles on an informal basis (refer to the Assistant Engineer's example cited above). However, the imposition of a highly structured performance monitoring system has resulted in the disintegration of the informal structures. This aspect has been identified in the internal reports generated by the Computer Audit department.

Discussions with the Auditors revealed that they had never anticipated the extent to which the norm structures within an organisation could break. This has led to significant problems for them. Traditionally, they used to look at individual systems and assess whether basic maintenance, housekeeping and security was being taken care of. Generally they were satisfied. With all the changes, the auditors feel that they are faced with a very difficult situation. Because of a new impetus from the Strategy Group, the staff are more concerned with getting their reviews right. Indeed the new IT based management system has dramatically changed the attitudes of different roles. The scope of the problem can be gauged from the following two extracts from the internal auditor's reports:

> Prior to the corporate initiative to introduce performance monitoring systems as part of the federal IT infrastructure, one of the reports submitted by an auditor read as follows:
>
> > "On the whole, in the departments so far reviewed, staff have demonstrated a very professional and co-operative attitude in their approach to all matters relating to security. ... the staff are receptive to suggestions and are keen to *take on responsibilities*, even though they are not formally required to do so."
>
> In a subsequent audit review, after the performance monitoring system had been implemented, the auditors report noted the following:
>
> > "IT responsibilities .... tend to be Sectional within the department although some thoughts on *centralising the responsibility* are being given .... There are no <u>formal</u> procedures and standards for IT for the whole department .... There are no security functions for networks and housekeeping .... {with respect to Systems in general} There are no departmental procedures / standards for specifications / testing / documentations / enhancements and maintenance .... Specific responsibilities should be added to the job descriptions."

Thus it is clear that an environment that manages well with informal arrangements needs to do a lot more if behavioural norms are shattered. The auditing reports identify this and show concern about inadequate responsibility structures in the new organisational environment. It is therefore important that responsibility is ingrained into the behaviour of people. Though the formal designation of responsible agents is helpful, it is neither sufficient nor adequate if members of the organisation resent and reject change. This is especially the case of organisations that take a 'piecemeal' approach to change initiatives, rather than an incremental or radical approach.

Summary and discussion

Findings so far reveal that there is significant variance in the perceptions of different people. This has resulted in a lack of mutual understanding and communication gaps among the stakeholders. The resultant patterns of behaviour form a basis for conflict among the members of the organisation. There may also be problems about acceptability of the systems. Information system security problems emerge from such concerns. This eventually affects an organisation's performance.

In the case of the federal IT infrastructure at the Local Council, there is a wide gap in its utility as perceived by the top management and its actual performance. The significance of these gaps and the related problems can be understood by looking at the expressive content of the infrastructure and its significance within specific domains (table 5.3). In doing so the whole IT infrastructure is considered as a sign function. It is a sign function because of two reasons. First, it is an organisational activity that signifies certain events (e.g. performance monitoring). Second, it communicates these events. In the particular case of the Local Council it is a one-way communication from the top management to the users.

Table 5.3 The expressive content of the federal IT infrastructure

Expression given by the infrastructure	**Significance in the domain**		
	Top Management	**Users**	**Auditors**
Denotative	value judgement; facts; appraisals; corporate plans	instructive	plans and policies; appraisal
Connotative	rewards; inducement	coercion	threat

Table 5.3 categorises the meaning structures that are expressed and represented by the federal IT infrastructure, and the significance of these is assessed within specific domains. The denotative expressions of the IT infrastructure are those that refer to a set of objects or actions. The significance

of these would vary among the domains. The connotative expressions refer to the deep-seated feelings that are linked to the denotative expressions within each domain. The significance of the expression given by the IT infrastructure shows that top management views it as an output of a core corporate planning exercise. Consequently the systems are going to generate factual information and help in providing value judgements. At a deeper connotative level, the top management feels that not only will there be inherent rewards for them, but the infrastructure will also induce preferred behaviour. It must be noted that these are the conceptions of the top management, rather than actual outcomes. The findings so far have revealed that the converse is true.

The expression given by the infrastructure, for users and auditors, was significantly different. At a superficial observable level (denotative), the users perceive the federal IT infrastructure to be instructive. Findings presented in this section give a indication that users considered the infrastructure as saying, "what must or ought to be done". They got this feeling because the new infrastructure was 'ordering' instructions, rules and regulations. Besides, 'silent messages' were also given about the consequences of acting upon the instructions or failing to act upon them. At a deeper level, the users were getting the feeling of being coerced to do things in an extremely 'neat and a tidy' manner. Discussion in the previous sections has illustrated this aspect. The auditors on the other hand, while not having so adverse a reaction, were not pleased with the manner in which the federal structures were being introduced. At a broad policy level they believed in the usefulness of such an infrastructure. They felt that it was part of the corporate plans and policies. However, they had significant reservations about the implementation process. Because the federal systems were not well received, they felt that in many ways rather than providing benefits, the shifting edifice could result in disastrous consequences. Meetings with the auditors revealed their fears about disgruntled employees. A common message from the auditors indicated that however strong formal and technical controls may be, if the more deep-seated pragmatic concerns are not understood and managed properly, there is a potential security problem.

In conclusion, this section has reviewed the impact of various organisational actions on the systems in place. Problems with the current management systems were also analysed. Following this the significance of responsibility factors within the council were discussed. An emergent issue from the discussion so far relates to the gap between what systems are supposed to do, how they actually function and the different perceptions of the people involved. This is not just a simple implementation issue, rather it indicates that a fuller understanding of the basic policies and system designs is needed. In that respect the development of secure environments really cannot be separated from good systems development.

5.3.4 Analysis of the syntactic and empirical aspects

The previous section has highlighted the importance of understanding the meanings and intentions of different stakeholders. In an ideal environment, all concerned should have a similar perception of the organisational actions. In the case of the Local Council, these actions are an outcome of an interplay between rules and norms of service delivery. Since it is the stakeholders who operationalise service delivery, quality of service provision is based on the extent of matching between organisational purpose and perceptions of the staff. It is therefore important to consider the implementation issues and viability of rule structures. Furthermore, as noted in chapter 4, if the rules specified for an IT infrastructure do not adequately reflect an organisational environment, the systems run a high risk of being abandoned or misused. Therefore, the security concern for IT infrastructures is rooted in the system design and specification parameters. This section considers such issues and analyses the form and means by which the rule structures have been implemented within the Local Council.

Logical service specification at the Local Council

Previous sections have already emphasised the decentralised nature of IT infrastructure within the Local Council. The increased tendency towards developing federal structures has also been identified and reviewed. Over the past few years the core objective of the Local Council has centred around the notion of customer care. In providing such quality care, the emphasis of the council has been to view its service delivery as an input and output process[9] (also depicted in figure 5.1). A key area of concern in delivering quality care has been the processing of customer needs. Hence a relevant Local Council service is matched to the needs of the customers and finally the service is discharged through predetermined means. Quality assurance takes prominence during all the three stages of needs assessment, matching service to the needs and service delivery. The Local Council has devolved the development of the infrastructure and IT support to the lowest relevant levels of the organisation.

However, since the Council views quality of service provision as its mission, a new federal infrastructure has been developed. While individual systems development has been the responsibility of the individual departments, the specification of the federal structures has been within the remit of the top management. Since the management has viewed service delivery in terms of discrete steps, the imposition of federal structures has also been conceived in a similar fashion. With respect to the development of a federal IT infrastructure, no particular methodology has been used. However, the IT department has advocated the development of 'prototypes', with Public Services and Works department being the pilot site. However, during the course of the research presented in this book the Local Council never confessed to the use of prototyping as a methodology. Nevertheless all the symptoms in the developmental process were contrary to the assertions made by the management.

Prototyping as a methodology is most certainly an improvement over the traditional specification methods, most of which have been based on the "waterfall" model (e.g. Boehm 1976). In analysing the requirements, such models often take an incomplete and a static view of the world. Prototyping on the other hand helps in clarifying user requirements, verifying the feasibility of a design and developing the final system through an evolutionary methodology (see for example Albadvi and Backhouse 1995). Discussions with different people involved in developing the federal IT infrastructure revealed many inherent problems. The auditors in particular felt that an inadequate problem analysis had been done. The users thought of the prototype as being the final 'product'. Since little thought had been given to the political and cultural issues, from the very onset the users had feelings of rancour, dissension and antagonism. A similar situation was reported by Mattel Toys where an analysis revealed that the prototype had "cured the itch, not the disease" (as summarised in Sprague and McNurlin 1986; p249).

An example from the Public Services and Works department shows the extent to which the development of prototypes was a wasteful activity. Two of the sections within the department have Unix based systems (i.e. Waste Management and Transport) while others have PC based systems and none of the information systems are linked to each other. There is no electronic exchange of information among different sections. The need for such exchange is also minimal because their activities have very little overlap. In taking the notion of a customer care and federal IT infrastructures forward, the Strategy Group commissioned the development and implementation of a complaint monitoring system. The Public Services and Works department developed the prototype and implemented a small system which draws pertinent information from all sections. The manager in charge found some practical problems. Since the activities of all the sections are so diverse, the only commonality found was with respect to incoming complaints and the response rate. Because a system 'had to' be developed, the eventual outcome took the form of a letter management system – a totally different system from the original conception.

Logical security measures

It has been well recognised that in highly decentralised and networked environments the need for security is paramount (see for example Lobel 1991). Security aspects gain further importance when the IT infrastructure is federal in nature. Although significant research has been done with respect to integrated systems and distributed environments (e.g. Gable and Highland 1993 Jamieson and Low 1990; Baskerville 1989), little has been written on federal architectures. In fact the notion of federal infrastructures is germane to local governments in the UK.

Considering the logical security measures with respect to the federal IT infrastructure within the Local Council, it becomes evident that these are indeed skimpy. Discussions with the auditors confirmed this belief. In fact the auditors had made several recommendations about the logical structure of the security measures, but these had not been heeded. Blame can be attributed to the inherent lack of communication between different stakeholders. These issues have been discussed at length in the previous sections. In their review of the security measures, the auditors revealed that all the Local Council servers are on the corporate backbone and thus, theoretically, anyone on the same backbone could access any of the servers provided that they have the appropriate password. Furthermore, in practice the IT department has overall responsibility for the administration of each server. All supervisor passwords for the servers are known to the IT department (these are the top-level passwords which give the highest level of access to an entire server). Clearly there are good reasons for giving some responsibility to the IT department. Although the IT staff are technically proficient and understand and appreciate the finer points of networks, the Council is nevertheless open to a number of security risks. At a logical level the arrangements may seem to be satisfactory; however, the political games by different stakeholders leave a lot of scope for 'creating' disgruntled employees. As has been discussed earlier, most of the IT department has been outsourced and the only way in which the remaining staff can show their worth is by 'creating' a need for their services. This has been done through the federal IT infrastructure project. Since a complete federal infrastructure would result in linkages with existing servers, all vulnerabilities in the network would be inherited by the new infrastructure.

Considering specific concerns, it became clear that even at a basic procedural and technical level, considerable security issues have been left unattended. For instance, in the Local Council, the most common forms of LAN transmission architecture are Ethernet and Token Ring. The insecure attributes of these add a further dimension to the already precarious climate within the Council. Without going into the technicalities, it is important to recognise that every 'packet' that is sent out on the network passes through every workstation on the network. The network adapter card on each workstation looks at the header of each 'packet'. It then either accepts it or passes it down the line. A competent programmer can alter a network card quite easily so as to make a copy of every 'packet' it receives in the workstation. In fact a hacker would most likely use a LAN analyser which would do the same thing. The auditors recognised this problem and recommended encryption. Up until the time of this study the recommendation had not been considered.

The extent of complacency in implementing basic security measures can be judged from the nature and scope of physical access control mechanisms. The hub of the IT department of the Local Council is the Networking and Information Centre. This Centre has a Help Desk for the convenience of the users. At present there is no physical access control to prevent unauthorised access to the Help Desk area and to the Networking and Information Centre. The file servers and network monitoring equipment remains unprotected even when the area is unoccupied. In fact the file servers and network monitoring equipment throughout the Council should be kept in physically secure environments, preferably locked in a cabinet or secure area. This would prevent theft or deliberate damage to the hardware, application software or data on the network. Access to the Help Desk area can typically be restricted by a keypad. The auditors had identified these basic security gaps, but concrete actions are still awaited.

Discussions with security auditors revealed that earlier security reviews had identified risks resulting from the complex interplay between the political motives, procedural control issues and the development of new technical infrastructures. Although the auditing reports had not made the concerns explicit, these had been hedged in the recommendations. Considering the sensitivity of the issue, this is understandable. For instance, the auditors recognised the problems of the new infrastructures and felt that there would be an increased tendency to subvert controls by some employees. Hence they recommended that to prevent the possible damage afflicted by a disaffected or disgruntled employee working in the Networking and Information Centre, the data safe containing the back-up security copies of the network data and application software should be kept in a more secure environment. This would prevent deletion or damage to both the live and back-up copies of the data and application software.

Discussions with users revealed that the Council had experienced real problems because of current practices. It was a documented fact within the Council, that an employee had subverted the slender controls to gain unauthorised access to the Supervisor passwords. In another instance data and application software on a network could not be restored from the back-up copy, and as a result a significant time and effort was lost in restoring the system. In a secure environment data integrity can be preserved if all file servers are either backed up automatically or on demand as a standard procedure. Security copies should then be kept in an off-site location. Departmental network system administrators should be responsible for ensuring that security copies have been run correctly and that network data and application software can successfully be restored in case of need.

Another issue of concern relates to the organisational structures supporting network administration. Currently the network system supervisor function is carried out on behalf of departments by the Information Centre analysts, who have routine day-to-day supervisor profile access to all data and application software on the file servers. This in itself is a security hazard. Help Desk Supervisor access to the networks should be restricted to an "as required" basis, even more so for sensitive files and applications. Information Centre analysts currently have unrestricted access to the data and application software on all the Council file servers. This is again a cause of concern, since the Council possesses very powerful network data transmission analysis tools that can monitor, read, intercept and change data transmission across the networks. Without any possibility of detection network data traffic can be passively monitored by simply plugging into spare connectors on the cables. In this way it is possible to read user passwords without detection[10].

Summary

Discussions in the previous sub-sections have shown that logical and physical security measures become useful only when they are supported by an adequate organisational infrastructure. Such considerations relate to the deep-seated cultural issues as well as a consistent meaning structure. Furthermore, the importance of a fuller analysis before system design activities was related to the development of secure environments. The research in this book has also shown that the security of systems is an outcome of a complex interaction of socio-political aspects and rule based structures that support organisational purposes. The recommendations given by the auditors support this contention. Although the security reviews conducted by the auditors identified potential weaknesses, these had not been taken up seriously by the managers. A possible reason for this is the skewed interest of the IT people in saving and 'creating' their jobs. This also reaffirms the argument presented in this book that information system security can only be achieved by considering deeper pragmatic aspects of the organisation.

5.4 Emergent issues

The purpose of this section is to reflect on the key findings from the Local Council case study. These are then related to problems of managing information system security. In light of the definitions established in chapter 1, information system security is considered as the prevention of occurrence of any adverse event. It represents a state of caution and safety with respect to the information handling activities of an organisation.

The findings so far reveal that indeed the aspiration towards a federal IT infrastructure made sense. However, the meaning structures afforded by it and the form and means of implementation were dubious. The top management felt that the customer care objective could be achieved by implementing an information and communication network. The top management designated this as an 'intelligent infrastructure'. Managers at the departmental level, in carrying forward the corporate objectives, tried to force a technical system on to highly decentralised sections. This was directly in conflict with the existing informal culture which is strong at the section level. Moreover there was a general feeling among individuals at the operational level that the whole exercise was a futile effort. They regarded the new system as nothing more than an electronic letter ledger. A manager of the Waste Management section substantiated this view by saying that at the operational level one sees real customer orientation and "and what they (the Chief Executive's Office) are doing is not customer care". Thus in trying to impose technical controls on to a predominantly informal setting, the integrity of the organisation and the formal systems in place was being sacrificed. Such a situation could not only result in a loss of productivity but also in a lower standard of customer care.

It is possible that discussions between top management, user departments, the IT department and the auditors could provide a solution that takes into account the responsibilities of the Local Council in respect of integrity of the systems and core purposes. At an operational level confidentiality of data and limited potential accidental damage to servers could also be considered. The auditors recommended a probable way forward by building trust among the users. As one security audit report put it, "...the way forward is to entrust supervisor passwords to end users who after all are privy to confidential data, in some instances, by the very nature of their work, and who on balance are responsible and intelligent enough...".

The auditors in the Local Council have been very discerning and identified the potential problems with the IT infrastructure and the management systems. Although the process of performing security audits in itself is a subject of much debate, most of the recommendations given by them have been valid. These have largely been ignored by the management. Particular criticism of the audit procedures relates to their focused orientation towards logical and physical security issues. Only a few high level cultural and semantic issues have been identified. Moreover, there was no consistency in the method for eliciting such attributes.

It is interesting to note that the conception of security within the Local Council was different for different stakeholders. Although the auditors understood the importance of maintaining integrity in the operations of the Council, there was little they could do in terms of operationalising their recommendations. The top management on the other hand was less interested in the security aspects, and the managers involved had political objectives to be fulfilled. The user departments had practically no say in any of the matters. In such an environment, whatever the nature of security measures and related controls, there is a strong likelihood that the emergent behaviour of people would not conform to the formally specified expectations. In order to develop and sustain a successful IT infrastructure, there is a need to develop commonality in purpose between different groups and acquire coherence between the technical structures and the environment. Furthermore, it is important to develop a culture where planning activities are not carried out in a vacuum, but rather all the strengths and weaknesses of the options are assessed and opportunities and threats offered by the environments are taken into account. Within the Local Council, for example, the information technology policy neither reflects the needs and expectations of the users, nor does it take into account the potential security implications. In that respect the information systems and security related policies are inadequate.

Analysis of the Local Council identifies four key themes pertaining to the management of information system security. These are: the planning and security policy issues; the evaluation of security; information systems design consideration in security; the implementation of security. Brief interpretations are presented in table 5.4. These are then discussed at length in chapter 6.

Table 5.4 Résumé of major issues

Emergent issue	Interpretations from the Local Council case
Planning and security policy	Corporate emphasis with respect to the IT infrastructure has shifted towards federalism. The information systems planning process is ad hoc. A very narrow perspective is adopted with respect to security planning.
Evaluation of security	The top management did not consider security evaluation to be an important issue. Simple auditing and checklist approaches were used to evaluate security of the IT infrastructure. Risk analysis was not conducted. Different stakeholder perspectives were not accounted for.
Design considerations for security	A proper analysis of the current infrastructure was not carried out. The new IT infrastructure does not consider security at all. The system designers have vague security goals.
Implementing information system security	The controls related to the existing system and that of the new infrastructure contradict each other. Implementation of the IT infrastructure and the related security controls was done without understanding the existing environment. Objectives of different users contradict each other. This reflects substantial incoherence in their purposes, thus questioning the integrity of the operations

5.5 Conclusion

This chapter has attempted to describe how the information technology infrastructure within the Local Council was conceived, analysed, designed and subsequently implemented. The analysis was conducted by using the conceptual framework proposed in chapter 3. The findings from the case revealed significant incoherence in the design and management practices. The implementational aspects with respect to the IT infrastructure have also not been properly thought through. With respect to information system security, conclusions similar to the Hospital Trust case can be drawn. The top management within the Local Council considered the information technology infrastructural issues at a syntactic and an empiric level only. For them the pragmatic and semantic aspects were either not important or did not exist. This was in contradiction to the conceptions of the auditors, who appreciated the importance of more subtle deep-seated aspects. This conclusion supports the main argument of this book – that deep-seated pragmatic aspects of an organisation are critical for the security of an enterprise. The key emergent themes identified in this chapter form the basis for further discussion and in developing a synthesised perspective later in the book.

[1] The Citizens' Charter redefines the contract between the citizen and the state in the UK. It has three underlying assumptions. First, the citizen is entitled to receive some level of service in return for the taxpayers' money. Second, the citizen is entitled to know what level of service is being provided. Third, the citizen is entitled to some form of redress if that level is not attained.

[2] In recent years there has been an increased use of Service Level agreements (SLAs) between departments. This is especially the case with the central services, such as accountancy and the locally managed units (i.e. the service departments). The provider of services is usually required to supply a service description and a charge is made to the purchasing department.

[3] This role is in charge of liaisons, both internally and externally, on all matters concerning computer based information systems.

[4] It is interesting to find that someone from IT department would be part of the Chief Executive's support team. This is because the Chief Executive has a vision that information technology can be a prime enabler for changing the way in which the Local Council carried out its business. This is discussed at length in the following sections.

[5] The terms 'corporatism' and 'professionalism' were first described in the 1972 Bains Report (The new local authorities: management and structure, HMSO, 1972).

[6] The past few years have seen many local authorities follow a similar pattern. Kent County Council in particular has developed a federal information technology strategy which captures the benefits of both central and decentralised systems.

[7] This opinion was voiced by one of the employees in the Public Services and Works department.

[8] Hall (1959) classifies modes of communication as formal, informal and technical. The same classification was used to analyse CIS within the Hospital Trust in chapter 4.

[9] It may be noted here that even the health care delivery process of the Hospital Trust was conceptualised in a similar fashion. This is because of similar wider contextual influences on the two organisations.

[10] Netware version 3.x supports encrypted passwords which cannot be read when the default parameter for unencrypted passwords is OFF. However, if the parameter has been changed then passwords would be unencrypted and read by this method.

6 Principles for managing information system security

6.1 Introduction

This chapter brings together some of the key issues identified in the two case studies, and draws out some general statements for interpreting the management of information system security. Maintaining the interpretive mode adopted in this book, various elements of this synthesised perspective deliberately avoid considering problems as a consequence of a systems function. They are viewed as an emergent property of reflexive interaction between a system and its context. Four major themes are identified: the security policy itself; evaluation of security; design considerations in security; implementing information system security.

6.2 Planning and security policies

This section discusses the concept of a security policy. The intention is not to undertake an exhaustive literature review, but to understand the systematic position of policies within an organisation. The first sub-section highlights some of the basic ideas. The second part interprets the security policies in the two case studies. Finally a synthesised perspective on security polices is presented.

6.2.1 Corporate planning, strategy, policy

There is often a confusion between the various terms – strategy, policy, programmes, and operating procedures. The term *strategy* is used to refer to managerial processes such as planning and control, defining the mission and purpose, identification of resources, critical success factors, etc. Corporate strategy has been considered as the primary means to cope with the environmental changes that an organisation faces (Ansoff 1991; Andrews 1987; Mintzberg 1983a; Quinn 1980). It is often considered as a *set of policies* which guides the scope and direction of an organisation. However, there is much confusion between what is designated as a policy and what as strategy. Ansoff (1987; p114) traces the origin of the term *strategy* to "military art, where it is a broad, rather vaguely defined, 'grand' concept of a military campaign for *application* of large-scale forces against the enemy". In business management practices, the term *policy* was in use much before *strategy* but the two are often used interchangeably, despite having very different meanings. In practice a policy refers to a contingent decision[1]. Therefore implementing a policy can be delegated, while for implementing a strategy executive judgement is required. The term *programme* is generally used for a time-phased action sequence that guides and co-ordinates various operations. If any action is repetitive and the outcome is predetermined, the term *standing operating procedure* is used.

In the realm of information system security, there has been an overemphasis on developing policies. A literature survey for research presented in this book revealed no reference to the use of the term 'strategy'. Studies have shown that there is generally a lack of commitment on the part of the top management when participating in the policy formulation process (see for example Warman 1991). The skewed emphasis on security policies can be explained on the basis of the functionalist preconceptions of many practitioners and researchers alike. Their understanding of organisations as formal-rational entities forces them to conceive of information system security in a similar fashion, and security policy formulation is seen as a series of discrete steps. This has mostly been the premise of IT professionals.

If we accept that secure information systems enable the smooth running of an enterprise[2], then what determines the ability of a firm to protect its resources? There are two routes (figure 6.1). Either, a firm considers security as a strategic issue and hence operates in an environment designed to maintain consistency and coherence in its business objectives, or, a firm may position itself such that it gains advantage in terms of the risks afforded by the environment. This has traditionally been achieved by performing a risk analysis. This demarcation identifies two levels of a strategy within an organisation: the corporate and the business level[3].

At a corporate level the security strategy determines key decisions regarding investment, divestment, diversification and integration of computing resources in line with other business objectives. The primary concern here is to take decisions regarding the nature and scope of computerisation. At a business level, the security strategy looks into the threats and weaknesses of the IT infrastructure. In the security literature many of these issues have been studied under the banner of risk analysis. The manner in which risk analysis is conducted is a subject of much debate, as are the implementation aspects. While a business security strategy defines the overall approach to gain advantage from the environment, the detailed deployment of the procedures at the operational level are the concern of the functional strategies (i.e. the security policy). These functional strategies may either specifically target major organisational activities such as marketing, legal, personnel, finance, or may be more generic and consider all administrative elements.

Most of the existing research into security considers that policies are the *sine qua non* of well managed secure organisations (see for example Olnes 1994; Dorey 1991; Denning 1987). However, it has been contended that "good managers don't make policy decisions" (Wrapp 1991; p32). This avoids the danger of managers being trapped in arbitrating disputes arising out of stated policies rather than moving the organisation forward. This does not mean that organisations should not have any security policies sketching out specific procedures. Rather the emphasis should be to develop a broad security vision, that brings the issue of security to the centre stage and binds it to the organisational objectives. Traditionally, security policies have ignored the development of such a vision, and instead a rationalistic approach has been taken which assumes either a condition of partial ignorance or a condition of risk and uncertainty. Partial ignorance occurs when alternatives cannot be arranged and examined in advance. A condition of risk presents alternatives that are known along with their probabilities. Under uncertainty alternatives may be known but not the probabilities. Such a viewpoint forces us to measure the probability of events occurring. Policies formulated on this basis lack consistency with the organisational purpose.

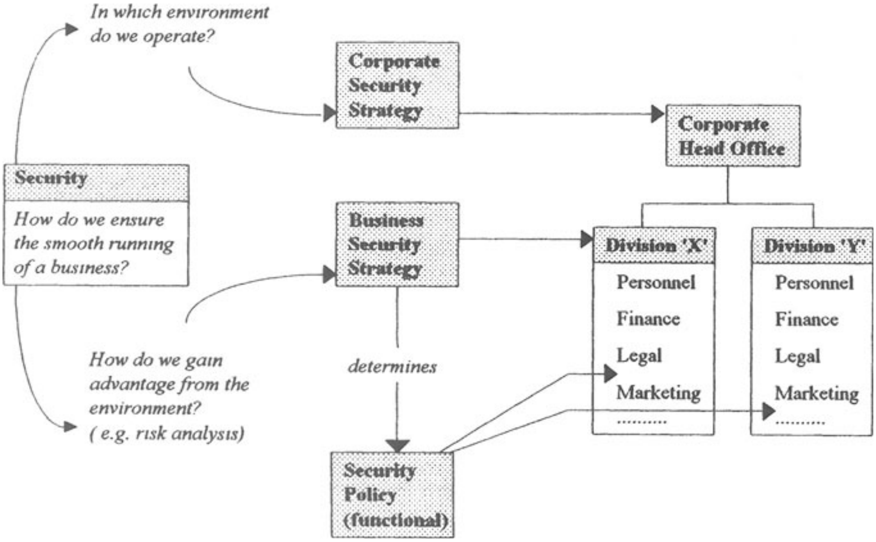

In which environment do we operate?
Corporate Security Strategy
Corporate Head Office
Security
How do we ensure the smooth running of a business?
Business Security Strategy
Division 'X'
Personnel
Finance
Legal
Marketing
....
Division 'Y'
Personnel
Finance
Legal
Marketing
....
How do we gain advantage from the environment? (e.g. risk analysis)
determines
Security Policy (functional)

Figure 6.1 Levels of strategy

6.2.2 Interpreting security policy in the case studies

The Hospital Trust and the Local Council case studies show discontent with measures taken for developing and managing information system security. Significant blame can be attributed to the manner in which the management of the two organisations have viewed the very concept of security, if at all. It becomes evident from both the case studies that security has been aligned to the form of IT infrastructure rather than with organisational culture and the prevalent meaning systems. This is in spite of the vociferous demands by academics and practitioners alike that security should be considered at the highest levels in an organisation. What is needed is to consider security as a strategic issue, especially in today's climate where it is becoming difficult to dissociate business processes from computer based information systems.

A major consideration in developing a secure organisational environment is to develop a vision for security. The emphasis should be to provide a 'common thread' between organisational purposes and core activities. A common vision would help in developing a security culture in the organisation, thereby establishing a norm structure with respect to information handling activities. In the case of the Hospital Trust such a common thread is lacking. The prevalent vision is that the security policy developed by the Information and Management Group of the NHS could be implemented at the Trust level. In fact the outside consultants have made no effort to analyse the particular requirements of the Hospital Trust. Rather they have developed a set of guidelines modelled on two of the NHS Management Executive documents: 'Basic information systems security' and 'Information system security and you'. These documents are not prescriptive, but they emphasise the importance of addressing data protection legislation, developing a top level security policy, installing baseline security, undertaking a small systems review and conducting a risk analysis. So the Hospital Trust does not have a security policy of its own, but has adopted the one developed by the NHS Management Executive.

The Local Council considered things differently. A definitive corporate strategy and an information technology strategy exists. These documents reflect the changes taking place within the wider context of the council. In recent years individual departments have also been developing their own information technology strategies. This trend is part of the overall emphasis to devolve IT responsibilities to the lowest levels. The individual strategies however come together to form an overarching IT strategy for the whole council. In terms of security, there is a skewed emphasis towards auditing. No top level security policy exists. The security measures adopted emerge from the checklists developed by the internal computer auditors. Thus, on the one hand there is a common purpose and a shared vision for developing and sustaining an IT infrastructure; on the other hand there is only rudimentary concern for security.

With respect to the security strategy the Hospital Trust and the Local Council need to address the question: 'Which environment do we operate in?'. This means that high level corporate planning issues should address the nature of the business and the opportunities and threats afforded by the environment. An associated concern of the strategic plan should be to reflect on the information system security aspects. These issues have not been addressed within the

Hospital Trust.The Hospital Trust statement of purpose devised by the managers has many problems. Since it focuses on moving people out into the community, it questions the very existence of the hospital trust. Once people move out into the community, the role of the hospitals is minimal. In reality this may not happen, thus highlighting the inadequacy of the strategic objective. In this scenario, the strategic role of the information system in also blurred. In fact information systems are conceived of in a very narrow technical sense, contrary to the definitions proposed in chapter 1. Information system security is therefore regarded as a technical activity that is delegated to the outside consultants.

In the case of Local Council the individual user departments are more involved with strategic IT issues. These are regarded as synonymous with information systems concerns, and therefore anything to do with computers falls within the remit of the IT department. In considering the question, 'Which environment do we operate in?', high level corporate planning issues have been addressed inadequately. The main pressure on the Council has been to reduce its costs, leading to individual departments being considered as business units. Emerging from this was the belief that the IT services should be outsourced. However, these activities and the related decisions are accounted for neither at the corporate planning stage nor at the IT strategy level. Furthermore, information system security issues seem irrelevant to managers at the corporate level. The devolution of purchasing power and IT strategy formulation on to the individual departments is in direct conflict with the outsourcing of IT function. Although there is a concerted effort to formulate and implement corporate plans and IS strategies, there is a lack of coherence in the purpose and content of the actions. This is a major integrity concern in itself.

Another question that needs to be addressed is 'How do we gain advantage from the environment?'. This question is linked with the development of a business security strategy. The main concern is to identify the internal strengths and weaknesses of the organisation. This requires numerous internal reviews targeted at different business functions. Since security is considered as a main enabler to the business, the strengths and weaknesses of the systems in place should also be analysed. The Hospital Trust management recognised the importance of such reviews. However, these were prioritised according to perceived financial gains. Since a typical security review does not produce any immediate cost savings, the Hospital Trust has not considered such a review with any seriousness. The Trust undertook a CRAMM review but it was a half-hearted attempt (detailed discussion in chapter 4). Ideally, a comprehensive risk analysis should lead to the formulation of a business plan that determines the nature and extent of the controls that may be put in place. This takes the form of a security policy.

In the case of the Local Council a somewhat similar situation existed. The environment is typically characterised by a number of legacy systems. Some of these systems are constantly being upgraded while others are being phased out. Such a situation necessitates a fuller analysis of the strengths and weaknesses of the operations. However, the only mechanism used was that of auditing where existing controls were reviewed on basis of a predefined checklist. Although auditing helps in checking specific controls, it falls short of performing a more comprehensive environmental review. Had an adequate review been commissioned, the need for a security policy would also have been felt.

To summarise, it becomes clear from the two cases that there is a need to develop a vision for security. Such a vision brings security to the centre of all business activities. Furthermore, it lays a foundation for security of information systems being considered at the highest levels of the organisation. Emerging from this vision is an intrinsic need to assess the prevalent risks in any given environment. Such an assessment would dictate the formulation of specific policies for specific organisational functions. This is contrary to the beliefs that security policies should be developed *ab initio* without understanding the environment and that top management support be gained at a later stage in formulating, managing and implementing them. What is proposed is an alternative route where the purpose and the content of organisational actions is first understood and a security culture developed. Formulating a security policy should be considered as an emergent activity.

6.2.3 A synthesised perspective on security policy

It becomes clear from the discussion so far that organisations need to develop a strategic security vision that ties corporate plans with the tactical security policy issues. Both in the case of the Hospital Trust and of the Local Council, although information technology has been considered as a strategic resource, little effort has been made to address the security concerns. Even where security implications have been thought of, a mere functionalist technical perspective has been considered. This is contrary to the security viewpoint propounded in this book. This section identifies some key principles for developing security policies. These are summarised in a diagrammatic representation that appears in figure 6.2.

Principles

In furthering our understanding of security policies within the interpretivist tradition, we should be able to study the security policy formulation process from the perspective of people in an organisation, thus allowing us to avoid causal and mechanistic explanations. By adopting a human perspective, we tend to focus on

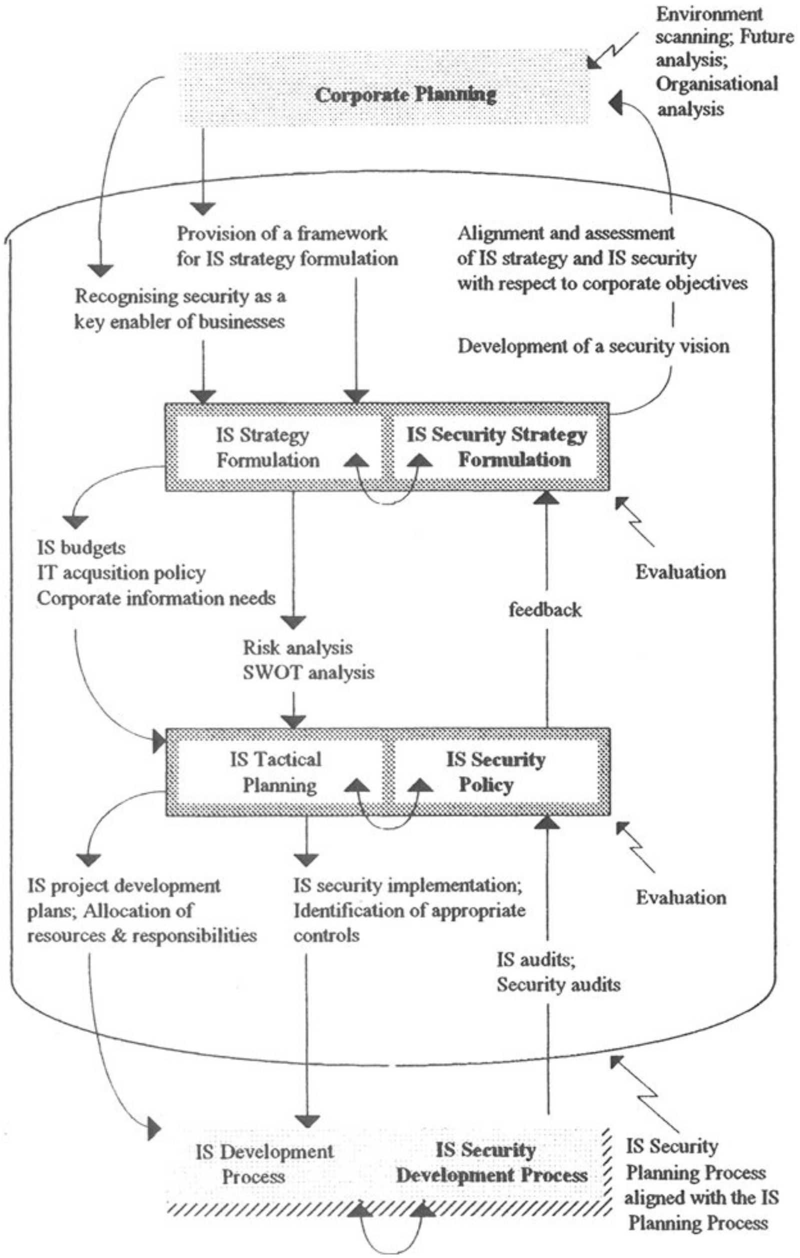

Environment scanning; Future analysis; Organisational analysis
Corporate Planning
Provision of a framework for IS strategy formulation
Alignment and assessment of IS strategy and IS security with respect to corporate objectives
Recognising security as a key enabler of businesses
Development of a security vision
IS Strategy Formulation
IS Security Strategy Formulation
IS budgets
IT acqusition policy
Corporate information needs
Evaluation
feedback
Risk analysis
SWOT analysis
IS Tactical Planning
IS Security Policy
IS project development plans; Allocation of resources & responsibilities
IS security implementation; Identification of appropriate controls
Evaluation
IS audits; Security audits
IS Development Process
IS Security Development Process
IS Security Planning Process aligned with the IS Planning Process

Figure 6.2 A framework for IS security planning process (some parts based on the original IS planning process framework of Galliers 1987; p50)

the human behavioural aspects. Security policy formulation is therefore not a set of discrete steps rationally envisaged by the top management, but an emergent process that develops by understanding the subjective world of human experiences. Mintzberg (1987) contrasts such 'emergent strategies' from the conventional 'deliberate strategies' by using two images of *planning* and *crafting*:

> Imagine someone planning strategy. What likely springs to mind is an image of orderly thinking: a senior manager, or a group of them, sitting in an office formulating courses of action that everyone else will implement on schedule. The keynote is reason – rational control, the systematic analysis of competitors and markets, or company strengths and weaknesses, the combination of these analyses produces clear, explicit, full-blown strategies.
>
> Now imagine someone crafting strategy. A wholly different image likely results, as different from planning as craft is from mechanization. Craft invokes traditional skill, dedication, perfection through the mastery of detail. What springs to mind is not so much thinking and reason as involvement, a feeling of intimacy and harmony with the materials at hand, developed through long experience and commitment. Formulation and implementation merge into a fluid process of learning through which creative strategies emerge. (p66)

This does not necessarily mean that systematic analysis has no role in the strategy process, rather the converse is true. Without any kind of an analysis, strategy formulation at the top management level is likely to be chaotic. Therefore a proper balance between *crafting* and *planning* is needed. Figure 6.2 hence is therefore not a rationalist and a sequential guide to security planning, but only highlights some of the key phases in the information system security planning process. Underlying this process is a set of principles which would help analysts to develop secure environments. These are:

1. **A well conceived corporate plan establishes a basis for developing a security vision.** A corporate plan emerging from the experiences of those involved and the relevant analytical processes forms the basis for developing secure environments. A coherent plan should have as its objective the concern for the smooth running of the business. Typical examples of incoherence in corporate planning are seen in the two case studies. The divergence of clinical and business objectives in the Hospital Trust and the mismatch between corporate and departmental objectives in the Local Council illustrate this point. Hence an important ingredient of any corporate plan is a proper organisational and a contextual analysis. In terms of security it is worthwhile analysing the cultural consequences of organisational actions and other IT related changes. By conducting such a pragmatic analysis we are in a position to develop a common vision, thus maintaining the integrity of the whole edifice. Furthermore, this

brings security of information systems to the centre stage and engenders a subculture for security.

2. **A secure organisation lays emphasis on the quality of its operations.** A secure state cannot be achieved by considering threats and relevant countermeasures alone. Equally important is maintaining the quality and efficacy of the business operations. There is no quantitative measure for an adequate level of quality, as it is an elusive phenomenon. The definition of quality is constructed, sustained and changed by the context in which we operate. The Hospital Trust and the Local Council attitude for maintaining the quality of business operations is extremely rationalist in nature. The management have made an implicit assumption that by adopting structured service quality assurance practices, it is possible for them to maintain the quality of the business operations (for reference see figures 4.1 and 5.1). The top management, in the Hospital Trust for example, has assumed that their desired strategy can be passed down to the clinical and nursing professions for implementation. However, this is a very 'tidy' vision of quality, whereas in reality the process is more diffuse and less structured. In fact the 'rationalist approaches' adopted by the management of the two organisations causes discontentment, rancour and alienation among different organisational groups. This is a serious security concern. A secure organisation therefore has to lay emphasis on the quality of its business operations.

3. **A security policy denotes specific responses to specific recurring situations and hence cannot be considered as a top level document.** To maintain the security of an enterprise, we are told that a security policy should be formulated. Furthermore top managements are urged to provide support to such a document. However the very notion of having such a document is problematic. Within the business management literature a policy has always been considered as a tactical device aimed at dealing with specific repeated situations. It may be unwise to elevate the position of a security policy to the level of a corporate strategy. Instead corporate planning should recognise secure information systems as an enabler of businesses (refer to figure 6.2). Based on this belief a security strategy should be integrated into the corporate planning process, particularly with the information systems strategy formulation. Depending on risk analysis and SWOT (strengths, weaknesses, opportunities and threats) analysis specific security policies should be developed. Responsibilities for such a task should be delegated to the lowest appropriate level.

4. **Information systems security planning is of significance if there is a concurrent security evaluation procedure.** In recent years emphasis has been placed on security audits. These serve the purpose insofar as the intention is to check deviance of specific responses for particular actions. In the case of Local Council the whole concept of quality, performance and security has been defined in terms of conformity to auditable processes. A similar situation is seen in some functionalities of the Hospital Trust as well. The emphasis should be to expand

the role of security evaluation which should complement the security planning process. Section 6.3 covers security evaluation aspects in detail.

6.2.4 Summary

The aim of this section has been to clarify misconceptions about security policies. The origins of the term are identified and a systematic position of policies with respect to strategies and corporate plans is established. Accordingly various concepts are classified into three levels: corporate, business and functional (figure 6.1). This categorisation prevents us from giving undue importance to security policies, and allows us to stress the usefulness of corporate planning and development of a security vision. Finally, a framework for information system security planning process is introduced. Underlying the framework are a set of four principles which help in developing secure organisations. The framework, based on the IS planning process framework of Galliers (1987), considers security aspects to be as important as corporate planning and critical to the survival of an organisation. An adequate consideration of security during the planning process helps analysts to maintain the quality, coherence and integrity of the business operations. It prevents security from being considered as an afterthought.

6.3 Evaluation of security

Much of the literature on information systems evaluation takes a quantitative stance (Symons 1991). The emphasis has often been to carry out a cost benefit analysis of the technical systems (Hirschheim and Smithson 1988). Information system security literature has also had a skewed orientation towards quantitative security evaluation methods. Consequently risk analysis has emerged as one of the primary means to evaluate the security of information systems installations. This section discusses the notion of security evaluation. The first part identifies the various issues and concerns. The second part interprets security evaluation in the two case studies. Finally the third presents a synthesised perspective on evaluation of information system security.

6.3.1 Issues and concerns in security evaluation

Evaluation of security is problematic both conceptually and operationally. There are concerns as to what should be involved in the evaluation and how it can be carried out. Most security professionals are still locked in the belief that adequate security can be instituted through the use of evaluation criteria such as TCSEC and ITSEC. They fail to recognise the rationalistic and deterministic premises of these evaluation criteria. The criteria strive for maintaining security by looking at individual sub-systems, the basic principle being: 'overall information system security can only be maintained if individual sub-systems are made secure'. The emphasis therefore is to seek assurances for individual components (figure 6.3).

This is fine insofar as a computer based information system operates in a highly 'controlled' environment[4], but falls short in a commercial setting. There have been claims however that by using such criteria and by developing trusted computing bases, it is possible to develop highly secure environments (Charles *et al.* 1993). Such claims are rather dubious because it is assumed that all controls have been identified, implemented and adhered to by the employees; that is, employees are viewed as machines, acting mechanically. Current research results render support to the contrary view (see for example Dhillon 1994; Dhillon and Backhouse 1996; Parker 1991).

Assurances for individual components in figure 6.3 do not include organisational elements. It is assumed that people behave appropriately and so if adequate controls are implemented a secure state can be achieved. This belief is rooted in the categorisations of the evaluation schemes (table 6.1). The approaches emphasise more of the technical aspects of the systems. The thrust therefore is on the efficiency and effectiveness criteria and less on interpreting organisational consequences. A similar observation is made by Hirschheim and Smithson (1988) who stress the importance of understanding the functions and nature of the evaluation process as well as its limitations and problems. Much of security evaluation therefore has been ill-conceived and has focused more on the means rather than on the ends.

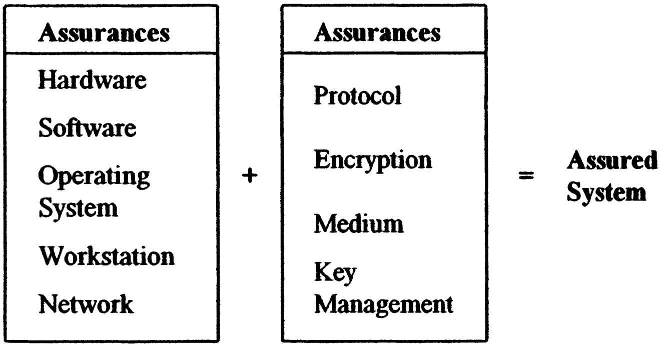


Figure 6.3 A functionalist viewpoint adopted by the current security evaluation practices

Moreover, even though systems analysis is regarded as the most important phase in developing good information systems, its evaluation is often carried out after the design has been completed and the system implemented (table 6.1). This is a direct consequence of limitations in the traditional evaluation processes. Many researchers have recognised such unsoundness and there has been some effort to rectify the problems. Lane (1985), for example, proposes the use of Checkland's Soft Systems Methodology to develop a 'rich picture' before conducting any kind of a risk analysis. Similarly Willcocks and Margetts (1994) stress the importance of a contextual analysis in evaluating system risks. Solms *et al.* (1994) propose a framework for security evaluation that gives importance to certain baseline controls. The problems addressed by these researchers fall into three categories. First, that there are flawed assumptions regarding the phenomena under investigation. Second, that evaluation is a simplistic process which assesses the causes and effects. Third, that there is an over-reliance on formal-rational approaches to security evaluation.

Problems identified by the researchers are directly related to the nature of security evaluation carried out by the professionals and to the mind-set of the people involved. This is clearly illustrated in Currie's information systems evaluation research in the manufacturing sector (Currie 1989). In this particular case engineering management was overtly critical of the formal accounting techniques as a basis for evaluation. But their own holistic and relatively qualitative approach was unacceptable to the top management. The emergent concern relates to the narrow perspective adopted by certain stakeholders, forcing them to interpret organisations as machines. It is for this reason that security evaluations are carried out in a very focused manner.

Table 6.1 Dominant security evaluation scheme (some categories have been adapted from Chokhani 1992)

System development phase	Associated evaluation phase	Related activities
System architecture and high level design	Preliminary technical review	Basic architecture review
Detailed design and implementation	System developer assistance phase	Security evaluation criteria interpretation (TCSEC/ITSEC); Review of design choices; Documentation review
Integration and testing	Design analysis phase	Systems analysis review; training; documentation review
Final testing (Beta testing)	Formal evaluation phase	Code review; test planning; testing; documentation review

This narrow tunnel vision is dominated by an engineering paradigm that advocates objectivity of knowledge both in the natural as well as the social worlds. It postulates both natural and social world phenomena as governed by immutable laws of causality. Therefore the main emphasis is to discover means, through unbiased observation, that will support them with empirical evidence. This is very much in the spirit of natural sciences. Most generic security evaluation approaches (for example see table 6.1) are based on causal laws, being prescriptive and consequently normative. The evaluation criteria such as TCSEC tend to be extremely objective and systematic. The security evaluation process is therefore considered in terms of methodologically discrete steps and develops linearly in a stable and a controlled environment.

Finally, current security evaluation practices are pragmatic in substance, mechanistic in style and ahistoric in context. The approaches deal with tangible issues that can be expressed intelligibly. Such problems generally render themselves to practical, mechanistic explanations. Hence historical and organisational contextual concerns are considered less important. The following sub-section interprets security evaluation in the two cases in the light of the issues and concerns identified above.

6.3.2 Interpreting security evaluation in the case studies

Both the Hospital Trust and the Local Council have made half-hearted attempts at conducting security evaluations. The problems can be traced to the manner in which the respective managements have viewed their information systems. System analysts and project planners in both cases tend to consider the newest developments in technology as offering some real benefits. It is a common belief in both the organisations that by implementing more advanced technology, the security of systems can be maintained. They have however failed to consider the real nature of information systems. Information systems are not just concerned with an understanding of hard facts and some *ad hoc* soft 'people' issues, but purely in terms of social interactions. Such a viewpoint forms the hallmark of information exchange and the basis for any evaluation.

Security evaluation in the Hospital Trust has been carried out on the basis of certain ontological beliefs. Various modules of CIS have been viewed as distinct entities with definitive boundaries. It is assumed that there are no external environmental influences on these modules. Consequently they represent a reality that is external to human consciousness. The aim of the evaluation process therefore has been to discern the objective reality of the various modules of CIS and assess their functioning in terms of the totality of the form (i.e. the physical state). The main objective of the CIS team has been to gain competitive advantage by focusing on the *efficiency* criteria. As a result the security evaluation has just focused on those aspects of CIS which produce efficiency. In the health care delivery process (figure 4.1) particular attention has been given to evaluating risks for service quality assurance. The Hospital Trust presented a two tier approach to security evaluation. A fairly informal approach was taken to evaluate risks related to contract management, service delivery and health care expenditure. The probable reason for this is the importance attached to *economy* and *efficiency* by the managers. At a more general level CRAMM was used to carry out the evaluation. The limited manner in which CRAMM was used indicated a deterministic perspective. As a result the impact of information systems on individuals and the organisations was viewed as a function of technology alone (a detailed discussion appears in chapter 4). Security evaluation processes therefore took a very narrow approach with a very limited use of risk analysis.

The Local Council case portrays a similar situation. The Council dwells on the philosophy of being 'customer oriented' and measuring service performance is its *raison d'être*. The prevalent belief is that the pursuit of 'efficiency through measurement' is strategic and leads to the well-being of not only the Council but also the public at large. Emerging from this, the strategic objective of *efficiency* is justifiably rational. Such an orientation of the Council is because of pressures from the Audit Commission which emphasised *economy*, *efficiency* and *effectiveness*.

Since the Council focused more on *efficiency* than *effectiveness*, the security evaluation process has been oriented towards auditing. Security audits at the Council are based on purportedly causal laws that take the form of extensive checklists. The thrust is on a scientific method which makes the evaluative process objective and systematic. The security auditors at the Local Council evaluate information systems by comparing existing controls to a given range of possible controls. Certain key controls are identified by selecting the best inventory of controls from the complete data set rather than examining the problem at hand. This results in providing solutions on basis of "what can be done" rather than "what needs to be done". Baskerville (1993) brands approaches such as checklist methods as belonging to the "first generation" of information systems design methodologies.

The mode of investigations and evaluations both at the Hospital Trust and the Local Council took a 'positivist' stance. Security evaluations were conducted in a cause and effect mode. This meant sorting out what is to be regarded as 'right' and what is to be regarded as 'wrong'. Such investigations resulted in 'hard', 'real' and 'tangible' measures of security. The evaluators failed to recognise that the degree of security is in fact a 'soft' and subjective issue. It is context dependent and largely unique to different application domains. In the case of the Hospital Trust the security review was carried out by conducting a 'business impact analysis'. Weights were established for confidentiality, integrity and availability of information for each of the business functions. This resulted in a final score being calculated for the level of security which was later ranked on a three point scale (high, medium and low risk). In the Local Council though no security measures were established, but the evaluation process proceeded in a logically sequential manner. Responsibility for security evaluation was given to an 'expert' who generates an allegedly objective and expert viewpoint of the level of security. The perspectives of the rest of the stakeholders are considered superfluous. The entire evaluation process is 'scientifically' planned beforehand. Such a planned process facilitates any rational observer reaching the same decisions given the objective facts of the situation.

The Hospital Trust and the Local Council have not considered different stakeholder perspectives in their security evaluation processes. Any such consideration calls for recognising different perspectives and subsequently entertaining, and legitimising, the non-rational aspects of human existence. It is a dominant belief in both organisations that incorporating multiple perspectives implies sub-optimal or dysfunctional choices on the part of the analysts. This tends towards elitism which is so typical of *functionalist* approaches in business management.

To summarise, in both cases the security evaluation process has been dehumanised. Determinism has been brought to the centre and all the contextual issues have been relegated to the periphery. Furthermore, the evaluation processes have sought to replace the non-rational qualities of human beings with mechanistic rules of rationality. Indeed, the hope is to develop measures for the level of security and to have an objective view of the consequences.

6.3.3 A synthesised perspective on security evaluation

It becomes clear from the above discussion that in order to maintain security of information systems, organisations need to develop security evaluation procedures that complement the strategic security vision. In the case of the Hospital Trust and the Local Council, such a match does not exist. In the Hospital Trust, security evaluation is an *ad hoc* affair, while the Local Council pursues a functionalist perspective in assessing the security of information systems. The limitations of such a position have been discussed at length in chapter 2. Based on the understanding gained so far, this section establishes some principles for evaluating the security of information systems.

Principles

There is a general lack of comprehension about the social context and how it interacts with the implementation of information technology. Therefore it is important to evaluate the linkage between the environment and the manner in which technology is implemented. This evaluation brings to the fore certain inherent risks that cause security concerns in an organisation. The previous sub-sections have demonstrated the limited viewpoint in conducting a security evaluation. The literature suggests risk analysis to be one of the primary means to develop secure systems. However in the context of the cases discussed in chapters 4 and 5, the use of risk analysis as a technique has been minimal. Criticising the prevalent evaluation approaches Webler *et al.* (1992) note that:

> technical risk assessment makes determinations of risk and acceptability based on fact selected arbitrarily. Facts are chosen and interpreted systematically, but in a way that is oriented toward drawing out select types of information and conclusions. Scientific perception has been systematically biased by powerful interests which are not interested in knowing the true essence of

> reality, but in assuring that the interpretation of reality suits those interests (p38).

Following this there is a need to establish principles which form a basis for security evaluation. In establishing such principles it is assumed that the criteria by which knowledge is constructed relate to describing organisational practices and how meanings are formed through tacit norms shared by actors in the situation under investigation. The epistemological belief therefore endeavours to interpret and analyse the social world from the participants' perspective.

1. **Security evaluation can only be carried out if the nature of an organisation is understood.** Security evaluation of information systems can be done if analysts develop an understanding of the nature of an organisation. This facilitates diagnosis of problems in a very effective manner. The framework introduced here allows us to consider different security problems for each aspect of the organisation. This allows us to comment on existing security measures and potential security threats. The framework incorporates both quantitative and qualitative aspects of security evaluation (figure 6.4).

In conducting a security evaluation it is important to classify various organisational co-ordination mechanisms. This is done by using Mintzberg's conceptualisation of an organisation into *Structure in Fives* (Mintzberg 1983b). Mintzberg's thesis is that:

> the structure of an organisation can be defined simply as the sum total of the ways in which its labor is divided into distinct tasks and then co-ordination is achieved among these tasks. ...The elements of structure should be selected to achieve an internal consistency or harmony, as well as a basic consistency with the organisation's situation... (p 2,3).

Based on this premise, security evaluation should focus on each of the five structures identified by Mintzberg. These are the: operating core; strategic apex; middle line; technostructure; support staff. The operating core encompasses the operators who perform basic work related to the production of products and services. The strategic apex ensures that an organisation's mission is served in an effective way and that it serves those who control it. The middle line represents managers with formal authority. It joins the strategic apex with the operating core. The technostructure consists of control analysts who serve to effect certain forms of standardisation in the organisation. The support staff consists of specialised units that provide support to the organisation outside its operating work flow.

The framework evaluates the efficiency, effectiveness and transformational aspects of information technology on to the potential beneficiaries. They are the individuals in an organisation, the whole organisation or a sub-group within an organisation – a business function. By superimposing the matrix on to Mintzberg's conceptual structures it is possible to identify co-ordination mechanisms within an organisation that help either in increasing the efficiency and effectiveness or to transform completely the work practices. The mapping provides analysts with a 'rich picture' and helps in identifying specific issues that need to be addressed in carrying out a security evaluation.

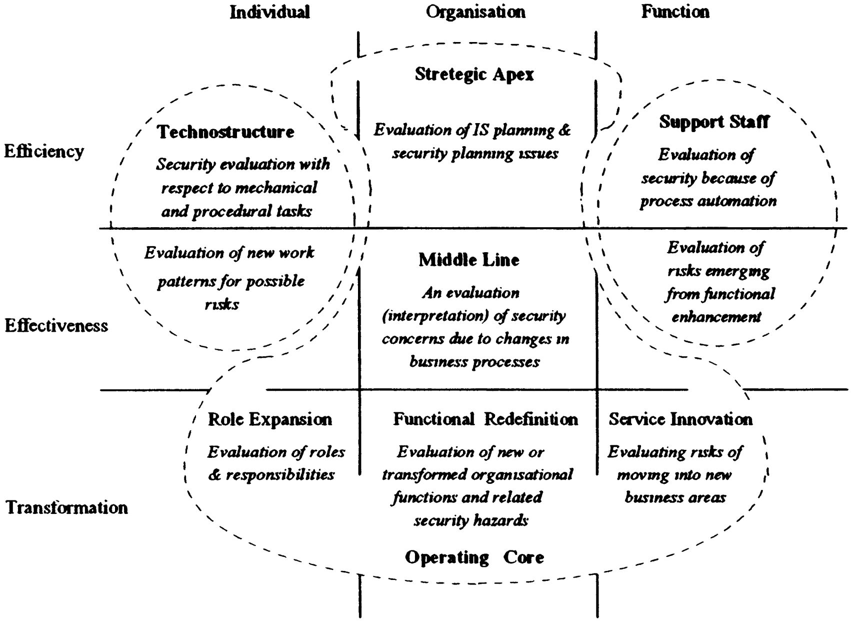

Individual
Organisation
Function
Efficiency
Effectiveness
Transformation
Stretegic Apex
Evaluation of IS planning & security planning issues
Technostructure
Security evaluation with respect to mechanical and procedural tasks
Support Staff
Evaluation of security because of process automation
Evaluation of new work patterns for possible risks
Middle Line
An evaluation (interpretation) of security concerns due to changes in business processes
Evaluation of risks emerging from functional enhancement
Role Expansion
Evaluation of roles & responsibilities
Functional Redefinition
Evaluation of new or transformed organisational functions and related security hazards
Service Innovation
Evaluating risks of moving into new business areas
Operating Core

Figure 6.4 An interpretive framework for security evaluation

The nature of the evaluation process varies in accordance with the structure under consideration. A synthesised perspective on generic issues of concern is presented in figure 6.4. The framework provides insight into the purpose of the particular evaluation. For instance, a security evaluation of the mechanical and procedural tasks focuses on the *technostructure* of the organisation and risks emerging from changes in formal business processes are concerned within the *middle line*. The basic purpose of information systems in the former case is to provide efficiency to individuals, while in the latter case it enhances the effectiveness of the organisation. Such a categorisation not only takes care of the organisational context, but also identifies issues that can be quantified. Having come to grips with this substantive task, the choice of a security evaluation tool or technique becomes a secondary issue.

It should also be noted that the security evaluation process is 'contextual' in nature. Security evaluation of information systems cannot be carried out by reviewing specific applications alone. It is important that a complete analysis of the formal and informal organisational aspects is conducted. Informal issues can be understood by examining silent messages in an organisation and subsequently interpreting them for security (for example see table 4.1 and 5.1). Security evaluation in the Hospital Trust and the Local Council, rudimentary as it is, is processual in nature and no consideration has been given to the contextual influences. The process of evaluation has been seen as a continuous sequence of actions explaining the origins, continuance and outcome of security measures. It is of fundamental importance that any evaluation is linked to an organisation's environment. The aim should be to describe systematically, properties and patterned relationships of organisational processes supported by computers, and of the changes in context through which such processes emerge. The evaluation process then looks at the interplay between the context and the processes. This helps in developing a fuller understanding of various consequences and forms a basis for establishing appropriate baseline controls.

2. **The level of security cannot be quantified and measured; it can only be interpreted.** Though security evaluation at the Hospital Trust and the Local Council can be considered as focused, clear and conceptually simple, the extreme focus on quantification may be considered inappropriate. The sequential and structured approach to security evaluation no doubt allows analysts to control the vagaries of the process, but it represents a naive and a limited view of the phenomenon. Furthermore, a skewed emphasis on rationality limits consideration being given to the socio-political aspects of an organisation. Therefore, what is needed is an approach which not only focuses on the *efficiency* and *effectiveness* aspects of the security controls but gives equal consideration to understand the 'soft' and subjective human aspects. Such an understanding can be gained by evaluating the prevalent meaning structures in an organisation (for example see tables 4.4 and 5.3).

3. **Security evaluation cannot be based on the expert viewpoint of any one individual, rather an analysis of all stakeholders should be carried out.** In both the cases, the security evaluation process has been highly dependent on the expert viewpoints. The Hospital Trust provides a typical example where respondents for the CRAMM review were chosen arbitrarily. A proper stakeholder analysis would have identified individuals specifically affected by the CIS system, helping to generate a better understanding of the context and better risk analysis. The situation in the Local Council was similar. The computer auditor is regarded as an expert who goes through the checklist of controls and identifies appropriate organisational controls. A proper stakeholder analysis is equally important when developing new security measures or modifying existing ones. This shifts the focus to the requirements rather than the end product.

6.3.4 Summary

The purpose of this section has been to provide a basis for proper security evaluation. It reviewed the skewed orientation of security evaluation towards functionalist approaches. In the light of these it identified the weaknesses in the evaluation practices in the two case studies. These related to the *ad hoc* nature of security evaluation approaches and to undue importance placed on the efficiency and effectiveness criteria in the two case studies. This formed the basis for establishing a set of principles that helped in evaluating security of information systems within organisations. The principles emphasise a contextualist orientation that allows analysts to identify the limits of quantification and to incorporate multiple perspectives in the evaluation process.

6.4 Design considerations for security

This section is concerned with information system security design. It presents a general discussion of issues and concerns when designing secure information systems and the relationship with systems development. This is followed by an interpretation of security design considerations in the two case studies. Finally, a set of principles is identified that should form the basis for designing and developing secure information systems.

6.4.1 System design and security

Most systems are not intentionally designed to be insecure; however specification and design methods are unclear in considering the security features. Such ambiguity can be attributed to the inability of system analysts to recognise security as a central component in development activities. Baskerville (1988), in his seminal security work, stresses that security should not be considered as an afterthought. He suggests that controls should be incorporated into the logical design phase of systems development. More recently the CCTA (1991) has designed an interface between CRAMM and SSADM. The underlying requirement is to consider security during the system developmental stages.

In practice, however, such recommendations have not been followed assiduously. This is partly because system developers and security professionals are still rooted in the ontological belief that computer based systems exist as prior socio-technical artifacts. Furthermore, since they regard reality to be independent and external to human consciousness, an information system is perceived to have a definitive boundary that separates it from the environment. Consequently, it is presumed that security can be built into systems by discerning the objective reality of the systems and by developing discrete steps to evaluate risks and to build respective countermeasures.

In terms of system design activities there appears to be difficulty in giving due consideration to such objective issues. In reality, systemic hierarchy is subjective and the boundaries between a system and its environment are blurred. The issue becomes even more complex when the purpose is to develop secure information systems. In the literature there have been endless calls to consider the social issues prior to providing technological solutions, but there have been problems with changing the mindset and the tunnelled vision of analysts. Such mindsets can be linked to the design ideals of the system developers. Klein and Hirschheim (1987) synthesise the core design ideals as originally postulated by Rule (1974) and Kling (1978). Table 6.2 compares them with the sociological paradigms of Burrell and Morgan (1979) and identifies respective security design ideals. Orienting information system designers to particular ideals not only determines the nature of the system being developed but also the manner in which security is handled.

Table 6.2 Classification of 'mindsets' for security design (the table, in part, is based on the categories identified by Rule 1974, Kling 1978, Burrell and Morgan 1979 and Klein and Hirschheim 1987)

Core design ideal	Sociological paradigm	Security design ideal
Private enterprise ideal: Main objective is profitability; Organisation rationalisation is considered fundamental	Functionalist: Objective is to gain competitive advantage through objective, structured and scientifically valid causal relationships	Systems ideal: The primary goal is that systems should be elegant, well-organised, efficient and reliable. Security can be designed by systematically evaluating the functionalities. The designs are ahistorical and non-contextual
Statist ideal: Strength and efficiency of institutions is the highest goal	Radical structuralist: Support a philosophy of dialectical materialism; Propound deterministic prescriptions for sustaining competitive advantage	Dialectical inquiry ideal: Systems should facilitate in generating 'objective' knowledge through the synthesis of most opposing points of view. Security designs are based on exposing conflicts and then negotiating among affected partners
Libertarian ideal: Civil liberties are maximised; profitability or welfare to institutions are sacrificed if they conflict with prerogatives of the individual	Radical humanist: Focus on liberating managerial consciousness from cognitive domination	Emancipatory ideal: Systemic concepts of hierarchy and emergence are used in systems design, the aim is to emancipate humans so as to realise their full potential. Because of blurred system boundaries, security designs and analysis of risks remains an elusive phenomena
Neopopulist ideal: Practices of enterprises should be easily intelligible to ordinary citizens and be responsive to their needs	Interpretivist: The endeavour is to comprehend subjectivity of experiences from the viewpoint of human actors rather than their own	Contextualist ideal: System designs emphasise content, social context and the associated processes. Security designs are not imposed but are based on an organisation's communication patterns and the intentional acts of agents involved

An understanding of the design ideals helps to overcome the pitfalls and take advantage of the opportunities when considering security design. Thus it becomes possible to develop a broader vision of the organisational environment and the associated security measures. It should however be noted that it is impossible to achieve a completely secure state. Security designers can work towards a secure state if they consider the development process to be socially constructed and emerging from the intersubjective experiences of people. A secure system could then be one where there is a coherence in shared meaning of the organisation and those of its members. This shows allegiance to the neopopulist core design ideal (table 6.2) requiring a contextualist understanding of the environment for system design and development.

At a methodological level, a secure system can be designed if a computer based information systen. is specified with ideologies rooted in the contextualist ideal. It is often contend›d that contextualist and interpretivist ideals provide little in terms of tangible and comprehensive approaches for system developers. However, Wing (1990) shows how a broader understanding of the pragmatic and semantic content provides a basis for writing system specifications using traditional specification methods[5] (e.g. Z, VDM, Larch, RSL). She stresses the point that the 'syntactic domain' (i.e. the program modules) should satisfy the 'semantic domain' (i.e. what the program modules mean in the real world). This requires a consensus to be struck between the behavioural and structural aspects of the specification. In practice systems that specify some structural constraints do not necessarily satisfy the same behavioural constraints. But the ability to identify the boundaries between what can and what should be formalised allows security to be considered adequately. Wing points out that:

> ...behavioural aspects, such as security, are included as part of, rather than separate from, a systems functionality. If the overall correctness of a system is defined so that it must satisfy more than one behavioural constraint, a system that satisfies one but not another would be incorrect. For example, if functionality and response time were the constraints of interest, a system producing correct answers past deadlines would be just as unacceptable as a system producing incorrect answers in time (p11).

The following sub-section interprets security design in terms of behavioural and structural specifications. It takes complex real life examples from the case studies and analyses situations which should have best been handled informally. These are then delineated from the more routinised ones. Some of these formalisable activities can then be computerised. Such understanding reveals the ambiguity, incompleteness and inconsistency in a system, thus allowing us to interpret the correctness level. Security designs therefore are linked to the requirements assessment and system specification stages of the developmental process, rather than with identifying countermeasures after a system has been designed and implemented.

6.4.2 Interpreting security design considerations in the case studies

As we have seen security design considerations in both the Hospital Trust and the Local Council are rooted in the systems ideal. In the case of the Hospital Trust it is relatively easy to identify the 'mindset' of systems developers since a new IT infrastructure is being developed and there is only one integrated information system. The Local Council, by contrast does not have an integrated information system in place (although a federated structure is being put in place), instead individual divisions and sub-divisions have their own small systems. However, in both cases, the primary motivation of system developers has been to produce elegant systems that address the 'efficiency' and 'effectiveness' drive of the NHS Management Executive and the Audit Commission.

The system development activities in the Hospital Trust have not been based on the real needs of the organisation but on the whims and fancies of a select group of people. Accordingly, system developers and project planners have considered systems to be good if they are based on causal laws, objective observations and empirical evidence. Therefore the totality of the organisation is seen as the sum of its parts, with each part serving a definitive function. Because of such beliefs in designing systems, factors such as organisational politics, culture, conflicts and resistance are considered as a consequences of ignorance. Thus according to the system developers and the project management team, CIS is an objective, structured, scientifically valid system; it manipulates the causal laws of the health care environment to yield a competitive edge. Security therefore has been considered as an 'afterthought' with security measures being reactive in nature rather than proactive. In this respect security problems are not seen as arising out of misinterpretation of data or misapplication of rules, but as gaining access to a computer or not.

The Local Council presents a somewhat different situation. Computer based systems have evolved over a period of time and have become an integral part of the work culture. New systems development is dictated by the corporate information systems strategy. The IT department has had an advisory role with respect to systems in place and any new needs that may arise. In recent years this function has been outsourced, leaving the management with ample time to initiate 'total quality initiatives'. However, particular interest groups within the organisation have been making attempts to use technology as a means to assert their influence. Typically, there are attempts to link electronically the diverse functions (ranging from waste collection to social services and housing), so as to create an 'integrated reporting system'. Such plans go against the ethos of generic information systems planning strategies currently in place within the Council and raise a new generation of security design questions. The security arrangements of such system design initiatives are rooted in the systems ideal, as are the initiatives themselves[6].

The preconceptions with respect to systems design in the two cases present an elitist nature of developmental activities. The belief in scientific rationality of the system developers legitimises and endorses their preconceptions of how organisations and businesses ought to function and be structured. However, organisations and the constituent business processes comprise conflicting interest groups and differing viewpoints, which may not necessarily be represented rationally. Therefore, the systems ideal adopted in the two case studies appears unscientific and denying of the social reality. This has severe consequences for the manner in which security has been considered in the design process. Findings and analysis of the two cases reveal that indeed security has been considered as an afterthought, as postulated by Baskerville (1988).

An issue of concern in both the cases centres around vague security goals. This is partly because of the blind faith of people involved in system development. Consequently, system design objectives have emerged from the objectives of system developers rather than from the actual business need. This is more so in the case of the Hospital Trust than it is in the Local Council. As a result of system developers setting the agenda, the emphasis within the Hospital Trust has been to automate a process at the expense of evaluating a process against its purpose. As a result of this, members of the project team focused their attention on making the system 'fit in' with what is currently done. In relation to security designs this has typically resulted in 'over-engineering' of the controls. Because clear objectives and relative priorities have not been stated, system developers become involved in incorporating the most trivial of the controls into a system specification. Such designs not only become unacceptable to most people, but are also unresponsive to change and expensive to maintain. The nature of the designs also questions the correctness and completeness criteria of the systems analysis and design activities. This has implications for the integrity of the information technology infrastructure – a serious security threat.

Another concern with respect to security designs in the two cases has been the 'big is beautiful' syndrome. Project teams in both the organisations have been overwhelmed with the idea of developing large integrated complex systems. Although such ideas have been realised in the Hospital Trust, in the Local Council the initiatives are still in the conceptualisation stage. Ideally a computer based system automates only a small part of the rule based formal system of an organisation, and commensurate with this relevant technical controls are implemented. However, our analysis of the case studies reveals an over-reliance of the organisation on the computer based systems and related technical controls (see figure 6.5).

The Hospital Trust typically represents a situation where the computer based information system and the related controls have been over-engineered. A system that not only spans the formal rule based work practices but also computerises the traditionally informal activities has severe implications for the integrity and coherence of the whole organisation (detailed discussion appears in chapters 4 and 5). In such situations, it is often the technical controls that dominate. Little or no consideration is given to the more pragmatic and cultural issues that help in developing appropriate norm structures that act as a natural system of checks and balances. The Local Council though does not have an 'over-engineered solution' as yet, but if integrated reporting systems are put in place, the Council will face similar problems as the Hospital Trust.

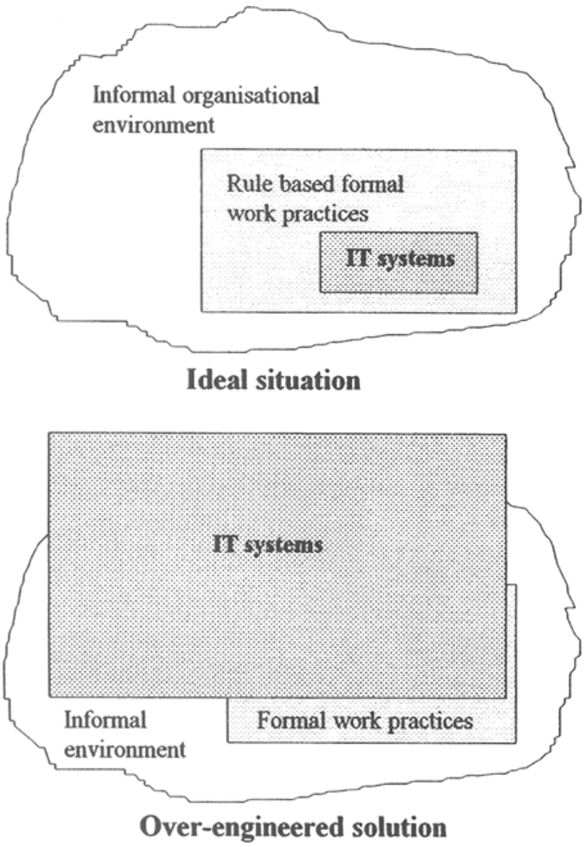


Figure 6.5 Over-engineered systems and related security controls

6.4.3 A synthesised perspective on designing secure systems

The discussion so far suggests that inadequate designs are a consequence of functionalist preconceptions of the developers as well as the managers. Furthermore, security design cannot be separated from the core system development activities, a secure system is the one in which requirements have been assessed specified and implemented properly. Lessons learnt from the case studies are synthesised into a set of principles for designing secure systems.

Principles

The design and development of computer based systems is a social process that encompasses communication, learning and negotiation between different stakeholders in an organisation (Walsham 1993). The process draws upon structured methodologies as a means of accomplishing the design and development tasks. The methodologies evaluate the problem domain by either taking a technical and an objective view of the phenomena or by being more subjective in interpreting the issues. The objective orientation in system design emerges from a 'systems ideal' and a 'dialectical inquiry ideal', while a subjective viewpoint is associated with an 'emancipatory' and a 'contextualist' design ideal (see table 6.2). Security design methods are rooted deeply in systems design methods and therefore share the same ideals. The question that is often asked is whether we need a separate security design methodology or are the existing systems design methodologies sufficient? The analysis of the findings presented in this book indicate that indeed security can be integrated into the existing systems analysis and design approaches. The emphasis however should be less on the technical, programmable aspects and more on the requirements elicitation and specification criteria. This adjustment will produce a system that is comprehensive, correct and complete. Having developed a good quality system would implicitly mean that it has a good security design. Such beliefs form the basis of principles, adherence to which would determine the integrity of the designs.

1. **The adherence to a specific security design ideal determines the overall security of a system.** Since systems development and security designs relate to shaping of new forms of identity at work, new social structures and new value systems, an appropriate design ideal should be identified and adhered to. Research presented in this book suggests that the contextualist ideal is most appropriate for developing secure systems. However, the choice is often determined by the mindset of the people involved in the systems development activity. In this case it is worthwhile knowing the worth of the respective viewpoints so that the overall quality of the systems is maintained.

The systems ideal is criticised on the grounds that it requires ahistoric and non-contextual controls to be implemented during systems design. The systems design in itself is based on isolating dependent and independent variables from their context. Consequently the designs and the related controls are not situational, holistic and emergent. Rather they are grounded in objectivity. Objectivity by itself is not criticised here, but since the emphasis is to institute controls by giving primacy to the mechanics of socio-economic structures there is a significant element of determinism in this ideal. The emancipatory ideal does not provide any practical guidance for designing secure systems. Moreover since it is based on a preconception that there are blurred hierarchies and boundaries in an organisation, the implementation of controls remains an elusive concept. The most suitable security design ideal, and the one propounded in this book, is the contextualist ideal. Thus in developing systems and instituting controls, primacy is given to realism of context, and theoretical and conceptual development is the goal (Pettigrew 1985).

2. **Good security design will lay more emphasis on 'correctness' during system specification.** Correctness in system specification is the key to good security design. However, system developers and researchers alike have had

varying degrees of success in proposing mechanisms which facilitate the development of appropriate systems. There have been attempts to take the 'best' aspects of various approaches so as to extend the usefulness of the methodologies. Avison and Fitzgerald (1988) however note that doing so may result in the whole spectrum of information systems development lacking a coherent philosophical base.

In order to specify systems that are 'correct', it is useful to distinguish between the human information communication functions and the technology platform needed to carry out such processing. The underlying belief here being that an organisation in itself is an information system which allows human agents to communicate with each other, resulting in purposeful activity. In this case a system specifier should first address the social issues related with beliefs and expectations of different people, their culture and value systems. Next the intentionality and communications of various agents needs to be analysed. This is followed by developing an understanding of the different meanings associated with the actions. Such an interpretation provides an analyst with a deep understanding of the organisational issues and facilitates decision making about what aspects can best be supported by technology. There are no discrete steps to arrive at such a decision; the process is interpretive and contextually motivated. Understanding so gained allows formal specification of the rules and procedures, formal structures and logical connectivity of different modules. These can then be translated into computer programs. The emphasis here is on developing a sound understanding of the deep seated pragmatic aspects of the problem domain. The better an understanding, the greater is the probability of achieving 'correctness' in system specifications.

3. **A secure design should not impose any particular controls, but choose appropriate ones based on the real setting.** The preoccupation of most system developers with respect to implementing controls is with 'what ought to be, rather than what actually is'. This flows from the assumption that there is only one best way to organise elements of a system. In such a situation prescriptive recommendations are made and a system is expected to behave in a predetermined manner. In fact control is "the use of interventions by a controller to promote a preferred behaviour of a system being controlled" (Aken 1978). In that sense, a control refers to a broad range of interventions. Such interventions relate to the composition and modification of the tasks of individuals or groups, to an increase or decrease in the number of formal rules and procedures or changes in management practices related to training and education. In practice controls do not always provide the desired results. Therefore it is important to evaluate the context in which controls will be implemented.

With respect to systems analysis and design, a major threat is that control issues are generally considered when user requirements have been abstracted into a logical model[7]. Without having contextual clarity, such controls generally lack the catalysing effects that were originally claimed for them. Leavitt (1964), while addressing the issue of organisational change, refers to such 'acontextual' controls as "one-track solutions". These are solutions that are offered for isolated problems without considering other control systems and their contexts. Controls therefore cannot be placed arbitrarily within the design of a system. Implementing system security controls is context driven and should be considered as a major managerial issue.

6.4.4 Summary

This section stresses the significance of a contextual analysis for designing secure systems. It emphasises the narrow viewpoint adopted while specifying the requirements of a system. By emphasising and eliciting the security issues and linking them to requirements analysis, the design for good security is equated with the 'correctness' issues during systems development. Since the notion of security design ideals classifies the mindsets of people involved in systems development, implications for the quality of secure designs can be interpreted. This forms the basis for a set of principles that determine secure systems development.

6.5 Implementing information system security

This section discusses the concept of implementing information system security measures within organisations. The intention is to analyse the effectiveness of security implementation with respect to the processes in place, the content of the change and the context of the organisation. This is accomplished by understanding and interpreting the actual implementation of solutions by security specialists, managers and staff. The first sub-section reviews some ideas pertaining to implementation and security. The second part interprets security implementation in the two case studies. Finally a synthesised perspective on implementing security is presented.

6.5.1 Implementing security and policy considerations

Although there is a significant amount of literature on security policies, evaluation and design, there has generally been a lack of research emphasis on the implementation aspects of security. Baier *et al.* (1988) identify implementation problems as a consequence of bureaucratic incompetence in executing policies and the conflicting interest groups. This situation is further complicated when there is inherent ambiguity in the policy making process and in related organisational actions. These ambiguities fall into three categories: uncertainty, confusion and contradiction (Martin and Meyerson 1988). Contradiction refers to the cultural manifestations of any changes brought about because of security measures. Confusion results from a lack of communication between different stakeholders in a particular domain. Uncertainty refers to the inability to predict the consequences of any security measure. In terms of implementing computer based systems, the three categories provide a means to interpret the security level of the computer based solutions and the organisational information systems.

A similar classification is also provided by Lyytinen and Hirschheim (1987). They categorise factors of relevance to information systems implementation into three parts. These include the environmental aspects including the individual, organisation and the wider context; features of the systems development process; and technical features of an information system. This categorisation, along with the ambiguity classes, can be extended to evaluate security implementation issues. Table 6.3 identifies the various classes which are subsequently discussed below.

Table 6.3 Problems in implementation and the related implications

Problem	**Illustration of a security measure**	**Implication**
Contradiction – resulting from a lack of a clearer understanding of the environmental influences	A typical control that questions the expectations of an individual	Need to evaluate security strategies and shape the political dynamics of change
Confusion – resulting from an inability to develop a correctly specified system	A typical control that means different things to different people	Need to communicate and involve users
Uncertainty – resulting because of inappropriate technical security measures in place	A typical control that radically changes the processes of doing things	Need to motivate change

There is complex interrelationship between how a particular security measure is conceived, the manner in which it is designed and the form of its implementation. Often the conceptualisation of security measures with respect to computer based systems is highly politicised. This has direct consequences for developing security strategies and policies (see section 6.2). Commenting on the manner in which policies are developed in organisations, Baier *et al.* (1988) argue that managers place more stress on the symbolic meanings of policies than on their implementation. This lopsided emphasis is concerned with overselling the cause and exaggerating support for a particular policy. Managers also give undue consideration to the constituent elements, thus being vigorous in enacting policies but lax in enforcing them. Such an attitude can be linked to the functionalist roots of the policy makers which imposes determinism, emphasises rationality and gives little consideration to the socio-political aspects during policy formulation. An understanding of the way in which security measures are conceptualised facilitates clarification of various contradictions in the implementation process.

If the security measures are conceived properly, it allows analysts and managers to develop systems that are complete, correct and with appropriate security controls. This aspect of designing appropriate security controls also determines the success in implementation. Warman (1993) emphasises the communicative content of secure systems development as being a key to effective implementation of security measures. He states:

> Managers must be seen to be bound by security mechanisms at least as much as other employees. Without that compliance, the security measures will not be taken seriously, and in the best case will then be rendered ineffective against the threats. The worst case, a half-hearted attention to security can suggest that a similarly gentle approach will be taken with any transgressions, and this is not a message that managers should communicate to their staff (p91).

Therefore an awareness of user requirements and perceptions becomes the basis for implementing security measures. The numerous organisational rules and regulations pertaining to security measures take second place. Instead the focus shifts on to explaining decisions that went behind particular security measures. This results in understanding and compliance with the measures. In this respect user issues become a key to improve security in general, and computer security in particular (Warman 1993). Though user participation as a concept has been well accepted in the system development activities, with respect to eliciting appropriate security controls its significance has been rather limited. This can be related to the preconceptions of most analysts, who are grounded in the engineering paradigm. Consequently, the controls implemented in the systems take an authoritarian, top-down approach, and are strongly influenced by cybernetic theory.

Related to the influences of policy and design on implementation is the form of the security measures that are instituted. The form of the measures has serious consequences for the effectiveness of the overall security measures of a computer based system. Typically, if a set of controls hinders the normal course of work, there is an increased likelihood of complacency on the part of the users in adhering to the security measures. In such situations users tend to find ways around the controls thus making them ineffective. Thus in order to achieve a smooth implementation of security measures, it is of paramount importance that the controls are conceptualised and designed appropriately. A similar viewpoint is advocated by Dhillon and Backhouse (1996) who stress the importance of developing a holistic viewpoint in implementing controls. They focus on the importance of understanding and balancing the pragmatic controls with formal and technical ones. The implementation process is strengthened if an early evaluation of various system developmental activities is carried out.

6.5.2 Interpreting security implementation in the case studies

There is a wide variance in the implementation of security measures in the Hospital Trust and the Local Council. While in the case of the Hospital Trust the process of implementing security measures was in a complete shambles, the Local Council presented a situation of partial success. The implementation process in the two cases can be interpreted by using the classification proposed in table 6.3.

Implementation of security measures in the Hospital Trust has been such that the controls question the expectations of the key players. This is because of the failure to appreciate environmental influences and the context of the systems. A typical example is found within the pharmacy module of CIS. This module presents problems at two levels. First, the delivery of the system has been excessively delayed resulting in discontentment and dissatisfaction among the pharmacists. Second, the planning manager has specifically demanded extra controls in the module such that therapeutic drug monitoring and new drugs policies can be adequately monitored. This questions the values and expectations of not only the pharmacists but also the clinicians. The prevalent norm in drug prescription is that doctors 'recommend' and pharmacists 'give', but CIS forces doctors to 'give' and pharmacists to 'recommend'. Since the controls are changing the expectations of different groups there is a need to institute mechanisms for smooth implementation. Not only should the political dynamics of change be evaluated but also the security strategy should be realistic and based on a clearer understanding of the environmental influences. This has not been done in the case of the Hospital Trust.

In the Local Council though there is an emergence of a two-tier system developmental activity the controls pose few contradictions. This is primarily because no radically new systems are being implemented. However, if the proposed integrated system that would link all the departments is made fully operational (as part of the federal IT infrastructure), it would implement controls that go against the current organisational context. At the present time the Council is experiencing an increased trend towards outsourcing. As a result the operations of the in-house IT department have been substantially scaled down. Against this backdrop, any new control needs to be evaluated against the strategic agenda and the different interests of the key players. Failing to recognise these factors would result in an unsuccessful implementation process.

With respect to the correct interpretation of existing controls, the Hospital Trust presents a case of complete 'confusion'. Every control implemented within CIS is being interpreted differently by different people. Implementation of a simple audit control that collects data from different sources and collates it within CIS is considered as imposing a 'total control environment'. This is direct consequence of 'over-specification' of system requirements. Rather than identifying only a small number of pertinent controls that should have been implemented in a computer based system, all the existing controls of the paper based system have been automated. Confronted with the argument that new norm structures are being implemented, managers at the Hospital Trust contend that "nothing new has been implemented". This clearly shows that neither the user requirements were assessed in the earlier stages of system development, nor were the meanings of different controls understood.

The Local Council presents similar problems. Managers within the Executive Office conceived of certain controls that should exist at the departmental level. These were later translated into daily and weekly reports being generated. All this was carried out without even understanding the prevalent work practices. The managers presumed that they knew what was happening at the departmental and sub-sectional level and hence were in a position to introduce the changes. However, the employees at the 'front-end' considered the actions to be vague since the controls did not have any meaning in their working environment. Clearly, the managers should have understood the context better and also involved the actual users in the process.

The implementation of many controls within CIS has resulted in uncertainty within the Hospital Trust. This has been because certain controls have actually forced changes in work patterns. This does not imply that all changes are unnecessary, but the manner in which these are brought about determines the success or failure of the implementation process. In the case of CIS for example the control transform that forces a validity check, for the care provided with the information in an individual care plan, raises issues of user acceptance. The main user of this facility is a consultant doctor. In practice doctors rely on ward rounds for such a validity check rather than solely on an individual care plan. This has a number of consequences. First, the doctors are demotivated to use the system since it does not fulfil their immediate needs. Second, because of an ongoing discordance between the utility of care plans and ward rounds (see chapter 4 for details), such an implementation brings rancour and conflict to the forefront. Therefore, the very nature of the controls becomes a hindrance to their implementation.

Within the Local Council work practices have evolved around the existing control structures, typically those within computer based systems. However new controls have faced significant resistance. This has again been because they force changes in the work patterns. In practice it is possible to bring about such changes, but users need to be motivated. Typically, the identification and surfacing of dissatisfactions with the current security control measures can be the first step. Then by participating in the change process, identification of rewards and giving time and opportunity to disengage from the present state can often result in successful implementation of new measures. The Local Council fell short of motivating change, thus resulting in significant uncertainty among users. For example, a manual control was implemented that compares the 'service provision' data logged on to the departmental systems with the complaints received in the central office. The comparison generates a report on the mismatches. Though the immediate users were not affected directly, their work patterns changed significantly. Therefore the emphasis now was to make sure somehow that there was very little discrepancy in the figures. The intention of such a control was no doubt to increase the level of customer care, but since it was not 'sold' properly, it resulted in significant uncertainty among the users.

Successful implementation of security measures does not start after a system has been conceived, developed and evaluated, but at the beginning of the process. This ensures not only the appropriate identification of controls, but also their proper implementation. The next sub-section synthesises the various concerns raised above and identifies some principles which would determine appropriate implementation of the security measures.

6.5.3 A synthesised perspective on security implementation

The discussion so far links successful implementation of security measures to the wider contextual factors that affect content of the security strategies and the emergent system designs. In the case of the Hospital Trust and the Local Council, such a link was very weak. This suggests that in both the organisations the management and the analysts ignored the issues and concerns of the users. Consensus among different user groups is not always possible or even desirable; completely rejecting the requirements is also undesirable. This jeopardises the professional integrity of the managers. Furthermore, by being oblivious to the perspectives of other interest groups and the wider context, the implementation of security measures becomes difficult and ineffective, thus increasing the chances of occurrence of negative events. Based on the understanding gained, this section establishes principles necessary for bringing about successful implementation of the security measures.

Principles

Implementation of security is guided by the core principle: "garbage in, garbage out". This means that the ultimate consequence of implementing a security measure is dependent upon how it was conceived in the first place. If the initial thrust with respect to security measures was on rationality, mechanistic rules, scientific and technological solutions by relegating everything else to the periphery, then the possible outcome could be an ahistoric and an acontextual implementation. This may result in breeding resistance to change, conflicts and rancour among different people. As Keen (1981) notes:

> information systems development is an intensely political as well as technical process and organisational mechanisms are needed that provide MIS managers with authority and resources for negotiation. The traditional view of MIS as a staff function ignores the pluralism of organisational decision making and the link between information and power. Information systems increasingly alter relationships, patterns of communication and perceived

influence, authority and control. A strategy for implementation must therefore recognise and deal with the politics of data and the likelihood, even legitimacy, of counterimplementation (p24).

Though Keen's primary concern is with implementing computer based information systems, the ideas are equally applicable to implementing controls and specific security measures. This is because implementation is essentially a social process and follows a similar pattern to any other implementation. However, in the particular case of security, implementations should be based on the following principles:

1. **Successful implementation of security measures can be brought about if analysts consider the informal organisation before the formal.** Any security manager would say that informal organisation takes precedence over formal organisation, especially when the concern is to implement some security measures. It is for this reason that the implementation programme should concentrate on educational programmes which aim to teach new values, and introduce new norm structures. These, if accepted, create social pressures seeking conformity to preferred behavioural patterns. In the case of implementing security measures, the preferred behaviour would be the one in which members of the organisation operate under a set of controls. This process of inculcating a new culture has traditionally been the premise of the organisational development programs. Such programs gain further prominence when the implementation tends to constrain working patterns.

Our focus on the informal organisation may engender a value system and introduce some norms such that a preferred behaviour is achieved. However, the process may not make any headway if an organisation works under a very rigid autocratic setting. Therefore the education and training programme prior to introducing any security measure should also focus on the manner in which the formal organisation complements and reinforces changes in their behaviour. It should, however, be remembered that there is no one best kind of a formal organisation that would facilitate better acceptance of changes. The very concept is as parochial as the 'mindset' that believes in the notion.

This principle therefore draws attention to the traditional approaches that have been prevalent within the human resources departments. Unfortunately, the 'mindset' of the security professionals is restrictive and hence programmes such as organisational development are not easily taken on board.

2. **Implementation of security measures should take a 'situational issue-centred' approach.** There are no discrete steps in implementing a change. This is especially true in the high risk area of implementing security measures. For example, security controls cannot necessarily be made acceptable by logically considering the behaviour of an individual employee. Rather the focus should be on the small group in which an employee works and the related intergroup issues. The main concern with security implementation is that spontaneity of

resolving any issue can be stifled. It may just be that an individual relates the problems of implementing a particular security measure with the formal organisational structure. In this case it may be inappropriate to concentrate exclusively on inculcating a set of norms, as propounded by principle 1 above. Instead the focus should be on redesigning the structure. This shifts the emphasis from an 'individual-based' implementation programme to a more situational issue-centred one. Successful acceptance of security measures in this context is a purely managerial activity, but so is the whole process of implementation.

3. **To facilitate successful implementation of security controls, organisations need to share and develop expertise and commitment between the 'experts' and managers.** The very nature of the security measures creates a dichotomy of roles. Not everybody in an organisation understands the controls and the technical aspects of the infrastructure. This results in a substantial degree of over-dependence of managers on 'experts' (these may be the outside consultants), to bring about a successful implementation of the systems and the embedded controls. Often these controls are not even overtly visible to most managers. It is usually the complex interplay of the systems, and the controls with the environment that results in some emergent effect. Because of this lack of awareness, the 'experts' tend to recommend general methods and techniques to deal with the implementation issues. Moreover they do not have the responsibility of the daily operating decisions. Consequently there is conflict and discontentment with the whole implementation programme. This is typically illustrated by our two case studies. In the case of the Hospital Trust, the outside consultant dictated the control identification and implementation programme. It resulted in a completely inappropriate set of solutions. In the Local Council on the other hand the top management's inability to comprehend the expectations of the users is resulting in an unsuccessful implementation. There is a necessity to share and to develop commitment among the experts and the manager. This would mean that organisations need to train their staff and develop a good level of communication among them. This would also make explicit the level of competence of the major players.

6.5.4 Summary

The purpose of this section was to make explicit the general problems of implementing security measures. The underlying argument is that implementation of controls is a managerial activity. Hence there is a need to develop appropriate competencies to deal with the resultant issues. This is illustrated by classifying different kinds of problems of implementing security measures and interpreting the manner in which these have been dealt within the case study organisations. Finally principles, grounded in a contextualist understanding of the implementation process, are presented. These hark back to the importance of traditional *organisational development* programmes.

6.6 Conclusion

This final section draws together some conclusions about interpreting the management of information system security. It is not the intention to draw out statistical generalisations from this interpretation. Instead the evaluation of the two cases has formed a basis for understanding the business and the social organisation. This allows us to evaluate those features which are most important in managing the security of information systems. Analysis of the case studies in chapters 4 and 5 identified security policies, security evaluation, system security design and implementation attributes as the key features in managing information system security. This chapter has explored issues surrounding these themes, with examples drawn from the two cases. The findings have then been synthesised into principles that are highly pertinent to the management of security. Within a given organisational setting these principles provide a framework for establishing a 'natural' and informal system of checks and balances. Better understanding of the principles further increases the awareness and sensitivity towards security among the broad base of employees, rather than merely concentrating on just a few who have responsibility for computer systems.

To manage information system security, managers in organisations will have to devise appropriate ways of coping with the development and use of IT based solutions. Since there is no universal 'recipe' for such secure developments, IT professionals will have to evaluate the nature of the organisational environment before considering whether to implement any IT based solutions and the related security measures. They will have to address issues arising at three levels: technical, formal and informal. At a technical level the choice of an appropriate technology and system and security design methodology is very important. The use of a 'hard' approach, such as SSADM, limits the consideration of the 'real world' issues. The situation becomes more deplorable if such approaches are not used appropriately. This especially becomes obvious when the problem situation is characterised by conflicting objectives (for example the Hospital Trust case). Equally important is the choice of hardware and software which allows 'interconnectability' and 'media independence'.

At a formal level an organisation needs structures which support the technical infrastructure. Therefore formal rules and procedures need to be established which support the IT systems. This would prevent the misinterpretation of data and misapplication of rules in an organisation and help in allocating specific responsibilities. If a new technology is being implemented, there is a need for a formal team which gives strategic direction to the project. Finally, a clearer understanding of the structures of responsibility needs to be developed. This would facilitate the attribution of blame, responsibility, accountability and authority (Backhouse and Dhillon 1996; 1995).

The informal level needs to address more pragmatic concerns. It is often the case that a new IT infrastructure is presented to the users in a form that is beyond their comprehension, thus being a major demotivating factor in their accepting the new technology. Thus users should be made aware of all the features and this should be supplemented by an ongoing education and training programme. The emphasis should be to build an organisational sub-culture where it is possible to understand the intentions of the management. An environment should also be created which is conducive to developing a common belief system. This would make members of an organisation committed to their activities. All this is possible by adopting good management practices. Such practices have special relevance in organisations which are highly decentralised and thus have an increased reliance on third parties for infrastructural support (for example the Local Council case). Inadequate understanding has consequences of increased vulnerability of organisations thereby increasing the probability of risks.

[1] The Oxford English Dictionary defines policy as: 'prudent conduct, sagacity; course or general plan of action (to be) adopted by government, party, person, etc.'. In business terms 'policy' denotes specific responses to specific repetitive situations. Typical examples of such usage are: 'educational refund policy', 'policy for evaluating inventories', etc.

[2] This premise is based on the definitions established in chapter 1 and the argument propounded by Warman (1993) that "...security relates not only to the protection of the system and the data being processed, but additionally to the well-being and continued profitability of the organisation" (p 71).

[3] Such a demarcation holds true in large organisations only.

[4] A typical example of such an environment is that of defence. Early development of various evaluation methods can indeed be traced to the DoD initiatives in the US.

[5] Recent research has shown that formal methods offer a way of specifying information technology security standards in a more rigorous way than natural language. It has also been observed that Raise Specification Language (RSV) is more versatile than other traditional approaches such as Z and VDM (for details see Harry, A. *Z and RAISE: a case study and comparison*. National Physical Laboratory, UK).

[6] The system design initiatives reflect a marked tendency towards creating 'self-regulating systems'. Such approaches are grounded in the belief that self-controlling forms of behaviour emerge, if interlocking, causal goal-seeking activities are either established or identified. These ideas form the basis of cybernetics – a branch of systems theory.

[7] Baskerville (1988), for example, emphasises the importance of instituting controls in the logical design phase of conventional structured systems analysis and design methods.

7 Conclusion

7.1 Recapitulating key ideas

This book has explored issues surrounding the management of information system security. Security has been viewed in terms of minimising risks arising because of inconsistent and incoherent behaviour with respect to the information handling activities of organisations. The purpose of this chapter is to bring together some key ideas and identify the contributions of this book. Concepts about the nature of information system security, the management of information system security and the crisis regarding the use of technology are presented.

7.1.1 The nature of information systems security

Information systems researchers and practitioners alike have always felt the need to minimise systemic risks arising out of the use of information technology. Research has identified the confidentiality, integrity and availability of information as vital concepts. However, in developing counter-measures to threats in these three areas the focus has been on questions such as computer viruses, hacking, system failures and access control. Thus the primary concern has been for the technical installations and their functionality. In contrast research presented in this book has considered information technology usage in terms of integrity and wholeness of systems, social as well as technical. It has related the management of information system security to the deep-seated pragmatic aspects of an organisation. The implicit argument is concerned with maintaining the integrity of the business operations and the information systems.

The purpose of the concepts presented in this book is not to propose another classification of information technology related risks such that problematic situations could be mapped on to it. In fact the argument presented in this work has broadened the scope of information system security management. The key concern has been the notion of maintaining information systems integrity. It is important to maintain the wholeness of systems because organisations depend so heavily upon information for their success. The availability of information not only helps an organisation to co-ordinate and control its internal and external relationships, but also influences the effectiveness of an enterprise. Therefore any disruption in the information and communication systems or in the organisational operations has a detrimental effect on the entirety of the concern and the systems that support it (see for example Dhillon and Backhouse 1996; Angell 1993).

In order to maintain the integrity of the organisations and prevent the occurrence of any adverse events, research presented in this book has stressed the importance of having a clearer understanding about the nature of organisations. This would result in not only the successful development and implementation of information systems, but also in minimising risks associated with information technology usage. Other research findings support the same viewpoint (see for example Holmes and Poulymenakou 1995; Dhillon 1995; Griffiths and Willcocks 1994; Willcocks and Margetts 1994; Bentley 1991). Figure 7.1 illustrates the conception of organisations and the related security measures.

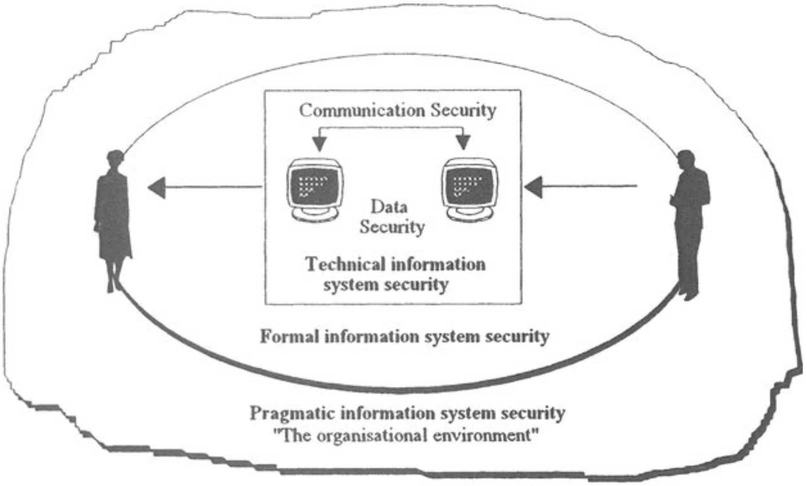

Communication Security
Data Security
Technical information system security
Formal information system security
Pragmatic information system security
"The organisational environment"

Figure 7.1 Conceptualising information system security

The literature review on security and the empirical research presented in chapters 4 and 5 identified the existing emphasis of researchers and practitioners to be skewed towards technical information system security measures. Although it is important to maintain the security of the technical edifice, it is not enough. Many forward looking organisations have recognised the shortcomings of having a narrow conception of their security strategies. Typical examples are found in the case of Shell[1] and British Petroleum[2]. Both organisations have recognised people to be a main component in developing secure environments.

Increased technical orientation has resulted in organisations ignoring the importance of formal rules and procedures in developing secure environments. Often, the simple manual checks and balances are either not implemented or are just ignored. The demise of the Barings Bank is another case in point. While the auditors recognised the failings in the dealings, the management preferred to ignore them. It should also be recognised that any number of good technical controls and formal procedures does not necessarily result in a secure environment (for details see Backhouse 1995). In any organisation, over a period of time a system of fairly cohesive groups with overlapping memberships is created. These social groupings of the informal system have a significant bearing on the well being of an organisation. The groups or even individuals may have significant power and may be in a position to influence other informal groups or even the formal structures. Thus when information technology is used to manage large organisations, a proper balance is needed between the three sub-systems. Failure to achieve such a balance generates uncertainty, creates complexity and introduces unnecessary risks, thereby increasing the probability of occurrence of adverse events.

7.1.2 Managing information system security

The field of information system security is relatively immature as compared to advances in information systems. It is important that information system security researchers and practitioners alike are able to examine critically their approaches, methods, tools and techniques by drawing on the research carried out in information systems. Moreover, it is important to understand the philosophical underpinnings of the approaches, thereby allowing an evaluation of the relative merits and demerits of the methods. Research presented in this book has demonstrated that along with understanding the nature of information system security, it is important to evaluate the socio-philosophical orientation of the approaches used. Investigation into the ontological and epistemological orientation of most information system security approaches showed a highly functionalist orientation (see chapters 2 and 3). The interplay between a functionalist mindset and a narrow conception about the nature of information system security has forced researchers and practitioners alike to be locked in an orthodoxy. Liebenau and Backhouse (1989) attribute reasons to "casual borrowings, cavalier attitudes and amateurish eclecticism, resting on the solid but inappropriate foundation of computer science". While exploring notions of ideology and information systems, Straub (1991) has also made criticisms to the same effect.

This book has introduced an alternative means for evaluating and managing information system security. The focus is on understanding the nature of the problem domain rather than criticising the current approaches. In that sense, this book lays a theoretical foundation for the management of information system security that is rooted in the interpretive paradigm as defined by Burrell and Morgan (1979). It is important that approaches are based on a systematic and a coherent perspective advocated by a paradigm. This avoids the theory building process from being based on the tenets of other theoretical approaches, thus preventing bias and eluding criticisms and counter-criticisms. Giving due consideration to these aspects, this book has proposed an interpretive approach for understanding information system security.

The use of an interpretive approach in this work has aligned the analysis of information system security with the mainstream information systems literature. In recent years there have been a significant number of studies, covering a range of topics and issues, that have used an interpretive approach (for example see Walsham 1993; Orlikowski 1991; Zuboff 1988; Suchman 1987). However, the information system security researchers have lagged behind in recognising the social nature of the security problems. This leaves a gap in the literature where research presented in this book has contributed.

7.1.3 The technological crisis

This book has highlighted the importance of understanding the deep-seated pragmatic aspects of organisations for preventing the occurrence of negative events. As a consequence an important issue regarding the use of technology has been touched upon. It is true that the application of technology has helped to improve the performance of businesses and even greater investments have promised increased benefits[3]. However, at a time when technology itself enters all aspects of our everyday lives, and becomes more accessible by almost anyone, it also becomes easier to abuse or misuse it. The case studies in chapters 4 and 5 have shown that even though technology may be used with all good intentions, an inappropriate use may result in increased risks. Such observations have been made in other studies as well. Georgiadou (1994), for example shows how fraud may actually emerge from the very application of technology.

If the application of technology into an organisational setting is not planned properly, the occurrence of any unforeseen phenomena or negative event cannot be ruled out. This is largely because of the complexity caused by technology in a social system. Such complexities are not restricted to information technology alone. In fact the emergence of a technological crisis can be traced back to the industrial revolution. Beniger (1986) links the effects on today's society to the increase in the speed of material processing and flows in the late nineteenth century. The speed and volume of this processing threatened the capacity of technology to control it. Today the speed of processing occasioned by information and communication technologies has resulted in organisations becoming highly susceptible to misuse. Increased organisational vulnerabilities have come into being because of commercial and social pressures, cultural incompatibilities, chaotic changes, resistance to change, criminal intent, malice and sabotage (see for example Angell 1995).

7.2 Critique of concepts

The purpose of this section is to examine critically the concepts presented in this book. This helps us in identifying those areas that may require further clarification. Such a critique is presented under two broad headings: type of theory and methodological issues.

7.2.1 Type of theory

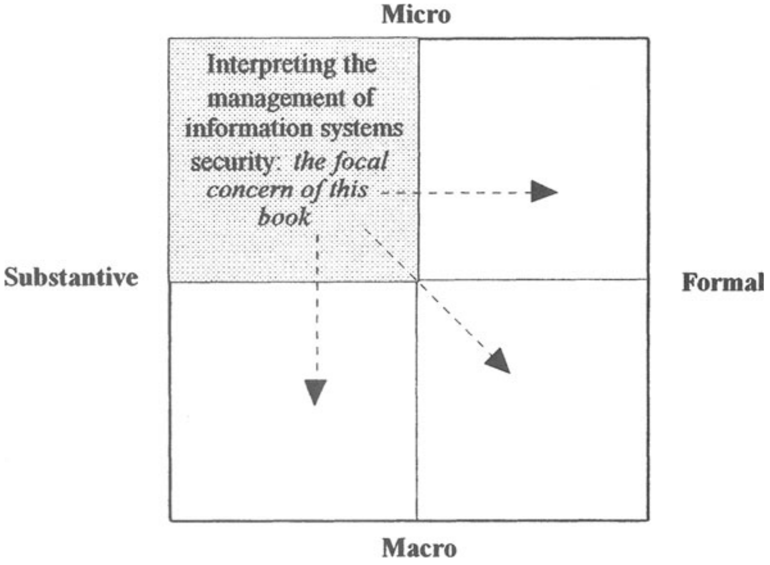
In sociology there is a well established, though by no means clearly expressed, macro-micro distinction in the level of analysis (see Ritzer 1992). The macro-micro categorisation relates to the variation of scope of cases under study. A 'macro' analysis refers to theories that are applicable to large scale social systems and relationships. The implicit assumption of such theories is to link different settings to one another and draw interpretations. A 'micro' analysis, by contrast, is concerned with an analysis of local forms of social organisation, being either particular enterprises or specific situations.

Cutting across the macro-micro dimension are the substantive-formal theories (as discussed by Glaser and Strauss 1967). The substantive-formal distinction concerns the generality of the categories with respect to the cases under investigation. Formal categories subsume substantive ones. For example, the study of information system security practices in a particular organisation can be used as a basis for a general theory about security.

The two dimensions provide a four-fold classification of theories. First are the macro-formal theories. These are concerned with the structure, functioning and development of societies. Angell's (1995) analysis of the impact of information technology on nation states falls in this category. Second, are the macro-substantive theories. Studies pertaining to particular industries fall in this category. Third are the micro-formal theories. These are concerned with more local forms of social organisation. Research done by Walsham (1993) is a typical example. Fourth are the micro-substantive theories. The focus of such research is on particular types of organisations or situations.

The research presented in this book falls into the micro-substantive category (figure 7.2). This is because the approach presented in this book has been to consider the deep-seated pragmatic aspects of organisations for managing information systems security. In the current form this work has looked at a particular set of organisations – those that can primarily be termed as public sector. However, it has not been possible to assess the implications of different contexts on the deep seated pragmatic aspects of organisations. Although the interpretations drawn in chapter 6 are fairly representative of organisations in a particular context, future work should broaden the scope to check the validity of the findings. There are several possible future research directions. These are illustrated in figure 7.2.

One possible future research direction is to develop a macro-substantive theory. Typically findings as presented in this book could be used to research into other public sector organisations. Conversely a more restrictive agenda could be pursued by just considering the Local Government or the National Health Service organisations. This would lead to the development of a micro-formal theory. Alternatively, future research could lead to a macro-formal theory for interpreting the management of information system security. This would involve extensive research, with case study organisations being sampled out from across the industry sectors.


Micro
Interpreting the management of information systems security: *the focal concern of this book*
Substantive
Formal
Macro

Arrows indicate future research directions

Figure 7.2 Types of theories and future research directions

7.2.2 Methodological issues

The methodological approach adopted in this book has been broadly interpretive. One of the major limitations of interpretive research is its reflexive nature. Researchers must recognise that they are part of the social world that they study. This is an existential fact. There is no way in which we can detach ourselves from the social world that we are studying. Often we rely on 'commonsense' knowledge to make judgements about the social phenomena under investigation. While conducting research for this book, many such judgements were made. Researchers grounded in the positivist traditions will perhaps consider this to be a limitation. However, experiences gained from research, as presented in this book, give us little justification for rejecting commonsense knowledge while conducting research. Researchers must proceed with their analysis and data gathering with what ever knowledge they have. In case there is any doubt with respect to problem situations, it is worthwhile subjecting the concepts to systematic inquiry.

Ideas propounded in semiotics have been used to conduct the case studies. In general the methodological approach provided a useful framework for analysis.

However, the use of semiotics and the staircase model in particular (figure 3.2) broadened the scope of the empirical work. As stated in chapter 3, semiotics is a mere regrouping of ideas from many disciplines. Each level of the framework has a number of theoretical models associated with it.

This book introduces the classification proposed by Hall (1959) to draw interpretations about the nature and significance of cultural aspects on information system security. However, such an analysis is by no means adequate and sufficient. Further research is needed across a broader spectrum of organisations to further investigate the relationship between culture and the management of information system security. Another area that has been touched upon, but needs further investigation is with respect to responsibility and blame. It is an emergent belief of this work that responsibility and the attribution of blame are strongly related to the management of information system security. The field of semantics offers a plethora of tools and techniques that can assist research in this direction (see Backhouse 1991). Recent research has in fact considered the use of speech act theory in explicating responsibility structures for secure systems development (Strens and Dobson 1993).

7.3 Epilogue

To summarise, this book presents insight into the following aspects of information system security:

- **Clarification of the concept:** This book clarifies concepts about the nature of information system security. Most of the literature on information system security has had a rather narrow technical perspective. Hence information systems security has been understood in terms of protecting the confidentiality, integrity and availability of information. This is fine in so far as the intention is to protect the technical edifice, but information systems are more than just computers – they are social systems. Hence with respect to information system security, our concern is to manage the integrity of the systems, formal and informal. This book broadens the definition of security and hence views it in terms of minimising risks arising because of inconsistent and incoherent behaviour with respect to the information handling activities of organisations.

- **Theory building and descriptive understanding:** Descriptive understanding is one of the main contributions of this book. The research presented takes the form of a systematic description of the properties and patterned relationships of the process of information technology adoption and the possible occurrence of negative events. This is a critical form of knowledge, essential for theory building in the field of information system security. Much has been written on the analysis, design and management of information systems and on the technical design of secure systems. The contribution of this work, beyond the previous literatures, is to bring together research in information systems and computer security and introduce an interpretive approach to the management of information system security.

- **Interpreting the deep-seated pragmatic aspects:** This book has argued that to solve the problem of managing information system security, we need to understand the deep seated pragmatic aspects of an organisation. The concepts of deep-seated pragmatic concept appears elusive and abstract to a novice. The book introduces an anthropological approach (E T Hall's culture map to analyse silent messages) to identify direct organisational interventions so as to assess implications for security. The interpretation gives a broad overview of the problem domain and hence helps an analyst to focus on specific issues of concern. However the analysis of silent messages is by no means a complete review of security.
- **Security review method:** Having developed conceptual clarity about the nature of information system security, this book presents a method for conducting a security review. The method is grounded in semiotics and identifies six levels of analysis. The security review approach is exemplified in the two case studies presented in this book. The process of analysis shows how the method can be applied in practice. The richness of the approach can be gauged from the breadth and depth of the analysis. The method helps to draw interpretations about the integrity of the organisation and the management systems in place.
- **Principles for managing information system security:** Based on the findings of the two case studies, a set of principles for managing information system security is established. These principles are intended to be 'first steps' in developing good management practices with respect to information system security. Careful consideration could serve as a catalyst for preventing the occurrence of negative events. The principles are organised under four major themes: planning and security policy; evaluation of security, design considerations for security; implementing information system security.
- **Practical relevance:** The concepts presented in this book are intended to be useful for various groups of practitioners engaged in the introduction computer based systems and management of security.

In general, what may be trivial in its self-evidence but profound in its truth is that the prevention of negative events is more effective than treatment. At an organisational level this can be achieved by developing good management practices. First steps in that direction emerge from understanding the deep-seated pragmatic aspects of an organisation and how these affect the occurrence of unforeseen events. At a social level, diffusion of ideas about security as part of the cultural infrastructure could reduce the burden placed on the shoulders of information systems managers in organisations. Many large organisations are engaging in awareness campaigns that seek to increase understanding of and sensitivity towards security issues among the broad base of their employees, rather than merely concentrate on those with responsibility for computer systems. There are initiatives being developed that target the school age population, seeking to educate youngsters in information system security as they learn about computing.

Ultimately the need is to have both a higher level of awareness among the workforce generally about the costs and benefits of good security, and a framework of computer law and enforcement and good management practice which will provide the necessary support where the more informal system of checks and balances fails.

[1] Based on the lecture given by David Lacey of Shell (UK) Ltd on 9th February, 1995 at the 1995 Security Colloquium, Computer Security Research Centre, London School of Economics. Title of the talk: IT security – developing baseline standards.

[2] The restructuring initiative at BP has particularly considered people to be a main component. This has specifically been done with respect to managing information system risks. Assessment is based on the MSc dissertation 'Role and effectiveness of information technology in networked organisations: a critical analysis' by S S Nair, Information Systems Department, London School of Economics, 1994.

[3] For instance, it is estimated that by implementing information and communication technologies, the British National Health Service could save £300 million per annum. Similarly, the UK Government's Central Unit on Purchasing could save £500 million per year on non-defence purchases.

Appendix E T Hall's Map of Culture

Description

Hall (1959) in his book *The Silent Language* introduces a taxonomy of different behavioural patterns. The framework helps in interpreting the cultural consequences of innovations that are likely to cause trouble if not perceived in time. Hall proposes ten streams of culture under which culture can be classified. These streams interact with each other to exhibit patterns of behaviour – the silent messages. Different combinations of the cultural stream relevant to information system security are shown in table A1, while a brief description of each stream is presented below.

Interaction: According to Hall, *interaction* has it basis in the underlying irritability of all living substance. One of the most highly elaborated forms of interaction is speech, which is reinforced by the tone, voice and gesture. *Interaction* lies at the hub of the 'universe of culture' and everything grows from it. A typical example in the domain of information systems can be drawn from the interaction between the information manager and the users. This interaction occurs both at the formal and informal levels – formally through the documentation of profiles and informally through pragmatic monitoring mechanisms.

Association: Hall uses the analogy of bodies of complex organisms as being societies of cells, in order to describe the concept of *association*. In this respect, *association* begins when two cells join. Kitiyadisai (1991) describes *association* in a business setting as one where an information manager acquires an important role of supplying relevant information and managing the information systems for the users. The prestige of the information systems group increases as their work gets recognised by the public. An association of this kind facilitates adaptive human behaviour.

Subsistence: *Subsistence* relates to the physical livelihood, eating, excretion, working for a living and income (indirectly). For example, when a company tells a new middle manager of his status, subsistence refers to access to management dining room and washing facilities, receipt of a fairly good salary, etc.

Bisexuality: This refers to differentiation of sexes, marriage and family. The concept of *Bisexuality* is exemplified in an organisation by the predominantly male middle management displaying machismo. Although *Bisexuality* is an important element in understanding aspects of a society, it has limited relevance to the study of information system security.

Territoriality (Location): *Territoriality* refers to division of space, where things go, where to do things and ownership. Space (or territoriality) meshes very subtly with the rest of the culture in many different ways. For example, status is indicated by the distance one sits from the head of the table on formal occasions.

Temporality (Time): Hall considers *temporality* to be intertwined with life in many different ways. The division of time, when to do things, sequence duration and space are typical examples. In a business setting examples of temporality can be found in flexible working hours, being 'on call', 'who waits for whom'.

Learning: Hall describes *learning* as: "one of the basic activities of life, and educators might have a better grasp of their art if they would take a leaf out of the book of the early pioneers in descriptive linguistics and learn about their subject by studying the acquired context in which other people learn" (p47). In an organisation management development programmes and short courses are typical examples.

Play: In the course of evolution, Hall considers *play* to be a recent and a not too well understood addition to living processes. *Play* and *defence* are often closely related since humour is often used to hide or protect vulnerabilities. In the western economies *play* is often associated with competition. *Play* seems to have a bearing on the security of the enterprise, however the nature and scope of the case studies presented in this book do not attempt to analyse this aspect in great detail. Hence it is excluded from the cultural streams as they appear in table A1 and in chapters 4 and 5.

Defence (Security): *Defence* is considered to be an extremely important element of any culture. Over the years people have elaborated their defence techniques with astounding ingenuity. Different organisational cultures treat defence principles in different ways which adversely affect the protective mechanisms in place. A good defence system would increase the probability of being informed of any new development and intelligence by the computer based systems of an organisation.

Exploitation: Hall draws an analogy with the living systems and points out that "in order to exploit the environment all organisms adapt their bodies to meet specialised environmental conditions". Similarly organisations need to adapt to the wider context in which they operate. Hence, companies that are able to use their tools, techniques, materials and skills better will be more successful in a competitive environment.

Table A1 - Part 1, Primary message systems (Only relevant streams are shown. Adapted from the original Map of Culture by Hall, 1959)

Primary Message Systems	**Interactional** **0**	**Organisational** **1**	**Economic** **2**	**Territorial** **4**
Interaction **0**	Communication patterns of individuals 00	Status and role within an organisation 01	Nature of economic exchanges 02	Location at which interaction takes place 04
Association **1**	Nature of the community formed because of interactions and associations 10	Issues pertaining to society; class; government etc. 11	What economic roles do different people have 12	The nature and significance of different roles in a localised environment 14
Subsistence **2**	Ideal manner in which different interactions take place 20	The nature of occupational groupings 21	Formal work relationships among individuals 22	Location of individuals with respect to subsistence 24
Location **4**	Territory established by communities 40	Territory established by groups 41	Economic areas established for business activities 42	Boundaries established by different groupings 44
Time **5**	Time periods established by communities for various activities 50	Time periods established by groups for various activities 51	Economic cycles 52	Cycles as a consequence of locational factors 54
Learning **6**	The community setting the context for the nature and scope of learning 60	Nature and scope of learning groups 61	Reward for teaching and learning 62	Places for learning 64
Security **8**	Security mechanisms put in place by the community 80	Security groups and police 81	Economic measures for protection 82	What places are defended 84
Exploitation **9**	Formal and informal networks in the community 90	Consortia and other corporate networks 91	Resources and equipment 92	Valuation of physical spaces 94

Table A.1 Parts 1 and 2 are adapted from *The Silent Language* by Edward T. Hall. Copyright © 1959, 1981 by Edward T. Hall. Used by permission of Doubleday, a division of Bantam Doubleday Dell Publishing Group, Inc.

Table A1 - Part 2, Primary message systems (Only relevant streams are shown. Adapted from the original Map of Culture by Hall, 1959)

Primary Message Systems	**Temporal** **5**	**Instructional** **6**	**Protective** **8**	**Exploitational** **9**
Interaction **0**	Time when interactions may take place 05	Manner in which teaching and learning is carried out 06	Nature and scope of protective mechanisms 08	Manner in which telephones etc. are used 09
Association **1**	Groups based on age, roles and positions within an organisation 15	Teachers and learners 16	Protectors (security personnel etc) 18	Use of group property 19
Subsistence **2**	Time when basic subsistence needs are fulfilled 25	Concurrence of learning and working 26	Individual physical care and protection of livelihood 28	Use of resources and equipment for subsistence 29
Locational **4**	Scheduling of space within an organisation 45	Specifying individual and group space allocations 46	Privacy 48	Use of fences and markers to define territory 49
Time **5**	Sequences and cycles 55	The time when an individual learns 56	Rest, vacation, holidays 58	Use of time-telling devices etc. 59
Learning **6**	Scheduling the time when group learning could be achieved 65	Education; informal learning 66	Learning how to defend one's ideas 68	Use of training aids 69
Security **8**	Timing of defence mechanisms 85	Security training 86	Formal and technical defence mechanisms 88	Use of artifacts for protection 89
Exploitation **9**	What periods are measured and recorded 95	Training aids etc. 96	The nature of safety devices 98	Types of material, systems and technology 99

References

1. Adam, N R and Wortmann, J C (1989). 'Security-control methods for statistical databases: a comparative study.' *ACM Computing Surveys* 21.

2. Advisory Committee for Coordination of Information systems (ACCIS) (1992). *Information systems security guidelines for the United Nations Organisations.* New York, NY: United Nations.

3. Aken, J E (1978). *On the control of complex industrial organisations.* Leiden: Nijhoff.

4. Albadvi, A and Backhouse, J (1995). 'Breaking the bottlenecks in dynamic systems development' *13th Annual International Conference, The Association of Management (Information Systems Group).* 2-5 August, Vancouver, British Columbia, Canada.

5. Alexander, J (1985). 'Neofunctionlism' . Beverly Hills: Sage Publications.

6. Alter, S (1992). 'Why persist with DSS when the real issue is improving decision making?' in Jelassi, T, Klein, M and Mayon-White, W (eds) *Decision support systems: experiences and expectations.* Amsterdam: Elsevier Science Publishers.

7. Ambaye, D and Hayman, A (1995). 'Causes of IT failure in teams' in Doukidis, G *et al.* (eds) *Third European Conference on Information Systems.* June 1-3, Athens, Greece.

8. Andersen, P B (1990). 'A semiotic approach to construction and assessment of computer systems' in Nissen, H-E, Klein, H K and Hirschheim, R (eds) *IFIP TC8/WG8.2 conference on Information Systems Research Arena of the 90's.* Copenhagen, Denmark: Elsevier Science Publishers.

9. Andersen, P B (1991). 'Computer semiotics'. *Scandinavian Journal of Information Systems* 3: 3-30.

10. Anderson, A M, Longley, D and Tickle, A B (1993). 'The risk data repository: a novel approach to security risk modelling' in Dougall, E G and Jones, D (eds) *Ninth IFIP International Symposium on Computer Security, IFIP/Sec '93.* Deerhurst, Ontario, Canada.

11. Andrews, K R (1987). *The concept of corporate strategy.* Homewood, Illinois: Irwin.

12. Angell, I O (1995). 'Winners and losers in the information age'. *LSE magazine* 7: 10-12.

13. Angell, I O (1993). 'Computer security in these uncertain times: the need for a new approach' *The tenth world conference on Computer Security, Audit and Control, COMPSEC*. London, UK: Elsevier Advanced Technology.

14. Angell, I O (1994). 'The impact of globalization on today's business, and why Information System Security is strategic' *The 1994 Annual Congress of the European Security Forum*. Hyatt Regency, Cologne, Oct 10th.

15. Angell, I O and Smithson, S (1991). *Information systems management*. London: Macmillan Press.

16. Ansoff, H I (1987). *Corporate strategy*. Harmondsworth, UK: Penguin Books.

17. Ansoff, H I (1991). *Strategic management in a historical perspective*. Chichester: John Wiley & Sons.

18. Ardis, P M and Comer, M J (1989). *Risk management. Computer, Fraud and Insurance*. Maidenhead: McGraw-Hill.

19. Audit Commission (1989). *Losing an empire, finding a role*. London: HMSO.

20. Audit Commission (1994). 'Opportunity makes a thief. Analysis of computer abuse'. The Audit Commission for Local Authorities and the National Health Service in England and Wales.

21. Austin, J L (1962). 'How to do things with words' in Urmson, J O and Sbisa, M (eds.) . Cambridge, MA: Harvard University Press.

22. Avgerou, C and Cornford, T (1993). *Developing information systems. Concepts, issues and practice*. London: Macmillan Press.

23. Avison, D and Wood-Harper, T (1991). 'Information systems development research: an exploration of ideas in practice'. *Computer Journal* 34: 98-112.

24. Avison, D and Fitzgerald, G (1988). *Information systems development: methodologies, techniques and tools*. Oxford: Blackwell Scientific Publications.

25. Backhouse, J (1991). 'The use of semantic analysis in the development of information systems'. PhD Thesis, London School of Economics, University of London.

26. Backhouse, J (1995). 'Protecting corporate information assets' *Managing for fraud prevention*. The Dorchester, London, 7th March: The Royal Institute of International Affairs.

27. Backhouse, J and Dhillon, G (1995a). 'Electronic thesauruses for clinical terms: a methodological approach' in Doukidis, G *et al.* (eds) *Third European Conference on Information Systems*. June 1-3, Athens, Greece.

28. Backhouse, J and Dhillon, G (1995b). 'Managing computer crime: a research outlook'. *Computers & Security* 14: 645-651.

29. Backhouse, J and Dhillon, G (1996). 'Structures of responsibility and security of information systems'. *European Journal of Information Systems* 5: 2-9.

30. Backhouse, J, Liebenau, J and Land, F (1991). 'On the discipline of information systems'. *Journal of Information Systems* 1: 19-27.

31. Badenhorst, K and Eloff, J (1990). 'Computer security methodology: risk analysis and project definition'. *Computers and Security* 9: 339-346.

32. Baier, V E, March, J G and Saetren, H (1988). 'Implementation and ambiguity' in March, J G (ed.) *Decisions and organizations*. Oxford: Basil Blackwell.

33. Bailey, J and Pearson, S (1983). 'Development of a tool for measuring and analysing computer user satisfaction'. *Management Science* 29: 530-545.

34. Banville, C and Landry, M (1989). 'Can the field of MIS be disciplined?'. *Communications of the ACM* 32: 48-60.

35. Bardach, E (1977). *The implementation game*. Cambridge, Mass: MIT Press.

36. Baroudi, J J, Olson, M H and Ives, B (1986). 'An empirical study of the impact of user involvement on system usage and information satisfaction'. *Communications of the ACM* 29.

37. Barras, R and Swann, J (1985). *The adoption and impact of information technology in UK local government*. London: The Technology Change Centre.

38. Barrett, S M and Masters, R J (1985). 'Information systems for policy planning' in England, J *et al.* (eds) *Information systems for policy planning in local government*. Harlow: Longman.

39. Baskerville, R (1988). *Designing information systems security*. New York: John Wiley & Sons.

40. Baskerville, R (1989). 'Logical controls specification: an approach to information systems security' in Klein, H K and Kumar, K (eds) *Systems development for human progress*. Amsterdam: Elsevier Science Publishers.

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

42. Baskerville, R (1993). 'Information systems security design methods: implications for information systems development'. *ACM Computing Surveys* 25: 375-414.

43. Beck, U (1992). *Risk society*. London: Sage Publications.

44. Bell, D and La Padula (1976). *Secure computer Systems: unified exposition and multics interpretation*. Bedford: MITRE Corp.

45. Benbasat, I, *et al.* (1984). 'A critique of the stage hypothesis: theory and empirical evidence'. *Communications of the ACM*: 467-485.

46. Beniger, J R (1986). *The control revolution: technological and economic origins of the information society*. Massachusetts: Harvard University Press.

47. Benjamin, R I, *et al.* (1984). 'Information technology: a strategic opportunity'. *Sloan Management Review*.

48. Bentley, D (1991). 'Managing risk in IT projects'. Cranfield School of Management.

49. Bequai, A (1987). *Technocrimes-the computerisation of crime and terrorism*. Mass.: Lexington Books.

50. Birch, D and McEvoy, N (1992). 'Risk analysis for information systems.' *Journal of Information Systems.*: 44-53.

51. Bloomfield, B and Coombs, R (1992). 'Information technology, control and power: the centralisation and decentralisation debate revisited'. *Journal of Management Studies* 29: 459-484.

52. Blumer, H (1969). *Symbolic interactionism: perspective and method.*

53. Boehm, B (1976). 'Software engineering'. *IEEE Transactions on Software Engineering.*

54. Boland, R J (1986). 'Fantasies of information'. *Advances in Public Interest Accounting*: 49-65.

55. Boland, R J and Day, W F (1989). 'The experience of system design: a hermeneutic of organisational action'. *Scandinavian Journal of Management* 5: 87-104.

56. Boland, R J (1985). 'Phenomenology: a preferred approach to research on information systems' in Mumford, E *et al.* (eds) *Research methods in information systems*. Amsterdam: Elsevier Science Publishers.

57. Boockholdt, J L (1987). 'Security and integrity controls for microcomputers: a summary analysis'. *Information & Management* 13: 33-41.

58. Boynton, A C and Zmud, R W (1987). 'Information technology planning in the 1990's: directions for practice and research'. *MIS Quarterly* 11: 59-71.

59. Brooke, R (1989). 'The enabling authority – practical consequences'. *Local Government Studies* 15: 55-63.

60. Brown, R K (1991). 'Security overview and threat'. National Computer Security Educators, Information Resource Management College, National Defence University.

61. Browne, P (1979). *Security: checklist for computer center self audits*. Arlington, Va.: AFIPS Press.

62. Brunsson, N (1990). 'Deciding for responsibility and legitimation: alternative interpretations for organisational decision making'. *Accounting, Organisations and Society*: 47-59.

63. Buchanan, J and Linowes, R (1980). 'Understanding distributed data processing'. *Harvard Business Review*: 143-153.

64. Burrell, G and Morgan, G (1979). *Sociological paradigms and organisational analysis*. London: Heinemann.

65. CCTA (1991). 'SSADM-CRAMM subject guide for SSADM version 3 and CRAMM version 2'. Central Computer and Telecommunications Agency, IT Security and Privacy Group,.

66. Charles, E C, Diodati, D A and Mozdzierz, W J (1993). 'Trusted systems: applying the theory in a commercial firm' *16th National Computer Security Conference*. Sept 20-23, Baltimore, Maryland, USA: National Institute of Standards and Technology/National Computer Security Center, USA.

67. Checkland, P B (1981). *Systems thinking, systems practice*. Chichester: John Wiley & Sons.

68. Chokhani, S (1992). 'Trusted Products Evaluation'. *Communications of ACM* 35: 66-76.

69. Chua, W (1986). 'Radical developments in accounting thought'. *Accounting Review* 61: 601-632.

70. Ciborra, C (1991). 'From thinking to tinkering: the grass roots of strategic information systems' *Twelfth International Conference on Information systems*. New York.

71. Ciborra, C (1994). 'The grass roots of IT and strategy' in Ciborra, C and Jelassi, T (eds.) *Strategic information systems. A European perspective*. Chichester: Wiley.

72. Ciborra, C (1987). 'Research agenda for a transaction cost approach to information systems' in Boland, R J and Hirschheim, R A (eds) *Critical issues in information systems research*. Chichester: John Wiley & Sons.

73. Clements, D P (1977). 'Fuzzy ratings for computer security evaluation'. PhD Thesis, University of California, Berkeley.

74. Clemons, E and Row, M (1988). 'A strategic information systems: McKesson drug company's ECONOMOST'. *Planning Review* 16: 14-19.

75. Clemons, E and Row, M (1991). 'McKesson Drug Company: a case of ECONOMOST, a strategic information system'. *Journal of Management Information Systems* 5: 36-50.

76. Cochrane, A (1993). *Whatever happened to Local Government?* Buckingham: Open University Press.

77. Computer Security Consultants (1988). *Using decision analysis to estimate computer security risk.* Ridgefield, Conn: Computer Security Consultants.

78. Computing (1992). 'MP prescribes NHS IT audit'. *Computing, 19 November.*

79. Confederation Of British Industry (1983). *Working for customers.* London: HMSO.

80. Cooke, B (1992). 'Quality, culture and local government' in Sanderson, I (ed.) *Management of quality in local government*. Harlow: Longman.

81. Coombs, R and Cooper, D (1992). *Accounting for patients?: information technology and implementation of the NHS white paper.* Milton Keynes, UK: Open University Press.

82. Courtney, R (1977). 'Security risk analysis in electronic data processing' *AFIPS Conference Proceedings NCC*: AFIPS Press.

83. Cummings, L L and ElSalmi (1968). 'Empirical research on the bases and correlates of managerial motivation: a review of the literature'. *Psychological Bulletin*: 127-144.

84. Currie, W L (1989). 'The art of justifying new technology to top management'. *Omega* 17: 409-418.

85. Davis, G B and Olson, M H (1984). *Management information systems: conceptual foundations, structures and development.* New York: McGraw-Hill.

86. DeMarco, T (1978). *Structured analysis and system specification.* New York: Yourdon Press.

87. Denning, D (1987). 'An Intrusion-Detection Model'. *IEEE Transactions on Software Engineering* SE-13 February: 222-232.

88. Dent, M (1992). *Modes of innovation in management information systems.* Milton Keynes, UK: Open University Press.

89. Dhillon, G (1994). 'Issues in management and control of computer crime' *Twelfth international symposium on economic crime.* Jesus College, Cambridge, UK.

90. Dhillon, G (1995). 'Complex managerial situations and the development of computer-based information systems' *BIT '95.* Manchester Metropolitan University.

91. Dhillon, G and Backhouse, J (1994). 'Responsibility analysis: a basis for understanding complex managerial situations' *1994 International System Dynamics Conference.* 11-15 July, University of Stirling, Scotland.

92. Dhillon, G and Backhouse, J (1996). 'Risks in the use of information technology within organisations'. *International Journal of Information Management* 16: 65-74.

93. Dietz, J L G (1992). 'Subject-oriented modelling of open active systems' in Falkenberg, E D *et al.* (eds) *Information system concepts: improving the understanding, IFIP TC8/WG 8.1.* Alexandria, Egypt, 13-15 April, 1992: Elsevier Science Publishers.

94. Dobson, J (1991). 'A methodology for analysing human and computer-related issues in secure systems' in Dittrich, K, Rautakivi, S and Saari, J (eds.) *Computer security and information integrity.* Amsterdam: Elsevier Science Publishers.

95. Dobson, J E, et al. (1991). 'Determining requirements for CSCW: the ORDIT approach' in Stamper, R K *et al.* (eds) *Collaborative work, social communications and information systems.* Amsterdam: Elsevier Science Publishers.

96. Donnellon, A, Gray, B and Bougon, M G (1986). 'Communication, meaning, and organised action'. *Administrative Science Quarterly* 31: 43-55.

97. Dorey, P (1991). 'Security management and policy' in Caelli, W, Longley, D and Shain, M (eds) *Information security handbook*. New York: Stockton Press.

98. Dubin, R (1969). *Theory building*. New York: The Free Press.

99. Dynes, M (1994). 'DSS accused of paying £500m benefits in error'. *The Times*, Oct 27, pp. 4.

100. Eco, U (1976). *A theory of semiotics*. Bloomington: University of Indiana Press.

101. Ehn, P (1988). *Work oriented design of computer artifacts*. Stockholm: Arbetslivs-centrum.

102. Farquhar, B (1991). 'One approach to risk assessment'. *Computer Security* 10: 21-23.

103. Fincham, R (1992). 'Perspectives on power: processual, institutional and 'internal' forms of organisational power'. *Journal of Management Studies* 29: 741-759.

104. Fisher, R (1984). *Information systems security*. Englewood Cliffs: Prentice all.

105. Forrester, J W (1994). 'System dynamics, systems thinking, and soft OR'. *System Dynamics Review* 10: 245-256.

106. Frye, N (1981). 'The bridge of language'. *Science*: 127-132.

107. Gable, G G (1994). 'Integrating case study and survey research methods: an example in information systems'. *European Journal of Information Systems* 3: 112-126.

108. Gable, G G and Highland, H J (1993). 'Information security in the small systems context: a framework for understanding' in Dougall, E G and Jones, D (eds) *Proceedings of the ninth IFIP International Symposium on Computer Security, IFIP/Sec '93*. Deerhurst, Ontario, Canada.

109. Gallegos, F, Richardson, D and Borthick, F (1987). *Audit and control of information systems*. Cincinnati: South-Western.

110. Galliers, R (1987). 'Information systems planning in a competitive strategy framework' in Griffiths, P (ed.) *Information management, state of the art report*. Maidenhead, Berks: Pergamon Infotech.

111. Galliers, R and Sutherland, A (1991). 'Information systems management and strategy formulation: 'the stages of growth' model revisited'. *Journal of Information Systems*: 89-114.

112. Galliers, R (1991). 'Choosing appropriate information systems research approaches: a revised taxonomy' in Nissen, H E, Klein, H K and

Hirschheim, R (eds) *Contemporary approaches and emergent traditions.* Amsterdam: Elsevier Science Publishers.

113. Galliers, R (1993). 'Research issues in information systems'. *Journal of Information Technology* 8: 92-98.

114. Galliers, R and Land, F F (1987). 'Choosing appropriate information systems research methodologies'. *Communications of the ACM* 30: 900-902.

115. Georgiadou, M (1994). 'Credit card fraud: a crisis of control in the credit system'. *Research and discussion paper CSRC/94/3, Computer Security Research Centre, London School of Economics.*

116. Giddens, A (1984). *The constitution of society.* Cambridge: Polity Press.

117. Glaser, B and Strauss, A (1967). *The discovery of grounded theory.* Chicago, Ill.: Aldine.

118. Griethuysen, V (1982). 'Concepts and terminology of the conceptual schema and the information base' : ISO Report No ISO TC97 SC5 N695.

119. Griffiths, C and Willcocks, L (1994). 'Are major information technology projects worth the risk?'. Oxford Institute of Information Management/IC-Park, Imperial College.

120. Gutting, G (1980). 'Paradigms and revolutions' . South Bend: University of Notre Dame Press.

121. Habermas, J (1972). *Knowledge and human interests.* London: Heinemann.

122. Hall, E T (1959). *The silent language.* New York: Anchor Books.

123. Hammer, M and Champy, J (1993). *Reengineering the corporation: manifesto for a business revolution.* New York, NY: Harper Business Press.

124. Han, C K (1991). 'Information technology policies and government information systems: a multiple level perspective'. PhD Thesis, University of Cambridge.

125. Highland, H (1985). 'Microcomputer security: data protection techniques'. *Computers and Security* 4: 517-531.

126. Hirschheim, R A (1985). 'Information systems epistemology: a historical perspective' in Mumford, E *et al.* (eds) *Research methods in information systems.* Amsterdam: Elsevier Science Publishers.

127. Hirschheim, R and Klein, H K (1989). 'Four paradigms of information systems development'. *Communications of the ACM* 32: 1199-1215.

128. Hirschheim, R and Smithson, S (1988). 'A critical analysis of information systems evaluation' in Bjorn-Andersen, N and Davis, G B (eds) *IS assessment: issues and challenges*. Amsterdam: Elsevier Science Publishers.

129. Hitchings, J (1996). 'A practical solution to the complex human issues of information security design' in Katsikas, S K and Gritzalis, D (eds) *Information systems security: facing the information society of the 21st century*. London: Chapman & Hall.

130. Hoffman, J, Michelman, E and Clements, D (1978). 'SECURATE - Security evaluation and analysis using fuzzy metrics' *AFIPS National Conference Proceedings*.

131. Holmes, A and Poulymenakou, A (1995). 'Towards a conceptual framework for investigating IS failure' in Doukidis, G *et al.* (eds) *Third European Conference on Information Systems*. June 1-3, Athens, Greece.

132. Hopper, M (1990). 'Rattling SABRE - new ways to compete on information'. *Harvard Business Review* 68: 118-125.

133. Hopper, T and Powell, A (1985). 'Making sense of research into the organisational and social aspects of management accounting: a review of its underlying assumptions'. *Journal of Management Studies* 22: 429-465.

134. Hoyt, D (1973). *Computer security handbook*. New York: Macmillan.

135. Hsiao, D, Kerr, D and Maduick, S (1979). *Computer security*. New York: Academic Press.

136. Huber, G P (1982). 'Organizational information systems: determinants of their performance and behavior'. *Management Science* 28: 567-577.

137. Hutt, A, Bosworth, S and Hoyt, D (1988). 'Computer security handbook' . New York: Macmillan.

138. IBM (1972). 'Secure automated facilities environment study 3, Part 2'. IBM, Armonk, NY.

139. Ives, B, Olson, M H and Baroudi, J J (1983). 'The measurement of user information satisfaction'. *Communications of the ACM*: 785-793.

140. Jamieson, R and Low, G (1990). 'Local area network operations: a security, control and audit perspective'. *Journal of Information Technology* 5: 63-72.

141. Jones, M and Walsham, G (1992). 'The limits of the knowable: organisational and design knowledge in systems development' in Kendall, K E, DeGross, J I and Lyytinen, K (eds) *The impact of computer supported techniques on information systems development*. Amsterdam: Elsevier Science Publishers.

142. Kailay, M and Jarratt, P (1994). 'RAMeX: a prototype expert system for computer security risk analysis and management' *Tenth IFIP International Symposium on Computer Security, IFIP Sec '94*. Curaçao (N.A.).

143. Keen, P G (1981). 'Information systems and organisational change'. *Communications of the ACM* 24: 24-33.

144. Ker, N (1994). 'Small is beautiful'. *The Computer Bulletin* 6: 5-6.

145. Kitiyadisai, K (1991). 'Relevance and information systems'. PhD Thesis, University of London.

146. Klein, H and Lyytinen, K (1985). 'The poverty of scientism in information systems' in Mumford, E *et al.* (eds) *Research methods in information systems*. Amsterdam: Elsevier Science Publishers.

147. Klein, H and Hirschheim, R (1987). 'Social change and the future of information systems development' in Boland Jr., R J and Hirschheim, R (eds.) *Critical issues in information systems research*: John Wiley & Sons Ltd.

148. Klein, R (1983). *The politics of the National Health Service*. London: Longman.

149. Kling, R (1980). 'Social analysis of computing: theoretical perspectives in recent empirical research'. *ACM Computing Surveys* 12: 61-110.

150. Kling, R (1987). 'Defining the boundaries of computing across complex organisations' in Boland, R J and Hirschheim, R A (eds.) *Critical issues in information systems research*. New York: John Wiley & Sons.

151. Kling, R (1991). 'Computerisation and social transformation'. *Science, Technology and Human Values* 16: 342-367.

152. Kling, R and Iacono, S (1989). 'The institutional character of computerised information systems'. *Office: Technology and people* 5: 7-28.

153. Kling, R and Scacchi, W (1982). 'The web of computing: computer technology as social organisation'. *Advances in Computers* 21: 1-90.

154. Kling, T (1978). 'Value conflicts and social choice in electronic funds transfer systems developments'. *Communications of the ACM* 21.

155. Knol, O M (1994). 'System dynamics concepts applied to the development and quality assurance of environmental information systems' *1994 International System Dynamics Conference*. 11-15 July, University of Stirling, Scotland.

156. Krauss, L (1972). *SAFE: Security audit and field evaluation for computer facilities and information systems*. New York: Amacon.

157. Krauss, L (1980). *SAFE: Security audit and field evaluation for computer facilities and information systems.* New York: Amacon.

158. Krueger, K H (1993). 'Internal controls by objectives: the functional control by objectives' in Dougall, E G and Jones, D (eds) *IFIP/Sec '93, Computer security: discovering tomorrow.* Deerhurst, Ontario, Canada.

159. Land, F (1990). 'Viewpoint: The government role in relation to information technology'. *International Journal of Information Management*: 5-13.

160. Land, F (1992). 'The information systems domain' in Galliers, R (ed.) *Information systems research: issues, methods and practical guidelines.* Oxford: Blackwell Scientific Publications.

161. Lane, D C (1994). 'With a little help from our friends: how system dynamics and soft OR can learn from each other'. *System Dynamics Review* 10: 101-134.

162. Lane, V P (1985). *Security of computer based information systems.* London: Macmillan Press.

163. Leavitt, H J (1964). 'Applied organisation change in industry: structural, technical and human approaches' in Cooper, W W, Leavitt, H J and Shelly, M W (eds) *New perspectives in organisation research.* New York: John Wiley.

164. Lee, A S (1991). 'Integrating positivist and interpretive approaches to organisational research'. *Organization Science* 2: 342-365.

165. Lehtinen, E and Lyytinen, K (1986). 'Action based model of information system'. *Information Systems* 11: 299-317.

166. Leifer, R, Lee, S and Durgee, J (1994). 'Deep structures: real information requirements determination'. *Information & Management* 27: 275-285.

167. Liebenau, J and Backhouse, J (1989). 'A need for discipline'. *The Times Higher Education Supplement*, March 31.

168. Lobel, J (1991). 'Proactive network risk management' in Dittrich, K, Rautakivi, S and Saari, J (eds) *Computer security and information integrity.* Amsterdam: Elsevier Science Publishers.

169. Loch, K D, Carr, H H and Warkentin, M E (1992). 'Threats to information systems: today's reality, yesterday's understanding'. *MIS Quarterly*: 173-186.

170. Longley, D (1991). 'Formal methods of secure systems' in Caelli, W, Longley, D and Shain, M (eds) *Information security handbook.* New York: Stockton Press.

171. Loveridge, R (1992). 'The future of health care delivery - markets or hierarchies?' in Loveridge, R and Starkey, K (eds) *Continuity and crisis in the NHS.* Milton Keynes, UK: Open University Press.

172. Lucas, H (1981). *Implementation: the key to successful information systems.* New York: Columbia University Press.

173. Lukes, S (1974). *Power: a radical view.* London: Macmillan.

174. Lyytinen, K and Hirschheim, R (1987). 'Information systems failures: a survey and classification of the empirical literature'. *Oxford Surveys in Information Technology* 4: 257-309.

175. Lyytinen, K and Hirschheim, R (1989). 'Information systems and emancipation. Promise or threat' in Klein, H K and Kumar, K (eds) *Systems development for human progress.* Amsterdam: Elsevier Science Publishers B.V.

176. Lyytinen, K (1985). 'Implications of theories of language for information systems'. *MIS Quarterly* 9: 61-74.

177. Lyytinen, K and Klein, H (1985). 'The critical theory of Jurgen Habermas as a basis for a theory of information systems' in Mumford, E *et al.* (eds) *Research methods in information systems.* Amsterdam: Elsevier Science Publishers.

178. Madon, S (1991). 'The impact of computer-based information systems on rural development: a case study in India'. PhD Thesis, University of London.

179. Madon, S (1992). 'Computer-based information systems for development planning: the significance of cultural factors'. *Journal of Strategic Information Systems* 1: 250-257.

180. Manning, P (1992). *Organizational communication.* New York: Aldine de Gruyter.

181. Manning, P and Cullum-Swan, B (1994). 'Narrative, content, and semiotic analysis' in Denzin, N K and Lincoln, Y S (eds) *Handbook of qualitative research.* Thousand Oaks: Sage Publications.

182. Marche, S (1991). 'On what a building might not be – a case study'. *International Journal of Information Management*: 55-66.

183. Markus, M L (1983). 'Power, politics and MIS implementation'. *Communications of the ACM* 26: 430-444.

184. Martin, J and Meyerson, D (1988). 'Organisational cultures and the denial, channelling and acknowledgement of ambiguity' in Pondy, L R, Boland, R J and Thomas, H (eds) *Managing ambiguity and change.* Chichester: John Wiley & Sons.

185. McCall, I and Cousins, J (1990). *Communication problem solving.* Chichester: John Wiley & Sons.

186. McFarlan, F, McKenney, J and Pyburn, P (1983). 'The information archipelago - plotting a course'. *Harvard Business Review* 83: 145-156.

187. McLeen, J (1990). 'Specification and modelling of computer security'. *Computer* 23: 9-16.

188. McMenamin, S and Palmer, J (1984). *Essential system analysis.* New York: Yourdon Press.

189. Melone, N P (1990). 'A theoretical assessment of the user-satisfaction construct in information systems research'. *Management Science* 36: 76-91.

190. Merten, A, *et al.* (1982). 'Putting information assets on a balance sheet'. *Risk Management.*

191. Miles, R (1993). 'MPs throw book at health chiefs over Wessex fiasco'. *Computing, 13 May*, pp. 7.

192. Mintzberg, H (1983a). *Power in and around organisations.* Englewood Cliffs: Prentice Hall.

193. Mintzberg, H (1983b). *Structures in fives: designing effective organisations.* Englewood Cliffs, NJ: Prentice Hall.

194. Mintzberg, H (1987). 'Crafting strategy'. *Harvard Business Review.*

195. Morris, C (1964). *Signification and significance – a study of the relation of signs and values.* Cambridge, Mass.: MIT Press.

196. Mumford, E and Weir, M (1979). *Computer systems in work design: the ETHICS method.* New York: John Wiley & Sons.

197. Murray, F (1989). 'The organisational politics of information technology: studies from the UK financial services industry'. *Technology Analysis and Strategic Management* 1: 285-298.

198. NHS Information Management Group (1987). *Guidance for information strategies.* London: HMSO.

199. NHS Information Management Group (1992a). *Basic information systems security.*

200. NHS Information Management Group (1992b). *IM&T strategy overview.* London: HMSO.

201. Nissen, H-E (1989). 'Information systems development for responsible human action' in Klein, H K and Kumar, K (eds) *Systems development for human progress.* Amsterdam: Elsevier Science Publishers B.V.

202. Nolan, R (1979). 'Managing the crises in data processing'. *Harvard Business Review* 57: 115-126.

203. Norman, A (1983). *Computer insecurity*. London: Chapman & Hall.

204. Office of Technology Assessment (1994). *Information security and privacy in network environments*: US Government Publication.

205. Olnes, J (1994). 'Development of security policies' *Tenth IFIP International Symposium on Computer Security, IFIP Sec '94*. Curaçao (N.A.).

206. Orlikowski, W J (1991). 'Integrated information environment or matrix of control? The contradictory implications of information technology'. *Accounting, Management and Information Technology* 1: 9-42.

207. Orlikowski, W J and Baroudi, J J (1991). 'Studying information technology in organisations: research approaches and assumptions'. *Information Systems Research* 2: 1-28.

208. Parker, D (1981). *Computer security management*. Reston: Reston Publishing.

209. Parker, D (1991). 'Seventeen information security myths debunked' in Dittrich, K, Rautakivi, S and Saari, J (eds) *Computer security and information integrity*. Amsterdam: Elsevier Science Publishers.

210. Parsons, G L (1983). 'Fitting information systems technology to the corporate needs: the linking strategy'. Harvard Business School.

211. Pettigrew, A M (1985). 'Contextualist research and the study of organisational change processes' in Mumford, E *et al.* (eds) *Research methods in information systems*. Amsterdam: Elsevier Science Publishers.

212. Pierce, C (1958). *Collected papers of Charles Sanders Pierce*. Cambridge, MA: Harvard University Press.

213. Polson, G (1995). 'Risk Analysis - a consultants perspective' *The 1995 Security Colloquium*. Computer Security Research Centre, London School of Economics and Political Science, London, January 26.

214. Porter, M (1980). *Competitive strategy*. New York: Free Press.

215. Porter, M and Millar, V (1985). 'How information gives you competitive advantage'. *Harvard Business Review* 63: 149-161.

216. Power, M (1994). *The audit explosion*. London: Demos.

217. Preston, A M (1991). 'The 'problem' in and of management information systems'. *Accounting, Management and Information Technologies* 1: 43-69.

218. Quinn, B (1980). *Strategies for change: logical incrementalism.* Homewood, USA: Irwin.

219. Rathswohl, E J (1990). 'Applying Don Idhe's phenomenology of instrumentation as a framework for designing research in information science' in Nissen, H-E, Klein, H K and Hirschheim, R (eds) *The information systems research arena of the 90's: challenges, perceptions and alternative approaches, IFIP 8.2.* Copenhagen, Denmark, Dec. 14-16.

220. Reason, P and Rowan, J (1981). *Human inquiry: a sourcebook of new paradigm research.* Chichester: Wiley.

221. Ritzer, G (1992). *Sociological theory.* New York: McGraw-Hill.

222. Roach, T W (1992). 'Effective systems development in complex organisations: a field study of systems development and use in the United States Army Medical Department (Army Medical Department)'. PhD Thesis, University of Texas at Austin.

223. Rockart, J F and Short, J E (1991). 'The networked organisation and the management of interdependence' in Scott-Morton, M (ed.) *The corporation of the 1990s.* New York: Oxford University Press.

224. Rule, J (1974). *Private lives and public surveillance.* New York: Schocken Books.

225. Saltmarsh, T and Browne, P (1983). 'Data processing – risk assessment' in Wofsey, M (ed.) *Advances in computer security management.* Chichester: John Wiley & Sons.

226. Sanderson, I (1992). 'Introduction: The context of quality in local government' in Sanderson, I (ed.) *Management of quality in local government.* Harlow: Longman.

227. Saussure, F d (1966). 'Course in general linguistics, (translated and edited)' in Baily, C et al (ed.) . New York: McGraw-Hill.

228. Scholz, C (1990). 'The symbolic value of computerized information systems' in Gagliardi, P (ed.) *Symbols and artificats: views of the corporate landscape.* Berlin: Walter de Gruyter.

229. Scrivens, E (1987). 'The information needs of district general managers in the English National Health Service'. *International Journal of Information Management*: 147-157.

230. Searle, J R (1969). *Speech Acts: an essay in the philosophy of language.* New York, NY: Cambridge University Press.

231. Solms, R, *et al.* (1994). 'A framework for information security evaluation'. *Information & Management* 26: 143-153.

232. Solms, R, Solms, S H and Carroll, J M (1993). 'A process approach to information security management' in Dougall, E G and Jones, D (eds) *Proceedings of the ninth IFIP International Symposium on Computer Security, IFIP/Sec '93*. Deerhurst, Ontario, Canada.

233. Sprague, R H and McNurlin, B C (1986). *Information systems management in practice*. Englewood Cliffs: Prentice Hall.

234. Stamper, R (1973). *Information in business and administrative systems*. New York: John Wiley & Sons.

235. Stamper, R (1985). 'Information: mystical fluid or a subject for scientific enquiry?'. *The Computer Journal* 28: 195-199.

236. Stamper, R, *et al.* (1988). *Semantic normal form?* London: ASLIB.

237. Stamper, R (1991). 'The semiotic framework for information systems research' in Nissen, H-E, Klein, H K and Hirschheim, R (eds) *IFIP TC8/WG8.2 conference on Information Systems Research Arena of the 90's*. Copenhagen, Denmark: Elsevier Science Publishers.

238. Strain, I (1991). 'Top bosses pose the main security threat'. *Computer Weekly*, October 3, pp. 22.

239. Straub, B H (1991). 'Ideology and information systems'. Unpublished PhD thesis, London School of Economics and Political Science, University of London.

240. Strens, R and Dobson, J (1993). 'How responsibility modelling leads to security requirements' *16th National Computer Security Conference, Sept 20-23*. Baltimore, Maryland: National Institute of Standards & Technology/National Computer Security Centre.

241. Strong, P and Robinson, J (1992). *The NHS – under new management*. Milton Keynes, UK: Open University Press.

242. Suchman, L (1987). *Plans and situated actions: the problem of human-machine communication*. Cambridge: Cambridge University Press.

243. Symons, V J (1991). 'A review of information systems evaluation: content, context and process'. *European Journal of Information Systems* 1: 205-212.

244. Taylor, F W (1911). *Principles of scientific management*. New York: Harper & Row.

245. Taylor, W (1988). 'Performance review is essential in today's world'. *Municipal Journal*: 2026-27.

246. Trubow, G B (1993). 'Protocols for the secondary use of personal information' *16th National Computer Security Conference, Sept 20-23*.

Baltimore, Maryland: National Institute of Standards & Technology/ National Computer Security Centre.

247. Turn, R (1982). 'Privacy protection in the 80s' *IEEE Symposium in Security and Privacy*. Silver Springs, MD: AFIPS Press.

248. US Department of Commerce (1979). 'Guideline for automatic data processing risk analysis'. US Department of Commerce, National Bureau of Standards, Washington, DC.

249. Veen, A M, *et al.* (1994). 'SMART: structured multi-dimensional approach to risk taking for operational information systems' *Tenth IFIP International Symposium on Computer Security, IFIP Sec '94*. Curaçao (N.A.).

250. Venkataraman, N and Short, J (1990). 'Strategies for electronic integration: from order entry to value added partnerships at Baxter'. *Sloan School Working Paper.*

251. Walsham, G (1993). *Interpreting information systems in organisations.* Chichester: John Wiley & Sons.

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

253. Wand, Y and Weber, R (1990). 'Toward a theory of deep structure of information systems' in DeGross, J I, Alavi, M and Oppelland, H (eds) *International Conference on Information Systems.* Copenhagen, Denmark: ACM.

254. Ward, J, Griffiths, P and Whitmore, P (1990). *Strategic planning for information systems.* Chichester: John Wiley & Sons.

255. Warman, A (1991). 'Organisational computer security policies'. *Research and discussion paper no. CSRC/93/3, Computer Security Research Centre, London School of Economics and Political Science, London, UK.*

256. Warman, A (1993). *Computer security within organisations.* London: Macmillan Press.

257. Watkins, S (1993). 'MPs push for IT check-up after health scandals'. *Computing, 18 February.*

258. Weber, M (1947). *The theory of social and economic organisation.* Glencoe, Ill: Free Press.

259. Weber, R (1988). *EDP Auditing: conceptual foundations and practice.* New York: McGraw-Hill.

260. Webler, T, Rakel, H and Ross, R J S (1992). 'A critical theoretic look at technical risk analysis'. *Industrial Crisis Quarterly* 6: 23-38.

261. Whipp, R and Pettigrew, A (1992). 'Managing change for competitive success: bridging the strategic and the operational'. *Industrial and Corporate Change* 1: 205-233.

262. Whynes, D K (1993). 'The NHS internal market: economic aspects of its medium-term development'. *International Journal of Health Planning and Management* 8: 107-122.

263. Willcocks, L and Margetts, H (1994). 'Risk assessment and information systems'. *European Journal of Information Systems* 3: 127-139.

264. Wing, J M (1990). 'A specifier's introduction to formal methods'. *Computer* 23: 8-24.

265. Wiseman, C (1985). *Strategic information systems*. Homewood: Irwin.

266. Wolstenholme, E F, Henderson, S and Gavine, A (1993). *The evaluation of management information systems*. Chichester: John Wiley & Sons.

267. Wong, K (1977). *Risk analysis and control*. Manchester: National Computing Centre.

268. Woodward, J (1965). *Industrial organisation: theory and practice*. London: Oxford University Press.

269. Wrapp, H E (1991). 'Good managers don't make policy decisions' in Mintzberg, H and Quinn, J B (eds) *The strategy process*. Englewood Cliffs: Prentice-Hall.

270. Wynne, B and Otway, H J (1982). *Information technology, power and managers*. Amsterdam: Elsevier Science Publishers.

271. Zuboff, S (1988). *In the age of the smart machine*. New York: Basic Books.

272. Zuurbier, J J (1992). 'On the design of group decision support systems.' in Jelassi, T, Klein, M R and Mayon-White, W M (eds) *Decision support systems: experiences and expectations*. Amsterdam: Elsevier Science Publishers.

273. Zyl, P W , Oliver, M S and Solms, S H (1994). 'MOSS II – a model for open system security' *Tenth IFIP International Symposium on Computer Security, IFIP Sec '94*. Curaçao (N.A.).

Index