Opportunities for Computer Abuse: Assessing a Crime Specific Approach in the Case of Barings Bank

Robert Andrew Willison
Department of Information Systems
London School of Economics and Political Science
Houghton Street, London WC2A 2AE, England

August 2002
Dissertation submitted in fulfilment of the requirements for
the award of the degree of Doctor of Philosophy in the faculty of
Economics at the University of London

I dedicate this thesis to my mother and father for their support, strength and encouragement.

Abstract

Within the field of IS security little has been written on the subject of criminal opportunity. More precisely, little has been written on what exactly constitutes an opportunity, and the relationship between employees, who may might act as potential offenders, and the IS context in which such opportunities may be afforded.

The purpose of this study is to assess the feasibility of a model known as the 'crime specific opportunity structure', which, as the name suggests maps out those elements which are thought to form an opportunity. Drawing on a number of criminological theories, the model considers the role of potential offenders in a work place setting by viewing them as rational decision-makers, who assess their environment, and possible opportunities, in cost-benefit terms. Furthermore, the model takes a crime-specific approach as each type of crime is made up of a unique mix of elements. Ignoring the idiosyncratic nature of specific crimes severely reduces an understanding of each type of crime, and further hinders effective prevention programmes. An ethnographic account of the collapse of a financial institution is used to assess the feasibility of the model.

Acknowledgements

Throughout my studies I have enjoyed the constant support and love of my family. Without their help, which came in many guises, I would not have been able to start, let alone finish, this research.

I am deeply indebted to my supervisor, Dr. James Backhouse, whose advice and encouragement, engendered the self-belief that sustained me throughout this research. Our many conversations have helped me to understand the complex issues that surround IS security, and inspired me to pursue an academic career. I am also extremely grateful to Derek Cornish, whose insights into criminology both stimulated and aided my studies.

Thanks are due to many members of the Department of Information Systems at the London School of Economics and Political Science, but in particular I should like to express my appreciation of the support and interest offered by Dr. Susan Scott, Dr. Carsten Sorensen and Dr. Edgar Whitley.

British Telecom provided much needed financial support in the early stages of my research, which I deeply appreciate. In this connection, I should like to thank Marek Rejman-Greene.

Finally, I should like to thank David Freestone, Riad Fawzi, Carol Hsu and Erica Wagner for their constant support and friendship.

Contents

List of Figures

Chapter One: Research Issues

The profile of information systems (IS) security in organisations has witnessed a shift over the last decade. Once considered a marginal function, many IS security officers now find themselves reporting directly to their CEO. This change is largely a consequence of the recognition by companies of their reliance on their IS, and the related recognition of information as the central resource for many organisations. Despite the general raised awareness of the importance of IS security, numerous organisations, for a number of reasons, fail to achieve effective control environments. As a consequence, such insecure environments may provide opportunities for criminal activity. The phenomenon of criminal opportunity is the focus of this research. This chapter commences with a discussion of the motivations and scope of the study, followed by a definition of what is understood in this research by the terms IS and IS security. The current state of IS security research into opportunity is then addressed with the penultimate section of the chapter examining the research objectives. The chapter concludes with an overview of the thesis's structure.

1.1 Motivations and Scope of the Research

The research stems from a general interest in criminology, and a more specific concern for activities which come under the umbrella term 'computer crime'. While there is an abundance of literature which addresses the threat posed by hackers (Taylor, 1999; Thomas, 2002), this study focuses on the internal threat of dishonest staff. In recent years organisations have become increasingly reliant on their IS, but such systems provide yet another means through which criminal actions can take place (Nosworthy, 2000, Von Solms, 2001). That said, organisations, albeit slowly, have come to realise the importance of securing their IS, particularly given the further realisation that information is now a central asset for many companies (Backhouse, 1997). Hence, there is now a burgeoning industry, offering advice and products for protecting organisational IS. Despite the increased recognition of the value of security, there are still many companies failing to implement and maintain the appropriate safeguards and procedures, which afford an effective control environment (Audit, 2001; CSI/FBI, 2002; Ernst & Young, 2002). In consequence those organisations with a flawed control environment may create opportunities for computer crime perpetrated by their own staff.

The concept of opportunity forms the focus of this research. More precisely it questions the very nature of this phenomenon. To this end the research assesses the feasibility of a model known as the 'Crime Specific Opportunity Structure'. Drawing on a number of criminological theories, the model is an attempt to provide a new perspective and original insights into the relatively unexplored area of opportunity.

To date the majority of IS security work has tended to focus on one aspect of the field, for example intrusion detection systems or biometrics (Barber, 2001; Harris and Yen, 2002). However, very few texts examine the interaction between these safeguards, because the majority of IS security writings have a technical orientation, and are unable to account for social aspects which form a key element in the interaction process (Dhillon, 1997; Dhillon and Backhouse, 2001). The current study, therefore, aims to explore the constituent elements that together, through deficient security, afford an opportunity in the organisational domain. Hence far from considering one aspect of security, this research is interested in examining how safeguards (including the role of people in this process) interact to form a coherent control environment. Research of this nature is important since organisations rely on input from a number of departments and functions (e.g. audit, personnel, IT) to create an effective control environment. A clearer understanding of the relationships between safeguards and the circumstances under which opportunities are afforded, would be of obvious interest to practitioners whose efforts are based on an inter-departmental approach.

As noted, the majority of writing in the IS security field focus on one form of safeguard, such as password systems (Peyravian and Zunic, 2000), viruses (Zenkin, 2001), public key infrastructures (Barber, 2000) and the like. The aim of these controls is to attempt to maintain the integrity of IS security. However, there is a paucity of texts which examine the actual individuals who are attempting to breach such security for whatever purpose. This would require the incorporation and adoption of theories and perspectives which afford consideration of the actions of individuals who perpetrate some form of computer abuse. This research is important for not only is it able to address the role of people in managing security, but central to the model assessed in this thesis, is a consideration of the 'potential offender'. Hence this research explores the actions and reasoning of these individuals in the workplace setting.

Given the technical orientation of most writings in the IS security field, it is perhaps no surprise to learn that very few texts in this domain examine what motivates individuals to perpetrate some form of computer crime (Willison, 2001). The current research, however, encompasses and examines such factors, while additionally considering those situations in which motivational factors can be negated.

1.2 Definition of IS and IS security

The research draws on the work of Liebenau and Backhouse (1990) for an understanding and definition of an IS. They divide an IS into three separate, but related elements, termed the technical, formal and informal. The technical element relates to those activities which have been formalised and programmed to run on computer systems. This is then supported by, and supports, the formal element of an IS characterised by bureaucracy and rules. Rules are used to control organisations by stipulating the business processes and procedures to be followed. The informal aspect of an information system can be characterised by the everyday behaviour of an organisation, or to use a more technical phrase, the cultural infrastructure of shared norms. It is within this domain that all rules and procedures are conveyed by actions. Hence this model departs from a conception of an IS solely in terms of the technical components, in other words computers and networks, and argues for an understanding of how these components operate in their social context (the informal), which is further influenced by the formal element. Consideration of how these elements interact is central to the model proposed by Liebenau and Backhouse.

The approach taken to IS security in this study further mirrors the holistic perspective afforded by the IFT model. Therefore, apart from acknowledging the need for technical controls, consideration must also be given to the informal and formal controls that together form a coherent and holistic understanding of IS security. Once again, an appreciation afforded by the IFT model of the interaction between the three elements is essential for a holistic understanding of IS security.

An example can perhaps best illustrate this interaction at work. Effective password systems require security measures to be working properly at the three levels. The technical element requires users to input their passwords for access to various computing resources, but this is not the whole story. Underpinning these actions should be a (formal) security policy, which prescribes the appropriate behaviour for staff with regard to using passwords. This normally encompasses instructions on how to formulate and safeguard personal passwords. However, security policies need to be enlivened through education and awareness programmes, which are designed to impact and influence the everyday behaviour of staff members with regard to security routines. In this sense education programmes can be considered as 'informal' measures.

The IFT perspective, through a consideration of how the three elements interact, allows for a clearer understanding of why password systems fail. More often than not, the reasons such systems fail is due not to a technical failure, but rather to problems of a formal and informal nature. Staff, for example, write their passwords down, leave them posted on their computers, and share them with colleagues. In these instances the question to be asked is whether staff are aware of their security responsibilities? Have they received training that informs them of procedures laid down in their organisation's security policy? Perhaps staff are aware of their responsibilities, but feel that the existing procedures restrict their ability to perform their work and hence ignore them. These security problems are not primarily technical in nature, but they do impact on this element of an IS to the extent that if formal and informal safeguards fail to be enforced, then dishonest staff may be able to discover the passwords of colleagues and circumvent the technical security.

1.3 Current Status of IS Security Research on Opportunity

The existing IS security writings on opportunity are addressed at length in the literature review chapter. However, for the sake of contextualising the current research, it is worth making the following points. Those IS security texts which directly address opportunity fall into one of two groups. There are those texts which address opportunities in terms of how they motivate criminal actions (Hitchings, 1995; Forester and Morrison, 1994; BloomBecker, 1984). The other group addresses how opportunities are created (Audit Commission, 2001; Stevenson, 2000; Comer, 1998). More specifically, this body of literature examines how opportunities are created through the absence, poor implementation and maintenance of safeguards.

While both these groups raise the spectre of how opportunities are a potential security problem, they fail to provide a definition of what exactly is understood by the term opportunity. Instead a common-sense understanding of this concept runs through the aforementioned literature. Hence an opportunity might be perceived as a computer left logged-on over lunch, when it should have been shut down, or a file left on a desk as a result of non-compliance with a clear desk policy. The major problem with the common-sense approach is that it cannot explain why some of these so-called opportunities are acted on in some instances and not in others. A suitable explanation requires an appreciation of other factors, most notably the role of the actor in explaining this variance.

Consistent with the approach to IS security advocated in the previous section, the Crime Specific Opportunity Structure allows for consideration of these 'other factors'. More specifically the model acknowledges the centrality of the agent by incorporating the role of the 'potential offender' as one of the factors involved in constituting an opportunity. To this extent the current research is interested in understanding the role of actors with regard to the formation of opportunities.

1.4 Objectives of the Research

The primary objective of this research is to assess the feasibility of the Crime Specific Opportunity Structure. As mentioned, this model draws on a number of criminological theories, and the importation of such theory into the field of IS security can be considered as an objective of this research in its own right. One deficiency of IS security generally is the lack of theory both used and advocated by researchers. The position taken in this study is that insight into computer criminals and their actions can be afforded through the application of criminological theory into the IS security domain.

As will be noted later in the thesis, the new perspectives and insights gleaned through the application of criminological theory in the IS security field has additional implications for practitioners. For not only can this body of theory provide a new understanding of existing and emerging problems, it can also be used to underpin security practices, which are often based on common-sense perceptions. Unfortunately, these perceptions often fail on closer scrutiny, hence practices based on rigorous theory can be seen as a progression for the IS security field.

A further objective is the advancement of the research strategy utilised in the study. While the approach taken can be identified as ethnographic, more specifically this study constructed an ethnographic account solely from secondary data sources. The approach taken can be seen as a pro-active solution to the challenge of gaining access to an organisation for the purpose of field research. Achieving access is problematic for most IS researchers, but this is especially the case with regard to those studying security. Companies are particularly sensitive about security issues and see those researching this area as a potential risk and hence access is frequently denied. However, inspired by developments in anthropology and ethnography which provide a body of literature supporting and therefore legitimating document-based ethnographies, the use of this approach in the current research can be seen as an attempt to advance this methodological practice in the IS field.

1.5 Thesis Structure

This thesis is divided into seven chapters. Chapter One begins with a description of the motivations and scope of the study, followed by definitions of what is understood in this research by the terms IS and IS security. The current status of IS security writings on opportunity is then briefly discussed with the objectives of the research forming the next section. The chapter concludes with a description of the thesis's structure.

The literature review forms Chapter Two. Those texts which directly address opportunity fall into one of two groups. First there are those writings which address how opportunities may criminally motivate individuals. The second group of texts focuses on how opportunities are created. After an examination of this literature the chapter moves on to highlight the existing deficiencies of the literature.

Chapter Three introduces the theoretical framework which is assessed in the thesis. The chapter begins with a discussion of a criminological school of thought known as Situational Crime Prevention (SCP). Central to this approach is the aim of reducing opportunities for crime. A number of like-minded criminological theories, which have proved influential in the development of SCP, are then described. These include the rational choice perspective, environmental criminology, routine activity theory and lifestyle theory. An attempt to synthesise these theories in the form of the 'Opportunity Structure for Crime' (Clarke, 1995) is described. The chapter then describes a number of changes made to this model, culminating in the 'Crime Specific Opportunity Structure', which forms the theoretical framework assessed in the study.

Chapter Four examines the research design. The chapter opens with a discussion of the philosophical assumptions which underpin the study, drawing on the interpretive and more precisely hermeneutic traditions. The reasons for these choices are examined, followed by a discussion of the study's research strategy, which can be categorised as ethnographic. Several key tenets which define this approach are described, followed by an examination of the existing IS ethnographic literature. The reasons for choosing this approach are discussed with a specific focus on why a document-based ethnographic approach was used. The final part of this chapter describes the data collection and analysis techniques.

The ethnographic account forms Chapter Five. This account focuses on the fall of Barings bank. The chapter commences with a brief history and background to the development of the bank, followed by a detailed description of those factors which were influential in bringing down the oldest privately owned merchant bank in the City's square mile.

The discussion and analysis section of the study forms Chapter Six. In this part of the thesis, the feasibility of a Crime Specific Opportunity Structure is assessed. Using the Barings case as a test bed, the chapter examines the extent to which the propositions and concepts inscribed in the model, hold theoretical water when applied to the ethnographic account. After this examination, the chapter moves on to address a series of related themes.

Chapter Seven opens with an overview of the thesis. This is then followed by a description of the theoretical, methodological and practical contributions of the study. The next section looks at the implications of the research approach, which encompasses research design limitations and the adequacy of the theoretical framework. The final part of this chapter discusses the options for further research in the area of opportunity.

Chapter Two: Literature Review

This chapter reviews the literature on opportunity. Of those texts which directly address opportunity, the literature divides into two distinct areas. The first group looks at how opportunities may act as a motivational factor with regard to individuals. The second attests to how opportunities are created through deficient security. A consistent message in the second group of texts is how opportunities arise through the absence, poor implementation and maintenance of safeguards. This literature is examined, focussing on issues such as the implementation of inappropriate safeguards, failure to monitor the efficacy of existing controls, and the need to address new and emerging risks. The chapter concludes with a discussion on the existing deficiencies with regard to the current literature on opportunity.

2.1 Opportunity as a Motivational Factor

Those texts that examine opportunity are few in number. This is probably due to the fact that the meaning of the term opportunity is regarded as obvious and hence there is little reason to examine the subject. However, there are some exceptions. A few writers have discussed opportunities in terms of the motivational impact they may have on individuals (Hitchings, 1995; Forester and Morrison, 1994; BloomBecker, 1984). In an early paper by BloomBecker (1984), for example, he cites eight types of motivational factors. One of these is 'the land of opportunity', where rogue employees exploit security loopholes spotted during the course of their daily work activities. Other writings in this vein, however, merely mention this phenomenon in passing (Hitchings, 1995; Forester and Morrison, 1994) as evidenced by Forester and Morrison who argue:

> Experts on computer fraud attest to the fact that opportunity more than anything else seems to generate this kind of behaviour.
> (Forester and Morrison, 1994, p. 41)

2.2 Opportunity Formation Through Deficient Security

Those remaining texts which explicitly discuss the subject matter focus on how opportunities are created through deficient security. With the aim of raising practitioners' awareness, the UK Audit Commission has been eager to spread the message regarding the relationship between poor security and opportunities. Its 1994 report, entitled *Opportunity Makes a Thief* (Audit Commission, 1994) indicates that one of the primary reasons for 'computer abuse' is a disregard for basic controls. More precisely this disregard manifests itself in a failure to implement and maintain such controls. These findings are mirrored in the Commission's *Ghost in the Machine* (Audit Commission, 1998) which cites 'little improvement' with regard to the provision of internal controls. Furthermore, this intransigence is reflected in the most recent report (Audit Commission, 2001) which states:

> Auditors and security specialists continue to stress the need for proper control and security measures. Nevertheless, the majority of breaches of IT security are still caused by a lack of the basic fundamental controls and safeguards.
> (Audit Commission, 2001, p. 17)

This assertion is supported by other writers in the field who have additionally and explicitly cited how poorly implemented and enforced controls might promote opportunities (Stevenson, 2000; Comer, 1988, Bologna, 1993). Indeed, both Comer (1998) and Bologna (1993) indicate how opportunities form one of the two key elements - the other being motivational factors - that must be addressed when combating computer fraud in organisations. But what exactly are those factors that lead to the absence, poor implementation and maintenance of safeguards? The chapter will now turn to address the literature in this area.

2.2.1 Organisational Complacency Towards IS Security

A primary reason for the absence of the appropriate safeguards is a complacency by many organisations with regard to IS security (Hinde, 2001; Audit Commission, 1998). As noted, this manifests itself in the failure of some organisations to implement even the most basic controls, leaving their IS vulnerable and possibly forming those conditions which represent opportunities. The last three UK Audit Commission reports clearly demonstrate this. A key control, for example is a security policy (Nosworthy, 2000; Osborne, 1998; Backhouse, 1997; Dorey, 1994). In 1994 and 1998, the respective reports indicated that one third of all surveyed organisations failed to implement this management tool. While this position improved by 2001, there remained almost one quarter of all organisations without this crucial safeguard. Another key requisite is the need to educate staff as to their security responsibilities. In all three surveys only one third of all organisations provided any form of security awareness training. A final example refers to the need for organisations to screen potential employees in order to guard against rogue employees. In 1994 less than 5% of organisations performed any form of vetting. Four years later the figure had risen to 10%, but by 2001 an increase of only 1% of organisations surveyed admitted to carrying out recruitment checks.

There is further evidence that the absence of fundamental controls is particularly acute in smaller organisations. A recent DTI report (DTI, 2000) asserts that in organisations with 50 or more employees, the use of passwords is nearly universal. However, amongst firms with nine or less employees only 68% incorporated this safeguard. A similar story can be told with regard to virus protection. Of those organisations which employed between 10-49 staff, 12% had no virus protection. This figure rose to 32% for those companies employing nine or less. On a relative scale, many large organisations could equally be charged with complacency. In a recent KPMG survey (KPMG, 2000) one hundred and seventy nine organisations with a turnover of more than £10 million were interviewed. Perhaps surprisingly, many of the organisations did not have a full time information security officer, and despite the fact that 98% used the Internet for business purposes, almost one third had no firewall protection. Furthermore, only 45% viewed security important enough to warrant ultimate responsibility for the function to be resting at board level.

One of the reasons for organisational complacency towards IS security may well be the inability of organisations to appreciate the value of their information assets, and the subsequent need to protect them. The aforementioned DTI report collated data from a fully representative sample of 1000 UK organisations. Surprisingly, of these 1000, 31% believed that they did not possess any information that they perceived as 'sensitive' or 'critical' in nature. Of this figure, 7% rather alarmingly related to organisations with over 500 or more employees. In America there is some evidence to suggest that larger organisations are increasingly aware of the value of their information. The latest CSI/FBI computer security survey (CSI/FBI, 2002) reports that in 1997 20% of respondents were victims of proprietary information theft. These figures are matched in the 2002 findings. Although the percentage of respondents who have been victims of proprietary data theft has remained fairly constant over the years between 1997-2002, this is not the case with regard to the figures representing the associated losses. In 1997 21 respondents were able to quantify their losses. The sum total amounted to $20,048,000. Of this amount, the average loss was $954,666 with $10 million representing the highest single loss. The figures for 2002 represent considerable increases. For the twenty organisations who were able to place a figure on their losses, the sum total came to $170, 827,000. The average figure amounted to $6,571, 000 while the highest was reported as $50 million.

The CSI/FBI survey then asks why there are such significant increases, even though the percentage of respondents remained fairly constant? The report states:

> The obvious answer is that those seeking information are more effective, perhaps because of more sophisticated technologies and techniques, at taking more valuable information. But the steady rise can also be attributed to two additional factors that have been rising exponentially over the same years as the study:
>
> 1. Increased recognition that information has value.
> 2. Increase in perceived value of information.
>
> In other words, while organisations like the Society for Competitive Intelligence Professionals help gatherers hone information collection skills, and the Internet makes it easier for information thieves to gather information used to bait and lure targets, the targets feel the pain of the loss more now because of an increased awareness that information translates into market differentiation, competitive positioning and even top line 'revenues' (CSI/FBI, 2002, p. 7).

Of course it should be recognised that knowing how to value information assets is a major problem for organisations. Although companies increasingly attest to how information is their central asset, it is rarely listed in their respective balance sheets (Backhouse, 1997).

2.2.2 Erroneous Perceptions of IS Security Risks

While companies may fail to appreciate the value of their information assets, they may also fail to recognise their potential threats (Yapp, 2001; Riem, 2001; Wright, 2001; Hinde, 2001 Parker, 1997). A recent global security survey by Ernst & Young (2002) reveals:

> Yet again we see greater concern about vulnerability to external attack (57%), than internal (41%), and yet leading research groups continue to confirm that more than three quarters of attacks originate from within organisations ... an alarming amount of evidence remains that organisations are lacking fundamental management information about security breaches (Ernst & Young, 2002, pp. 8-9).

This is confirmed by Parker (1997) who argues that the 'distorted image' of security held by top-level business people is often 'informed' by trade publications such as the Wall Street Journal and Forbes. In a similar vein, the most recent CSI/FBI (2002) report indicates how the actions of defrauded organisations help to reinforce erroneous perceptions of threats held by management. Concerned with the consequences of bad publicity for their reputation, most victims of financial fraud are unwilling to involve law enforcement agencies, preferring to deal with the matter in house. As fraud cases are rarely reported in the business publications, such as those discussed by Parker (1997), managers subsequently fail to appreciate the gravity of the problem. Indeed, Parker argues that information security practitioners must first attempt to understand what perceptions are held by top managers and then proceed to correct any unfounded beliefs. One consequence of the inability of organisations to appreciate the actual risks to their IS is that measures may be implemented to address risks which in reality are relatively minor at the expense of those areas where the risks are high, but receive little attention.

2.2.3 Technical Perspective of IS Security

Additionally the 'distorted image' of security held by managers, is often equated with a myopic understanding of the problem area and how it should be addressed. Several writers have attested to how with many organisations IS security is often perceived as a purely technical concern (von Solms 2001; Osborne, 1998; Parker, 1997; Wood, 1995). The downside to this perspective is that it fails to view the whole of the problem domain, and hence further fails fully to appreciate all the elements that constitute such an environment.

In a similar vein, most writings in the IS security field fail to take an holistic approach owing to the fact that they are unable to account for social aspects which form a key part of the security domain. One explanation for this apparent inability is largely a consequence of how information systems have been conceptualised, and this has ramifications for what is considered IS security. This topic is discussed in a recent paper by Dhillon and Backhouse (2001), who use the paradigmatic framework devised by Burrell and Morgan (1979) to traverse the current body of information systems and security literature. They assert that with respect to the information systems literature, there is an increasing dissatisfaction with the 'formal, rational, and overly mechanical conception in the analysis and design of information systems' synonymous with functionalist thinking. Dhillon and Backhouse argue that this 'narrow and technical viewpoint' suited past situations where the computer services provision was used to undertake a single function and organisations were predominantly hierarchical. However, given the prevalence and devolution of computing power in the new networked organisations, there is an increasing recognition for addressing the social aspects that impact on the analysis, design and workings of information systems.

Writings on information systems security, have, however been slow to recognise this shift. Instead the majority are essentially technocratic in orientation. Early risk analysis and security evaluation approaches, followed by more recent evaluation and design methods, are founded on functionalist conceptions influenced traditionally by systems theory. These tools and techniques have a limited scope, primarily focusing on issues of managing access control. The Achilles' heel of these safeguards is their conception of reality. Given how much of the early work on security was developed by the US military, it is perhaps not surprising that these safeguards were based on and reflect the reality that exists in a military environment. Organisational structures which mimic this environment, that is which are hierarchical and with centralised information processing, may accommodate such tools and techniques. But Dhillon and Backhouse argue that with organisations taking on flatter structures and becoming more organism-like in nature, there is a pressing need to address the behaviour of people and social groupings.

Given the inability of the technical perspective to view the problem domain holistically, security efforts underpinned by such a perspective will equally fail to address the whole of the problem domain. As Wood (1995) states:

> No matter how sophisticated the information security technology, controls will not be sustainable unless the human element has been adequately addressed. Too many people look at information security as strictly a technological problem, when in reality it is both a technological and a human problem. For example, setting up a firewall alone does not guarantee that Internet access will then be secure. One must also address a host of related considerations such as policies, procedures, standards, and other management instructions (Wood, 1995, p. 667).

2.2.4 Funding of IS Security

The organisational security budget is closely related to management perceptions. Osborne (1998) argues that the technical perspective often leads to a poor return on investment owing to the inability of those responsible for security to understand and address the necessary and related managerial aspects of security (e.g. implementing a security policy), while concentrating too heavily on technical safeguards. Hence Osborne (1998) argues that those organisations which take a technical approach, while spending considerable funds on safeguards such as cryptographic systems and firewalls, may still incur security breaches owing to the failure of those organisations to understand and act on an holistic approach.

For an adequate level of organisational funding Wood (1997) argues that management need to have a clear understanding of the complexity of IS security. Once this is achieved, then there is a greater motivation for providing the necessary funds.

Whether or not this message is getting through to the relevant parties is debatable. In the UK a KPMG (2000) survey found that almost 50% of respondents viewed budget restraints as an obstacle to providing effective security. The latest CSI/FBI (2002) report states that in American organisations there is only one person per thousand to undertake security duties. In terms of financial outlay, no more than 5% of the IT budget is spent on security. Furthermore, the survey indicates that security is often the first port of call when project costs need to be reduced with regard to new networks, systems or applications. Although at the time it is believed that security can be added 'later', very often this is not the case.

2.2.5 Assessing Risks

As noted, a purely technical approach could lead to vulnerabilities and potential opportunities, through the inability of those responsible in an organisation to understand the problem domain, and in consequence implement safeguards based on misguided perceptions. The alternative as advocated by the British Standard BS 7799: Code of Practice for Information Security Management (BS7799, 1999) is to identify an organisation's security requirements in a methodical manner by using risk assessment techniques (Ciechanowicz, 1997; Lichtenstein, 1996). By doing so organisations are able to identify and prioritise risks to their assets. Once the associated risks have been identified, the appropriate safeguards can be implemented. The range and types of safeguards are extensive. The aforementioned standard, for example, highlights eleven areas for the consideration of safeguard implementation, which include:

Security policy;
Security organisation;
Asset classification and control;
Information classification;
Personnel security;
Physical and environmental security;
Communications and operations management;
Access control;
Systems development and maintenance;

Business continuity management;
Compliance.

These diverse aspects of IS security highlight the not inconsiderable task faced by companies in implementing the requisite controls. Failure to do so will leave an IS system vulnerable and could provide the opportunity for some form of computer abuse.

2.2.6 The Interrelated Nature of Security Controls

One problem that companies must address when safeguards are introduced is their interrelated nature. Security is very much like a house of cards: inadequate consideration for one area will impact on another, possible creating those conditions that help form an opportunity. Section three of BS7799, for example, addresses the role of an information security policy. Through the creation and maintenance of a security policy, management can provide support and direction for information security in an organisation. More specifically, the standard stipulates that a policy should incorporate the following key areas:

> 1. a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;
> 2. a statement of management intent, supporting the goals and principles of information security;
> 3. a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization;
> 4. a definition of general and specific responsibilities for information security management, including reporting security incidents;
> 5. references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.
>
> (BS 7799, 1999, p. 3)

There is no denying the importance of a security policy as a cornerstone in the development of an organisation's control environment (Nosworthy, 2000; Osborne, 1998; Backhouse, 1997; Dorey, 1994). However, unless the policy is brought to life through education and awareness programmes (section 6.2.1 of the standard), then all the work undertaken to create a policy will ultimately have been a waste of time (Nosworthy, 2000; Thompson and von Solms; 1998; Spurling, 1995).

In practical terms, failure to enlighten staff as to their responsibilities and related procedures will lead to non-compliance. If people fail to follow the required security procedures, then this too will leave the IS vulnerable and could well form the basis for an opportunity. It is important to bear in mind that the aforementioned example highlights just one of the interrelationships between controls. The eleven areas cited by BS 7799, and the numerous safeguards specified in each section, highlight the complexity of IS security and the need for consideration of all the elements that constitute this function.

2.2.7 Implementation of Inappropriate Controls

Even prudent companies, who wish to establish effective security across the board may unwittingly create the conditions which help to form opportunities through the implementation of inappropriate controls (Luzwick, 2001; Olnes, 1994; Warman, 1993). If the introduced safeguards provide a sub-standard level of security then the IS will be left vulnerable. However, the same is also true if the safeguards are perceived by staff as unworkable in the organisational context. One of the perennial problems for IS security is its uneasy relationship with business objectives. Although there is an obvious need to reduce the risks to an IS, the respective countermeasures are often seen by users as a constraint around the range of tasks required to fulfil the aforementioned objectives. If the safeguards are perceived to be too heavy-handed or impractical (or both), staff may circumvent the controls. Again, non-compliant behaviour would leave the IS vulnerable, possibly providing opportunities for rogue employees. Hence, in this sense, although safeguards are obviously introduced to reduce risks, they may in reality create them.

Evidence of this is provided by Adams and Sasse's (1999) research into the use of passwords by organisational staff. A web-based questionnaire and a series of semi-structured/in-depth interviews were used to elicit data from Organisation A (a technology company), Organisation B (a construction company) and other users in firms situated around the world. The research indicates that many of the problems arising between users and safeguards originated at the design phase. More specifically, there was a lack of consultation with the users regarding the design of password systems. As Adams and Sasse note:

> Insufficient communication with users produce a lack of user-centered design in security mechanisms. Many of these mechanisms create overheads for users, or require unworkable user behavior. It is therefore hardly surprising to find that many users try to circumvent such mechanisms (Adams and Sasse, 1999, p. 44).

Multiple passwords were found to be one of the key factors influencing competent password use. Through their everyday activities, many staff were required to remember a number of passwords for a number of different applications. The more passwords, the more difficult it was for each user to remember them correctly. This led to half the respondents admitting to writing them down.

The problem of multiple passwords was compounded for users due to 'change regimes', which as the name suggests, requires staff to create a new password on a regular basis. As a consequence, users often constructed passwords that they found easy to remember. While this suited their needs, the password content was often of an insecure nature. Other users found it difficult to recall their passwords given the change regimes. As a memory aid, however, some members of staff created security vulnerabilities by writing down their passwords:

> I cannot remember my password, I have to write it down, everyone knows it's on a post-it note in my drawer, so I might as well stick it on the screen and tell everyone who wants to know (Adams and Sasse, 1999, p. 43).

Apart from multiple passwords, the study found that measures designed to create secure password content, while achieving this goal, made it harder for users to remember their revised passwords. So for example, a user who creates a password on an alphanumeric design i.e. a mixture of words and numbers, will have a relatively secure password. Owing to the fact that passwords of this nature are harder to remember, users admitted to writing them down. Additionally, the study discovered that some users circumvented the measures designed to create secure password content. Although, these users could more easily remember their passwords, the passwords themselves were, as a consequence, of a less secure nature compared to those constructed along alphanumeric lines.

Adams and Sasse additionally point to the need for compatibility between password use and work practices. They found that in Organisation A staff viewed the use of individually owned passwords as incompatible with group work, preferring instead shared passwords. Staff members in Organisation B, however, vehemently rejected their departmental policy of group (shared) passwords for accessing applications containing personal information e.g. e-mail.

A further point relates to the users' knowledge of security issues, and illustrates, as discussed earlier, the interrelated nature of controls. Adams and Sasse refer to how many security functions in organisations work on the adopted military principle of *need-to-know*. This principle advocates that the more people know about a security mechanism, the easier it is for them to breach it. In organisations, this leads to users being told as little as possible about safeguards and how they work, as those responsible for the security function perceive users as 'inherently insecure'. However, Adams and Sasse argue that a major finding of their study is that users who are under-informed about the password systems behave in an 'insecure manner'. They cite how organisations A and B introduced user-generated passwords, where previously system generated passwords were provided for the staff. Hence the onus and responsibility for creating secure passwords were placed with the users. Unfortunately, the study found that users were rarely educated in constructing secure passwords.

Apart from illustrating the interrelated nature of controls, the study additionally illustrates the social-technical nature of security. As noted, many of the issues raised in the password study concerned the interaction between the social and technical elements. Attempting to address password systems from a purely technical viewpoint would fail to view the whole of the problem domain, and would subsequently fail to provide any clear insight into how such systems could be improved.

2.2.8 Safeguard Implementation

Aside from the inappropriate nature of safeguards, a related issue concerns the implementation of controls. Failure to carry out this task effectively can negate any improvements in security for which a safeguard was designed to bring to its respective environment. Schneier (1998) discusses cryptographic systems as a case in point. He notes several problems pertaining to the poor implementation of this safeguard. With some systems, the plain text which the user wishes to encrypt is not destroyed after the process takes place. Other systems use temporary files on a computer in case of a systems crash. While this is prudent, if these systems are wrongly implemented, the plain text is left on the hard drive. Schneier further notes how some systems can even leave the cryptographic keys on the hard drive if poorly implemented. As illustrated the failure to adequately implement a safeguard can leave an IS vulnerable. Another example is provided by the latest CSI/FBI survey (2002) which cites the case of Adrian Lamo, who was able to hack into the *New York Times'* internal network, as a result of wrongly configured proxy-servers (firewalls):

> Once on the newspaper's network, Lamo exploited weaknesses in the Times' password policies to broaden his access, eventually browsing such disparate information as the names and Social Security numbers of the paper's employees, logs of home delivery customers' stop and start orders, instructions and computer dial-ups for stringers to file stories, lists of contacts used by the Metro and Business desks, and the 'Wire Watch' keywords particular reporters had selected for monitoring wire services (CSI/FBI, 2002, p. 5).

As previously stated, it is vital that organisations recognise the interrelated nature of controls. At the same time, they also need to recognise the interrelated nature of departmental security. Wood (1995) argues:

> One of the significant problems in the information security field involves the fragmented and inconsistent efforts. Too often one department will be supportive of information security efforts, while another department within the same organisation will be resistant. To the extent that these departments share resources – such as a local area network – the resistant department will jeopardise information security in the supportive department (Wood, 1995, p. 670).

2.2.9 Compliance Reviews

A key requisite of IS security is the need to confirm on a routine basis that the existing controls are working effectively. One of the consistent messages found in the UK Audit Commission (1994; 1998; 2001) reports is that many organisations are failing to check whether their controls are operating as intended. As a consequence those safeguards which are not fulfilling their tasks leave an IS vulnerable. Furthermore, these vulnerabilities may exist for considerable periods of time, given the negligence of some companies with regard to monitoring their controls. The reason for this neglect may be due to the perception held by some managers that IS security is a one time project with little need to consider the on-going nature of this function (Wood, 1997). The British Standard however advocates the need for compliance reviews at managerial and technical levels. With regard to the former, managers should consistently ensure that security procedures are working in their area of responsibility. Additionally BS7799 advocates that all sections of an organisation should be routinely reviewed to confirm that security practices are consistent with those prescribed in the security policy. One common problem in many organisations, which illustrates a failing in the management of IS security, relates to 'rights management' (*Computer Fraud & Security*, July 2001). More precisely, those responsible for IS security are often not informed when staff leave an organisation. As a consequence, the passwords and the associated accounts of the ex-employees fail to be disabled leaving on-line information vulnerable to these individuals. This problem is compounded by the fact that users generally have far more access to information than generally needed.

In terms of technical safeguards, both hardware and software, should be examined to ensure compliance to security implementation standards. It is worth noting the high maintenance nature of some technical controls. Virus software, for example, needs constantly updating. Failure to do so can leave an organisation extremely vulnerable. Software patches represent another sector of IS security in which constant vigilance is required. Unless those responsible for security are acutely aware of publicised flaws in software, and the associated patches that can be installed to rectify the problem, then once again an organisation's IS can be left vulnerable. The CSI/FBI 2002 survey highlights an example of the failure by a number of organisations to implement a patch for a web-site shopping cart software called 'PDG'. The flaw in the programme left exposed customer records on approximately 4000 web-sites. Despite the FBI issuing public warnings and providing details of where the patch could be downloaded to amend the problem, a number of organisations failed to take action. Two months after the initial warnings, the exploitation of the hole in the PDG software had become commonplace.

This example once again clearly demonstrates the need to understand IS security as a socio-technical problem. A clear explanation of why certain organisations fell victim to security breaches by hackers intent on stealing credit card details can only be provided by understanding IS security as a socio-technical phenomena. A purely technical perspective cannot account for why vulnerabilities existed on the victim organisations' web-sites, because it does not incorporate the social elements of security and how this interacts with the technical element. As noted, while the organisations' web-sites were breached owing to a flaw in the software, this flaw could have been eradicated, but due to inaction by many of those responsible for maintaining and enforcing security, it was not to be.

While advocating the need to review existing safeguards, BS7799 (1999) also advises organisations to address new and emerging risks to their IS. As explained, the standard asserts that organisations can identify their security requirements by using risk assessment techniques. By doing so companies can identify their risks and implement the requisite controls. However, just as organisations change in terms of business practices and resources, so too must the security function, for with change come new risks (Anderson, 1994).

From the mid 1950s to the early 70s security was a relatively simple affair. The focus of security efforts was the corporate mainframe. The model on which 'computer' security was based is known as the 'ring fence' approach. There are essentially three 'fences' to the model. The first consists of a physical barrier. The mainframes were located in secure, air-conditioned rooms to protect against not only unwarranted human entry but also humidity, dust and extreme temperatures. The second fence consists of a logical barrier. For users to gain access to the computing resource (via dumb terminals which had no processing power of their own) they were required to 'identify' themselves. This was achieved via a password system. The final barrier consists of personnel controls. Prior to an offer of employment, prospective staff were screened to ensure some degree of honesty. This method for securing computer facilities was extremely common, and suited the centralised mainframe facilities, cared for by the data processing department.

Given the centralisation of computing power, the major threat (aside from acts of God such as fire floods and earthquakes) came from those members of staff who had some access, either directly or indirectly, to the mainframe (Parker, 1976). This, however, began to change and the power-base of data processing departments was gradually seen to erode with the introduction of 'mini' computers in the early 1970s. Importantly, these machines were located within and under the control of the respective departments which used them and while this suited the individual departments it did mean that minis were not afforded the same physical security as the mainframes. Nevertheless, the minis could run programmes, manipulate data and create original software (Ceruzzi, 1999).

Another stage in the devolution of computing power was the arrival of the personal computers (PCs). As a consequence massive processing power was placed in the hands of the 'ordinary worker' (Davies , 1996) For those entrusted with the role of securing computer resources the PC represented another area for consideration. If the minis were seen as weakening the utility of the ring fence approach, the PCs made it redundant. Security was no longer an issue of simply securing a mainframe. The security domain was becoming more complex, particularly given the sheer number of PCs, and the people who used them. Donn Parker (1976) illustrates this point in his book *Crime by Computer*. In the early years of commercial computing, the number of reported crimes was remarkable small compared to today's figures. For instance in 1962 there were two cases, while in 1965 there were eight. With the devolution of computing within organisations, more people were being offered the means to commit some form of computer abuse.

Networking has further facilitated the dissemination of computing power both within and between organisations. As Weibschuh (2000) notes:

> As the years passed, PCs spread to everyone in the company and PC islands combined to form local area networks (LANs, now termed intranets). With the arrival of the LAN, data previously stored locally, migrated to a network server ... However, the network's rudimentary and often under-used access controls paved the way for misuse and theft of data, especially when combined with a constantly growing number of networked employees ... Linking LANs to form Wide Area Networks (WANs, now termed extranets) made matters worse. The number of employees grew as LANs were connected into WANs and employees, suppliers, distributors, partners and customers gained intentional or unintentional access to internal data files (Weibschuh, 2000, p. 9).

Hence as computing power has devolved through and between organisations, the potential for increasing numbers of opportunities for computer abuse has grown. This is because unless the appropriate controls are in place to safeguard the ubiquitous computing resources then vulnerabilities will be created and potential opportunities formed. Thus IS security should be seen as an evolving function, mirroring organisational change (BS7799, 1999). Furthermore, the British Standard asserts that the new and emerging risks that arise through organisational change need to be addressed through periodic risks reviews. Unless consideration is given to the security implications for the importation of new resources in particular settings, then vulnerabilities in an organisation's IS will be created. As Lindup (1996) notes:

> Technology can affect security and control because it creates new vulnerabilities. Many companies have seen the potential benefits of delivering information about their products and services to customers via the World Wide Web. Connecting to the Internet is not without its risks. An internet connection is a potential gateway into the corporate networks for hackers and computer criminals.
> (Lindup, 1996, p. 480)

But as stated, security is not just a purely technical concern. All aspects of security need to be catered for when attempts are made to address the risks associated with organisational change. One difficulty with regard to this task concerns the time required for security functions to mature. As Anderson states:

> It can take many years for a security capability to mature and become effective. Continuity matters; and we do not really understand how to maintain effective control in an organisation whose structure is constantly changing.
> (Anderson, 1994, p. 37)

Hence, if security functions are constantly having to respond to changes in organisations, it is feasible to assume that at certain points in time the respective information systems will be vulnerable, given the time lapse between such changes and such responses. Once again, these vulnerabilities may form the basis for criminal opportunities.

2.3 Deficiencies in Existing Notions of Opportunity

Although the literature concerned with opportunity has proven useful in highlighting the problem areas, certain deficiencies need to be addressed. First, very little is written about opportunity. This is probably due to the fact that the meaning of the term opportunity is regarded as obvious and hence there is little reason to examine the subject.

Secondly, there has been a failure to actually define what an opportunity is. Indeed, a common-sense understanding of this phenomenon runs through the literature. From this viewpoint an opportunity might be perceived as a file left on a desk as a result of non-compliance to a clear desk policy, a PC left on at lunch time which should have been logged off, passwords posted to machines, and the like. The failure of this common-sense perspective is that it cannot clearly explain why these so-called opportunities are acted on in some instances and not in others. Could it be that some of the instances simply do not afford an opportunity? This points to the interplay of other factors which the CS perspective is at a loss to explain, but an understanding of which would be of great value to security practitioners. A more suitable theoretical explanation would be able to account for these 'other factors' and in the process be in a better position to explain the aforementioned variances. Unfortunately, one of the deficiencies with regard to IS security generally is the paucity of theory both used and advocated by academics in this field.

Thirdly, the existing literature's prescriptive value is limited. A flawed understanding of opportunity offers little scope for developing effective solutions. If we can assume that opportunities arise in and as a consequence of the daily workings of an organisation, then any approach used to understand opportunity must be able to address those elements involved in these 'daily workings', and explain how interactions between them may create opportunities.

This unfortunately, is far easier said than done. How does one know which factors are influential and which are not? How does one address the interactions between such factors? How can one assume a group of these factors will create an opportunity? In essence how can one circumscribe the problem of opportunity in order to address it?

2.4 Conclusion

Through a review of the literature it is noted how those texts which address opportunity fall into one of two groups. One group addresses how opportunities may act as a motivational factor with regard to organisational staff. The other focuses on how opportunities are created through the absence, poor implementation and maintenance of safeguards. Despite the benefits of these two bodies of literature in raising awareness regarding the problems of opportunity, there are notable deficiencies. First there is little written about opportunity. This is probably due to the fact that the meaning of the term opportunity is regarded as obvious and hence there is little reason to examine the subject further. Secondly, the existing literature fails to define opportunity, but rather a common-sense understanding of the term prevails through the texts. The failure of this perspective is that it cannot explain why these so-called opportunities are acted on in some instances and not in others. This would require an explanation of the role of other factors, most notably the role of the agent in this process. The final deficiency relates to the prescriptive value of the existing literature. A flawed understanding of opportunity offers little scope for effectively addressing the phenomenon. However, addressing opportunities is easier said than done as a major problem is knowing how to circumscribe an opportunity in order to address it. The following chapter describes a model known as the 'Crime Specific

Opportunity Structure' which can be viewed as an attempt to overcome the problem of circumscription.

Chapter Three: Theoretical Framework

The purpose of this chapter is to describe the model which is assessed in this research. The chapter commences with a discussion of a criminological school of thought known as Situational Crime Prevention (SCP). Central to this approach is the aim of reducing opportunities for crime. The chapter then moves on to discuss other like-minded criminological theories which have helped to strengthen SCP. These theories include the rational choice perspective, environmental criminology, routine activity theory and lifestyle theory. The next section describes an attempt by Clarke (1995) to synthesise the aforementioned theories in a model entitled the 'Opportunity Structure for Crime'. The chapter then moves on to describe a number of changes made to Clarke's model, culminating in a description of the 'Crime Specific Opportunity Structure', which represents the theoretical framework assessed in the current research.

3.1 SCP

Situational Crime Prevention (SCP) is a relatively new school of thought. Differing in its focus from most criminology, its starting point is an examination of those circumstances which afford specific kinds of crime. Through an understanding of these situations, measures are introduced to induce change in the relevant environments, with the aim of reducing the opportunities for specific crimes. Its emphasis is thus on the criminal setting as opposed to the criminal. Rather than sanctioning or detecting offenders, the aim is to circumvent occurrences of crime, and rather than aiming to reduce criminal tendencies through the enhancement of certain aspects of society, such as better housing or education, the relatively simple aim is to make criminal action less appealing to offenders.

In striving to bring these aims to life, a pivotal role is played, not as might be expected by the criminal justice system, but by a plethora of public and private agencies including manufacturing businesses, schools, local parks, entertainment facilities, hospitals, public houses, shopping centres, and the like. Unfortunately for these organisations and agencies, through their respective services, products, and operations, emerge the unwelcome by-product of criminal opportunities for a number of different crimes and a number of different criminals.

Many case studies, however, can now be cited where preventive measures have been successfully implemented. Examples include surveillance systems for parks and underground stations, controls on alcohol at music festivals and sporting fixtures, conflict management training for bouncers, and street closure/traffic schemes for residential neighbourhoods (Clarke, 1997).

Despite these encouraging advances in combating specific crimes, little attention has been given to situational prevention from criminologists and policy-makers responsible for addressing crime control. Clarke (1997) argues that this is due to two 'mistakes' made by modern criminology. First, he asserts that the task of explaining crime has been assumed to be the same as explaining the criminal (Gottfredson and Hirschi, 1990). Unlike SCP, 'dispositional' criminological theories have been eager to provide accounts of why and how individuals through the assimilation of specific social or psychological influences, or the inheritance of traits, are as a consequence more inclined to acts of a delinquent or criminal nature. This is not the same as explaining the occurrence of crime, which, aside from requiring a motivated offender, also warrants an opportunity. Simply to explain criminal dispositions, Clarke contends, is only half the equation. What is further required are explanations of how offenders interact with the settings in which crime may or may not occur (Ekblom, 1994).

The second 'mistake' revolves around the issue of crime control versus dealing with the criminal (Wilkins, 1990). The predominant assumption is that if reductions in crime are to be achieved, the surest route is to concentrate on offenders or potential offenders. The literature has viewed the problem by citing the role of formal and informal social control. The former relates to those bodies that constitute the criminal justice system and the Law, responsible for the sanctioning, confining, or rehabilitation of offenders, and, on a wider level, deterring criminal acts among the public at large. The latter refers to the role of socialisation and attempts to instil conforming behaviour in young people through the recognition of appropriate norms, enhanced by behavioural prompts of censure, admonition, and more formal rules based systems. These two types of control can be seen to address offenders, be they potential or actual in nature.

Clarke (1997) contends that the failure to distinguish between controlling crime and how criminals are dealt with leads to the neglect (both by the majority of policy-makers and criminologists) of a third area of crime control safeguards distinct from, but interrelated and dependent upon formal and informal social controls. This third group is typified by the 'routine precautions' (Felson and Clarke, 1995) undertaken by organisations and members of the public to reduce the risks of crime. These precautions take the form of buying burglar alarms for homes, or steering locks for cars, counselling children on appropriate behaviour, securing valuables, and avoiding particular places and people. Organisations of all types similarly strive to implement measures designed to protect themselves, their staff, and their customers. SCP may be located within this third group of control. Indeed, this school of thought can be viewed as the 'scientific' arm of routine precautions, in that its aim is to provide a clearer understanding of specific crimes and thereby develop more effective and beneficial safeguards.

3.1.1 Situational Crime Prevention Defined

Before moving on to discuss its theoretical origins, a formal definition of SCP should be provided. SCP comprises the implementation of opportunity-reducing controls that a) target specific forms of crime; b) impact on the immediate environment via its design, management, or manipulation; and c) aim either to increase the effort and risks of crime, or to render these less rewarding or excusable. Examples of these measures, which are categorised into certain types, include the *controlling of facilitators* (e.g., gun controls: to increase the effort), *entry/exit screening* (baggage screening: to increase the risks), *target removal* (e.g., removable car radios: to reduce the rewards), and *rule-setting* (e.g., harassment codes: to remove excuses), (Clarke, 1997). A number of points derive from this definition.

As mentioned SCP's focus is crime-specific. This stems from a recognition that specific types of crime are unique in their mix of constituent environmental factors. Foregoing a discussion of crime prevention at the level of 'burglary' or 'robbery', greater emphasis is placed on those specific crimes that fall under these broader categories. For example, Poyner and Webb (1991) argue that preventive measures needed for tackling burglary of domestic electronic goods differ from those required to prevent the burglary of household cash or jewellery. This, they contend, is due to differences in the way these crimes are carried out as evidenced in their study of burglary in a British city.

The definition cites how this blocking of the commission of specific crimes involves the introduction of safeguards in the immediate environment. Such actions are designed to impact on the offender's perceptions about the potential costs and benefits of crime commission. Adjustments made in terms of the manipulation, design, or management of the environment are intended to either increase the perceived risks or reduce the rewards of the potential crime or both. The decision to commit a crime will be based on the perceptions and evaluation of the situation. It is no surprise, then, to learn that SCP has drawn heavily on rational choice theory, discussed further in the next section.

In addition, it is assumed as part of the decision-making process that some evaluation is made with respect to the possible moral costs of offending. While some offenders may be prepared to shoplift, this does not mean they are prepared to mug the elderly. In an attempt however to overcome any feelings of guilt or shame, offenders may try to neutralise such feelings through the construction of excuses such as 'everybody else does it', 'I'm just borrowing it', etc. Support for this assertion comes from earlier criminological writings by Sykes and Matza (1957) who discuss 'techniques of neutralisation' and Bandura (1976) who, in a similar vein, addresses the concept of 'self-exoneration'. Given this, attempts to negate the possibility of offenders using such methods may at times prove a useful preventive safeguard.

A final refinement to the definition relates to application areas. Although SCP takes a crime-specific focus, there is no mention as to which categories of crime it considers most useful to address. This is because writers in the field believe the approach can be used to address all types of crime, not just conventionally perceived 'opportunistic' crimes, but also deeply motivated crimes. Although offences may be carefully planned or underpinned by strong emotions such as hate or anger, the offenders are still susceptible to situational contingencies which impact on commission decisions (Tedeschi and Felson, 1994). This provides the requisite room for manoeuvring, in which measures may leverage the situational impact in a manner which benefits the potential target and hinders the offender.

3.1.2 Theoretical Origins of SCP

The catalyst for the development of SCP was a series of studies on correctional treatments, undertaken by the Home Office Research Unit in the late 1960s and early 1970s. These studies cast doubt on the rehabilitative model, leading workers in the Unit to review the utility of other options for crime control, including incapacitation, deterrent sentencing, preventive policing, and 'social' prevention. The latter refers to attempts at implementing measures to assuage social, economic, educational and community inequalities that are believed to be culpable for engendering criminal values and attitudes. Unfortunately, the review concluded that the aforementioned could do little to expand the scope of crime control, irrespective of pragmatic and ethical problems associated with their implementation. However, the research into correctional treatments highlighted a possible area for future research in the form of opportunity reduction. The particular studies which centred on probation hostels (Sinclair, 1971, 1975) and approved schools (Clarke and Martin, 1971) indicated that the likelihood of the youths absconding or re-offending seemed to be dependent more on the type of regime than on their personality or background. Of particular importance was how the institutional environment appeared to provide opportunities to misbehave. It was surmised that if the aberrant behaviour could be regulated by making changes to certain situational factors, there was the further possibility that other forms of crime could be controlled in this manner.

Such findings (as analysed within social learning theory) did not sit happily with dispositional theories of crime that emphasised biological, psychological, or sociological factors. They found greater support in the guise of psychological research into personality and behavioural traits, which pointed to the surprising extent of the influence of situational factors, and even questioned the utility of personality as a hypothetical construct (Mischel, 1968). During this period, work in the field of sociology was undermining the idea of deep motivational commitment to conformity (Matza, 1964), and, as with the psychological research, further evidence was being provided about the role of situational factors. In this instance, the pressures to deviate conferred by working class gang membership (Yablonsky, 1962; Short and Strodtbeck, 1965). The importance of environment and opportunity was further supported by earlier criminological research, which had found higher rates of property offences during the winter period, as a result of longer hours of darkness (Burt, 1925). Additionally, experimental studies of deceit indicated how the dishonest behaviour of children was tempered by the level of supervision afforded them (Hartshorne and May, 1928).

This body of work allowed for a much more dynamic view of crime compared to that espoused by dispositional theories. Contrary to the latter, criminal conduct appeared to be influenced by variations in opportunity, transitory pressures, and inducements. This new perception of crime was reinforced by further work produced by the Unit, including the examination of the impact of steering-column locks on car theft (Mayhew *et al.*, 1976) and the surveillance role of conductors in an attempt to combat vandalism on buses (Sturman, 1976). Research into residential burglary was also pointing out how target-selection was to some extent dependent on the avoidance of risk and effort (Scarr, 1973; Reppetto, 1974; Brantingham and Brangtingham, 1975; Waller and Okihiro, 1979).

The watershed in the development of SCP was a simple 'choice' model of crime first advanced in a seminal paper by Clarke (1980). In it the author reasserts the critique of dispositional criminological theories by arguing that, whilst these theories have been concerned to demonstrate how some people are born with or come to acquire such a disposition, they have neglected addressing situational determinants. One of the major drawbacks of the dispositional theories, Clarke suggests, is the implementation of policies in areas where it is difficult to achieve any positive effect, i.e., in relation to socio-economic conditions or bio-psychological factors. As James Q. Wilson (1975) notes when discussing the fortunes of America during the 1960s, even when attempts (although not directly aimed at decreasing crime) were made to reduce poverty, improve education, and provide better housing, crime rates did not fall, but instead, they 'soared'. Similar problems are faced when attempting to change a person's temperament, or other biological variables, and it is difficult to envisage what measures could be taken to make guardians care for and exercise more discipline over their children. These findings are echoed by more recent research undertaken by Smith (1995), who found that when Sweden and other European countries adopted more egalitarian income distribution policies, and improved welfare systems, rather than witnessing crime reductions, they witnessed crime increases. Clarke adds that although these problems are of a pragmatic nature, they do indicate the inconsistencies and uncertainties faced when addressing these 'causes' of crime. Knowing at which point to intervene in the regressive chain of causal events has therefore been a considerable stumbling block for dispositional theories.

Clarke (1980) advocates that such theoretical problems could be avoided if crime were not viewed in terms of dispositions, but rather as a series of 'choices' made by the offender. This would place a direct focus on the criminal event, and allow room for the development of explanations of separate categories of crime. Furthermore, the immediate features of the setting, and the individual's current circumstances would be given more explanatory significance than in 'dispositional' theories.

3.2 The Rational Choice Perspective

These ideas have been developed and evolved into the formulation of a 'rational choice perspective', which has been extremely influential in determining the theoretical base of SCP (Clarke and Cornish, 1985; Cornish and Clarke, 1986; Clarke and Cornish, 2000). Although rational choice theory has a considerable academic pedigree in its mother field of economics, it is a relative newcomer with regard to criminology. Admittedly, several criminological rational choice theories do exist (Clarke and Cornish, 1985; Cornish and Clarke, 1986), but it is the 'perspective' advocated by Clarke and Cornish that has probably drawn the most attention from researchers.

Essentially, there are six key propositions to this approach. First is the assumption that crimes are deliberate and purposive: that is, those who commit crimes do so with the intention of deriving some type of benefit from such acts. Obvious examples are cash or material goods, but a broader reading of the term 'benefits' allows for the inclusion of other forms such as prestige, fun, excitement, sexual gratification, and domination. Joyriding is an example of how the benefits may take the intangible forms of fun and excitement. Hence, on appraisal, crimes may make more sense once their respective motives and rewards are understood.

The second proposition relates to the concept of 'bounded' rationality. As mentioned within the field of criminology, several rational choice theories have been put forward (Hechter and Kanazawa, 1997), but there is a lack of consensus as to what is considered a 'rational' choice. Opp (1997) identifies 'wide' and 'narrow' positions in this debate. The wide position, which subsumes the Cornish and Clarke approach, assumes that choices are characterised by what is termed 'bounded' or 'limited' rationality. In other words, criminal decision making is at times less than perfect, as a consequence of the conditions under which decisions are made. With the associated risks and uncertainty in offending, criminals may make decisions without the knowledge of all the potential costs and benefits (i.e. the risks, efforts, and rewards). Devoid of all the necessary information, criminals may resort to 'rules of thumb' when perpetrating offences, or rely on a tried and tested general approach that may be called into action when unexpected situations arise.

As in everyday life, little thought may be given to the longer-term implications of actions, and a number of mitigating factors can lead to what are deemed rash choices. Decisions may have to be made quickly and under pressurised conditions. Peers may encourage criminal actions, and such actions may be taken whilst under the influence of drugs. These actions may end in the capture and punishment of offenders, leading some to conclude that the behaviour of the offender was of an irrational nature. The rational choice perspective, however, asserts that offenders are merely making the best of a sometime poor situation, given the constraints on resources, time, and information.

The third assumption relates to crime specificity. The factors considered by criminals and the related variables that influence the decision-making process vary considerably with the nature of the offence. Thus the analysis of decision-making needs to be made with reference to specific categories of crime. Legal categories of robbery and auto-theft are too generic because these umbrella terms cover diversely motivated offences undertaken by a broad spectrum of offenders utilising a plethora of skills and methods. For example, the theft of a car for temporary transport is different from the theft of a car for joyriding, which is again different to the theft of a car which may be sold locally or overseas.

Nevertheless, the crime-specific approach does not assume all crimes to be committed by specialists. While acknowledging the generalist nature of some offenders, however, this should not obscure the fact that the motives and methods used by the generalist offenders may vary greatly according to the specifics crimes they choose to undertake. Within the group offenders who are not generalists can be found those who act on specific opportunities that arise in their work or form part of their everyday lives. This group may on the whole be considered law-abiding, but succumb to specific temptations and can, perhaps surprisingly, be found to account for a large proportion of crime (Gabor, 1996).

Of further importance to the rational choice perspective, and forming the fourth proposition, is the division of criminal choices into two groups, viz., 'event' and 'involvement' decisions. The former refers to those decisions made during the commission of a crime, and in the case of suburban burglary, for example, could involve choices as to the target, the point of entry, and decisions about which items to steal. The latter is made at three stages of the criminal or delinquent career. The offender must make decisions about embarking on criminal activities, whether or not to continue these activities over a period of time, and when, if at all, to cease offending. Or, to use the technical terminology, choices must be made about the initiation, habituation, and desistance of a criminal career.

Again, the choices are framed within the crime-specific focus. As far as event decisions are made, the task of avoiding capture differs greatly for bank-robbers, compared to those who vandalise cars. Involvement decisions must also be seen through the lens of crime-specificity. Consideration of the factors that lead individuals to commence criminal careers, and the relevant experience drawn on by individuals, highlight the need to be crime-specific. The initiation decisions for a bank-robber for example, will obviously differ from those of a stock-broker who practises insider dealing.

The fifth assumption asserts that the crime-specific principle be applied to the three separate stages of involvement, i.e., initiation, habituation, and desistance. This is based on an understanding that the decisions made for each of these stages will be influenced by different sets of variables, which must accordingly be recognised for the purpose of prevention. These variables can be divided into three categories, including background factors, current life circumstances, and situational variables. Background factors include the biopsychological (e.g., temperament, gender, intelligence), upbringing (e.g., broken home, parental crime, poor education) and the social (e.g., class, ethnicity, and social exclusion). Current life circumstances include such factors as marital status, employment, housing, and leisure pursuits, e.g. drug-taking and gambling. The third category, that of situational variables, encompasses current needs and motives e.g. an urgent need for cash, and opportunities and inducements, be they of a legitimate (e.g. job offer) or illegitimate nature (e.g. invitation to commit a burglary).

Perhaps, not surprisingly, these three groups are of differing importance to the stages of involvement. Hence, background factors have their greatest impact on initiation decisions, whereas current life circumstances come into their own with respect to habituation choices. Decisions on whether to end a criminal career will further be influenced by current life circumstances and an enhanced knowledge of the potential costs of crime, with background factors playing no role in the decision.

The sixth and final proposition centres on the sequence of event decisions, which an offender faces during the commission of a crime. Original work in this area focused solely on choices made in terms of the potential target (Clarke and Cornish, 1985;

Cornish and Clarke 1986), but as a result of theoretical advancements it was realised that, as the criminal act unfolds, the perpetrator is required to make a series of decisions (Clarke and Cornish, 2000). The offender may have little time to make these decisions, due to the speed with which the criminal act presents the choices. Alternatively, the sequence may afford the offender greater breathing space. Consider the example of a suburban burglary. Two burglars, both of whom require money, may meet by chance. Plans are initiated through the theft of a vehicle for transport, after which attention turns to the choice of a target in a suitable neighbourhood. A suitable point of entry into the target house is decided, followed by decisions on what to steal. Further choices then have to be made about where to conceal the stolen property prior to the selling of the goods to a fence or other third party.

Two prominent criticisms levelled at the rational choice perspective have questioned first the degree to which offenders are rational, and second whether some crimes can be perceived as rational. The questioning of offender rationality may be based on the conception of crimes as impulsive, spur-of-the-moment type activity, prompted by an unexpected opportunity. At the other extreme may be situated those crimes that are meticulously planned and prepared. In the middle of this 'rationality' axis, however, is where the majority of crimes reside, with the offender, who has previously decided to undertake crime, acting on opportunities he has sought out. These points are argued in detail by Maguire (1980) and Bennett and Wright (1984) in their studies of residential burglaries.

While critics may be willing to concede that crimes of a white-collar nature and predatory crimes such as burglary and robbery, may be regarded as rational in nature, the same may not be said for other types of crime (Trasler, 1986). These 'other types' usually include some sexual component or make reference to crimes of violence and vandalism, which are often perceived as 'senseless'. Where crimes are underpinned by pathological compulsions or clinical delusions, the initial reaction may be to assume that such crimes are beyond the remit of the rational choice perspective. However, the 'irrationality' of these crimes may be only in terms of the motivational factors e.g., a serial killer who believes God has told him to murder prostitutes. Other aspects of the crime including, for example, its planning and commission, may show considerable rationality on the part of the offender. Either way, it should be noted that crimes of this kind form only a very small percentage of all criminal acts, and it does not stop the point being made that the rational choice perspective can be applied to all types of crime.

Those who view violent crimes or acts of vandalism as irrational or senseless fail to recognise the benefits that are derived from these crimes. Football or gang violence is often labelled as senseless, but once we consider the potential benefits, such crimes can be seen to harbour a rational element. They may provide great excitement amongst the perpetrators and allow for the developing of esprit de corps amongst the individual group. Gladstone (1978), in his study of vandalism committed by Liverpool youths, pointed to how such acts seemed to feed a hunger for fun and excitement, and afford individuals a chance to prove their toughness to their peer-group members.

In the case of domestic violence an individual who beats his wife might do so because it is the easiest way to get her to acquiesce to his demands. Indeed, an economic model of violence in a household has been developed by Witte, Tauchen and Long (1984). While discussing repeat victimisation with regard to domestic violence between estranged couples, Farrell, Phillips and Pease (1995) highlight the potential risks efforts and rewards associated with the offender's activities:

> ... it is certainly more effort to assault an ex-partner when her home has to be entered first. As for rewards, if the disruption of a normal life for the ex-partner is the pay-off, repetition is essential. Thus repetition can occur with relative impunity, and may be essential to the 'reward' of disrupting the victim's new life (Farrell *et al*, 1995, p. 387).

Supporting insights into the benefits of crime is provided by the work of Tedeschi and Felson (1994) who argue that all violence is essentially instrumental. Whether the latter is threatened or actually enacted is down to the benefits that accrue as a result. Their work has involved analysing the actions that occur between aggressor and victim. What helps to define the outcome between the two are situational factors and incremental choices made by both parties during their interaction. To some extent, the outcome is negotiated between aggressor and victim.

3.3 Environmental Criminology

Another notable influence on SCP has come from the body of knowledge known as environmental criminology. Clarke (1997) contends that in the last decade, environmental criminology has comprised two analytical paths. The first relates to offender decision making and has been seen to generally support rational choice premises. These studies have covered a multitude of offender types, including car thieves (Light et al., 1993; McCullough et al., 1990; Spencer, 1992), bank and commercial robbers (Normandeau and Gabor, 1987; Kube, 1988; Nugent et al., 1989) and burglars (e.g. Walsh, 1980; Maguire, 1982; Bennett and Wright, 1984).

Carroll and Weaver's (1986) study is illustrative of this type of research. Focusing on shoplifting, they were interested in obtaining first hand accounts of offender reasoning. After advertising in a local newspaper for respondents, Carroll and Weaver divided those who applied into 'experts' (those with an extensive self-reported history) and 'novices' (those with a lesser history). Owing to the fact that thinking aloud is an uncommon act for the majority of people, the members of both sample groups were then coached in using verbal protocols to help illuminate their patterns of thought. The subjects were then asked to take the researcher on a 'shopping trip' around a store that was familiar to them. Each respondent was reminded to 'think aloud' with their thoughts captured on a concealed tape recorder. During the shopping trip, which lasted approximately an hour, the researchers coded each store based on its characteristics, including store layout (e.g. height of aisles), item protection (e.g. locked cases, chained items), security devices (e.g. mirrors and cameras) and people (e.g. number of sales clerks).

The verbal responses of the subjects were subsequently analysed and provided clear insight into their shoplifting strategies. The experts were perceived to arrange their thought processes hierarchically i.e. consideration was first given to the type of store, next a department of the store, and finally items on sale in particular departments. Novices, however, displayed little evidence of this phenomenon. More refined strategic behaviour was further shown by the experts in terms of discussing a number of possible strategies, aside from discussing a strategy with respect to a specific item. Hence ten (out of seventeen) described shoplifting techniques that they had used or would consider for use in the future. This was in contrast to the novices who only mentioned strategies in terms of potential items worth stealing.

The verbal responses of the two groups also threw light on what would and would not deter shoplifting. The factors that acted as a deterrent included item inaccessibility (e.g. too large/heavy), the chance of being observed/caught, security devices, the presence of store personnel, and negative feelings e.g. guilt. The absence of the aforementioned as well as a store layout, which would aid the act (e.g. high counters which impeded surveillance), were seen as facilitators.

Carroll and Weaver also noted the patterns of deterrents and facilitators related to items that the respondents deemed worth stealing or leaving. For those items worth stealing, the novices made verbal references to one facilitator and no deterrents. For those items that they perceived as not worth stealing, the verbal responses included reference to at least one deterrent along with facilitators. Hence one deterrent was all that was required to stop the 'commission'. A different strategy seemed to be followed by the experts, who considered deterrents in terms of how to avoid or get around them.

With respect to the weight given to deterrent factors in terms of their importance, there were notable disparities between the two groups. Security devices and item inaccessibility were considered primary deterrents by the experts. These were of relatively less importance to the novices whose major concern was being observed or caught. Novices also displayed a greater amount of negative feelings compared to the experts, and this highlights to some extent the moral elements espoused by the rational choice approach. As one respondent stated about an item 'it would be, you know, against the law, and I guess that's where my mom comes in my head saying 'what right is it of yours to take'.

In terms of the degree of rationality, Carroll and Weaver's conclusion appears to support the rational choice premise that event and involvement decisions need to be clearly distinguished for the sake of effective prevention strategies. As they assert:

> Overall, this analysis (and conjecture) suggests a fairly high degree of rationality in the decisions of both experts and novices. Both pay attention to a lot of information that pertains to the consequences of their acts. However, this process appears to occur normally over an extended period of time, with different considerations at different points in time, each consideration being quite simple and manageable. The sequence is quite similar to the distinction between first choosing to have an academic career and later choosing to apply for a job or accept a particular job offer. (Carroll and Weaver, 1986, p. 33).

Studies such as the one undertaken by Carroll and Weaver have provided useful information about motives, methods, and target choices which can then be assessed for preventive implications.

This is also true of the second path taken by environmental criminology which involves the 'objective analysis of the spatial and temporal variation in crime patterns in order to discover aggregate factors influencing the patterns' (Brantingham and Brantingham, 1991: 239). These studies can take a macro, meso or micro focus. Clark argues that macro data, which focuses on a country or state level, rarely produces consequential findings for prevention (Clarke, 1997). The same cannot be said, however, for some micro level analysis work. Work of this nature, which examines the occurrence of crime in certain buildings or sites, can provide fruitful insight (Kennedy, 1990), as may 'meso' level studies. Poyner and Webb's (1991) study of domestic burglary in two cities is indicative of this kind of research. In their research, the majority of burglaries in their study were committed in older homes close to the city centre, where the target was cash or jewellery. Offenders made their getaway on foot, in contrast to burglars who targeted electronic goods in the newer distant suburbs, where, due to the nature of the haul, cars were required to facilitate the criminal act. As a consequence, the offender's transport needed to be parked close to the victim's house, without drawing the attention of neighbours. In the suburbs, the layout of the streets afforded this possibility. The suggestions for prevention advocated by Poyner and Webb involved increasing the natural surveillance over roadways and parking places. For the burglaries that took place in the older houses situated close to the city centre, recommendations were made to improve surveillance and security at the point of entry to the dwelling. This example suggests that if specific crimes are made up of a unique mixture of environmental factors, consideration must be given to blocking these crimes in highly specific ways (Clarke, 1997).

Aside from the analysis of spatial and temporal variations in crime patterns, environmental criminology has provided considerable insight into the 'search' patterns of offenders. More precisely, this school of thought illustrates how the majority of crimes are committed within areas visited by offenders during their routine work and leisure pursuits (Brantingham and Brantingham, 1991). Offenders develop an 'action space' in which these everyday pursuits take place and through such activities acquire a detailed knowledge of this environment, leading to what Brantingham and Brantingham (1991) describe as an 'awareness space'. Like the rational choice perspective, Brantingham and Brantingham (1991) argue that the motivated individual engages in a 'multi-staged decision process' prior to the commission (or not as the case may be) of a crime. Such a process is informed through knowledge gathered from the offender's awareness space. Furthermore, they argue that a specific environment emits cues relating to its spatial, cultural, legal and psychological characteristics. With experience an offender is able to discern certain sequences and configurations of these cues associated with a 'good' target.

3.4 Routine Activity Theory

SCP has further been developed by Routine Activity Theory, another relative newcomer to the field of criminology. In a ground-breaking paper on this approach, Cohen and Felson (1979) consider a sociological paradox noted by the U.S. National Commission on the Causes and Prevention of Violence (1969: 37).

> Why, must we ask, have urban violent crime rates increased substantially during the past decade when the conditions that are supposed to cause violent crime [poor housing, education, etc] have not worsened – have indeed generally improved (1969, p. 37)?

Drawing on statistics from the FBI Uniform Crime Report in the period 1960-1975, the authors point to how rates of aggravated assault, homicide, forcible rape, and robbery have increased by 164%, 188%, 174%, and 263% respectively. Similarly, property crimes fared no better - e.g. a 200% increase in the burglary rate - leading Cohen and Felson to argue that the paradox noted by the Commission applies equally well to instrumental crimes.

In an attempt to provide some insight into this anomaly, Cohen and Felson discuss how changes in what they describe as 'routine activities' of the U.S. populace have impacted on the levels of direct-contact predatory crimes, i.e. crimes where one or more persons directly take or damage the person or property of another. These routine activities can be defined as prevalent and recurrent activities involved in meeting the needs of the population and individuals. They include the provision of food, shelter, leisure, work, child-rearing, and sexual outlets. Of particular significance to the theory are the locations of these activities, which can take place a) at home b) in employment away from the home, and c) in other activities situated away from the home.

It is argued that these routine activities influence the direct-contact predatory crime rates by impacting on the convergence, in time and space, of the three elements required for a crime to occur. These elements include a likely offender, suitable targets, and the absence of a capable guardian, who, if present, would be in a position to stop a criminal act. A likely offender is perceived as anyone, who for whatever reason, might commit a crime. The second element, a suitable target, is any person or object that is attacked or taken by the offender. This might include a woman the offender wants to rape or a television he wishes to steal. With regard to the third factor, where our first reaction may be to think of law enforcement agencies with regard to issues of guardianship, the vast majority of guardianship is provided by members of the public over their own and other people's - i.e., relatives, friends, neighbours - property and well-being. Cohen and Felson assert that it takes merely the absence of one of these three elements for a crime not to occur. In addition, changes in the convergence in time and space of suitable targets and the absence of capable guardians may lead to crime-rate increases, even if the population of likely offenders remains the same. In other words, changes in routine activities may impact on the convergence of suitable targets and the absence of capable guardians, providing more opportunities for the same number of offenders. Hence it can be seen that illegal activities feed off changes in perfectly legal ones.

The intellectual roots of routine activity theory are to be found in the human ecology research of Amos Hawley (1950), which recognises the importance of the timing of different activities by hour-of-day and day-of-week for understanding human society. This is central to routine activity theory, which addresses changes from moment to moment and hour to hour in relation to what people are doing, where they are, and the consequences of these as a result (Felson, 1994).

Cohen and Felson maintain that post-war America has witnessed significant changes in routine activities away from the home, and toward employment or other activities situated outside the household and involving non-family members. This, they contend, has altered the relationship between the three elements required for a predatory crime to occur, as a result of decreases in the level of guardianship afforded. The rationale behind this line of thought posits that the home environment and family members provide considerable guardianship over potential targets and have a lower risk of victimisation compared with non-household, non-family activities. Evidence used by Cohen and Felson, from U.S. victimisation surveys covering the years 1973 and 1974, support their hypothesis. Rates of rape, robbery, and assault, for example, are far lower at home, compared with elsewhere. In addition, individuals in the presence of relatives have similarly lower rates of victimisation. Conversely, there are those individuals, who on leaving the safe harbour provided by families and households, are more likely to become victims of crime. For example, those who live on their own have less guardianship afforded them, as does their property when the individuals leave their place of residence, whether for work or leisure activities. In addition, young people who spend more time away from the household have higher rates of victimisation. More time spent on the streets equates with a greater chance of becoming a suitable target. An hour in such a setting is far riskier compared to an hour at the family home. This risk, however, can be counterbalanced by family members who provide additional guardianship outside the household setting. Hence, the combined levels of guardianship provided by families and households afford considerable protection against victimisation.

One other assumption made by the routine activities approach relates to how target suitability can influence the occurrence of predatory crime. Cohen and Felson cite the factors of value, accessibility, visibility, and inertia as influential, and point to how vehicles and electronic appliances constitute the highest rates of theft.

In brief, Cohen and Felson argue that significant increases in certain crimes can be related to changes in the routine activities of the U.S. population. These changes have eroded the level of guardianship afforded to people and their property. Besides highlighting fluctuations in the respective crimes, Cohen and Felson also examine U.S. census data to understand the movements in routine activities which, they argue, have facilitated the increase in predatory crimes. Figures such as a 31% increase in the number of married females participating in the labour force, or a 34% increase in the number of individuals living on their own, can be seen to affect the degree of guardianship over themselves or their property.

The role of households and families have led some to critique routine activity theory by asserting that it could not account for domestic violence, the majority of which occurs in the home context (Felson, 2000). In defence, Felson (2000) argues that this critique is based on a 'naïve interpretation' of the theory. Rather than assuming that the movement of activities away from the household and family members is definitive, Felson states that this is merely a simplistic example of the truly definitive elements required for a predatory crime. Hence, of fundamental importance to the theory is the underlying principle that, for a predatory crime to take place, requires the convergence in time and space of a likely offender, a suitable target and the absence of a capable guardian. Felson stresses that this applies to activities that take place inside as well as outside the home environment. He cites the example of a father raping his stepdaughter when the mother is away, i.e., when the capable guardian is absent.

Routine activity theory is still in a period of transition, as witnessed by the attempts of Felson (1992) to extend the scope of routine activity (by suggesting minimal elements for other categories of crime), and include a fourth element - that of the 'intimate handler' - in relation to direct-contact predatory offences. Drawing on social control theory (Hirschi, 1969), 'intimate handlers' refers to those individuals, who, by knowing an offender, may act as a 'brake' on illegal activities carried out by the latter. As a means of enhancing its contribution to crime prevention, Clarke (1992) advocates that routine activity theory could incorporate the category of 'crime facilitators'. These relate to items such as cars, guns, and credit cards, which act as tools for specific crimes - as well as dis-inhibitors such as alcohol, which facilitate the precipitation of crimes.

Indeed, the relevance of routine activity to the rational choice perspective has not been lost on Clarke and Felson (1993), who discuss their common frames of reference. Of importance to both approaches are the centrality of situational determinants of crime, crime specific explanations, and the important distinction between the criminal and crime. Both in addition provide organising perspectives for analysing crime: the rational choice approach through the four decision models and the elements of crime for routine activity theory.

3.5 Lifestyle Theory

Another school of thought closely related to the routine activity approach and which has proved influential in the development of SCP is the victimological work of lifestyle theory. In their text *Victims of Personal Crime*, Hindelang *et al.* (1978) put forward a theoretical model of victimisation based on the analysis of data from eight American cities. They assert that the probability of someone suffering personal victimisation is dependent to a large extent on the person's lifestyle, which 'refers to routine daily activities, both vocational activities (work, school, keeping house, etc.) and leisure activities'.

Central to Hindelang *et al.'s* model are 'role expectations' and 'structural constraints'. These act as constraints to which individuals must adapt, if society is to run smoothly and avoid inner conflict. For a given individual, role expectations and structural constraints are dependent upon the constituent demographic characteristics (e.g. age, sex, race, income, marital status, education, occupation) of that individual.

Role expectations, as used in the model, make reference to cultural norms associated with the ascribed and achieved status of individuals. These norms guide and define preferred and achieved behaviours. Of importance are those role expectations dedicated by the central statuses of individuals, i.e., their primary defining statuses. For example, the role expectations of a child differ dramatically to those of an adult. Likewise, the role expectations of a married person differ to someone unmarried.

Structural constraints are perceived as limiting behavioural options, and exist within the institutional orders of the economic, the familial, the educational and the legal. Economic factors, for example, can appear to impose limitations on the choices available to some people, with respect to where they live, educational opportunities, and modes of transportation. With the decline of the extended family in the U.S., this too has ramifications for choices made. People may have to spend more time at home for cooking and child-rearing activities, whereas previously these responsibilities could be shared with grandparents or other members of the extended family.

It should further be noted that there is a reciprocal relationship between role expectations and structural constraints. The role expectations of a parent in a social structure predominantly populated by nuclear families, may, therefore, be quite different to those of a parent in a social structure characterised by extended families.

So society's members do indeed seem to adapt their behaviour to the structural constraints and role expectations. This adaptation takes place at both the individual and group level. Each member acquires skills and attitudes which enable a person to operate, with some individuality, within the constraints imposed. Of particular relevance to the model are those attitudes and beliefs that individuals assimilate with respect to crime. Apart from adaptation at an individual level, shared adaptations also emerge. These type of adaptations have been discussed with reference to 'delinquent subcultures' (Cohen, 1955) and a 'sub-culture of violence' theory (Wolfgang and Ferracuti, 1967).

Through the process of adaptation emerge regularities in behavioural patterns. Identifiable within these patterns are the routine activities of employment, house keeping, school going, and leisure pursuits. Of paramount importance is how these separate routines collectively constitute a person's lifestyle.

In the model proposed by Hindelang *et al.*, disparities between people's lifestyles occur through differences in their structural constraints, role expectations, and individual or sub-cultural adaptations. Criminal victimisation is not randomly distributed across time and space. Rather, there are high-risk times, places, and people. Differences in lifestyles are associated with differences in exposure to those settings which carry a high risk of victimisation. Hence, the lifestyles of some people lead them into exposed situations that are high risk, compared to the lifestyles of others.

As a complement to their model, Hindelang *et al.* list a series of propositions with respect to how particular lifestyles carry greater probabilities of victimisation. These include:

> 1. The probability of suffering a personal victimisation is directly related to the amount of time that a person spends in public places (e.g. on the street, in parks, etc.), and particularly in public places at night (p. 251).
> 2. The probability of being in public places, particularly at night, varies as a function of lifestyle (p. 253).
> 3. Social contacts and interactions occur disproportionately among individuals who share similar lifestyles (p. 255).
> 4. An individual's chances of personal victimisation are dependent upon the extent to which the individual shares demographic characteristics with offenders (p. 257).
> 5. The proportion of time that an individual spends among non-family members varies as a function of lifestyle (p. 259).
> 6. The probability of personal victimisation, particularly personal theft, increases as a function of the proportion of time that an individual spends among non-family members (p. 260).
> 7. Variations in lifestyle are associated with variations in the ability of individuals to isolate themselves from persons with offender characteristics (p. 262).
> 8. Variations in lifestyle are associated with variations in convenience, the desirability, and vincibility of the person as a target for personal victimisations (p.264).
>
> (Hindelang *et al*, 1978)

The conclusion of Hindelang et al's work is that through an greater understanding of how people become victims, the risks of victimisation may be reduced through altering those aspects of their behaviour that increase exposure to high-risk situations.

More recent work in this area has addressed the scope for preventing repeat victimisation (Farrell, 1992, 1994; Pease, 1993, 1994). Reviewing several crime types ranging from domestic violence to shop theft, Farrell, Phillips and Pease (1995) argue a clearer insight into this phenomenon can be gained through the application of rational choice theory. Hence, the degree and differences in the rates of repeat victimisation reflect what they perceive as the actions of a reasoning offender. In an attempt to reinforce a theoretical understanding of repeat victimisation, they further draw on routine activity theory. As a consequence, a motivated offender would be considered to make a reasoned choice (based on the risks, effort and reward) with regard to the suitable target (victim) and the absence or existence of a capable guardian. They conclude by asserting:

> The rational choice theory of offender decision making seems to apply particularly well to repeat victimisation. Offences against the same target by the same offender are based on the experiences of the previous victimisation, and perception of known risk and rewards. This rational choice is based upon the motivated offender's greater knowledge of the victim's suitability and the likelihood of the absence of capable guardians. For repeat crimes against the same targets committed by different offenders, the 'rational' decision factors influencing target selection (perceived victim suitability, perceived likelihood of capable guardianship) will be those which prompted offenders to target the same victim (Farrell *et. al*, 1995, p. 396).

Environmental criminology, the rational choice perspective, and lifestyle and routine-activity theories have all played a part in strengthening SCP. Through the interviewing of offenders and the analysis of crime patterns, environmental criminology has provided useful food-for-thought with regard to countermeasures. The rational choice approach affords a framework to help organise such information, so that individual studies may produce more general benefits. With a focus on peoples' work and leisure activities and the implications for victimisation, lifestyle theory helps to shed light on what individuals can do (through changing their patterns of behaviour) to avoid this outcome. Lastly, routine activity has helped to broaden preventive options by enabling a greater understanding of the essential elements of certain crimes. As a result of highlighting the 'convergence' of these elements, it has been proposed, for example, that 'deflecting offenders' becomes an SCP measure (Clarke, 1992).

3.6 The 'Opportunity Structure for Crime'

An article, by Cusson (1986) asserts that differences between the aforementioned could turn out to be mainly of historical interest, and that a synthesis of these approaches is desirable and inevitable. Following on from this, Clarke (1995) attempts in a recent paper such a synthesis as shown in Fig. 1 and entitled the 'Opportunity Structure for Crime'. What is useful about this synthetic model is its ability to incorporate dispositional variables of traditional criminology. Within the model itself is situated the *criminal opportunity structure*. This is made up of *targets* (cars, ATM machines, convenience stores, etc.), *victims* (e.g. drunks, women alone etc.), and *facilitators* (guns, cars, as well as disinhibitors such as alcohol or other drugs).

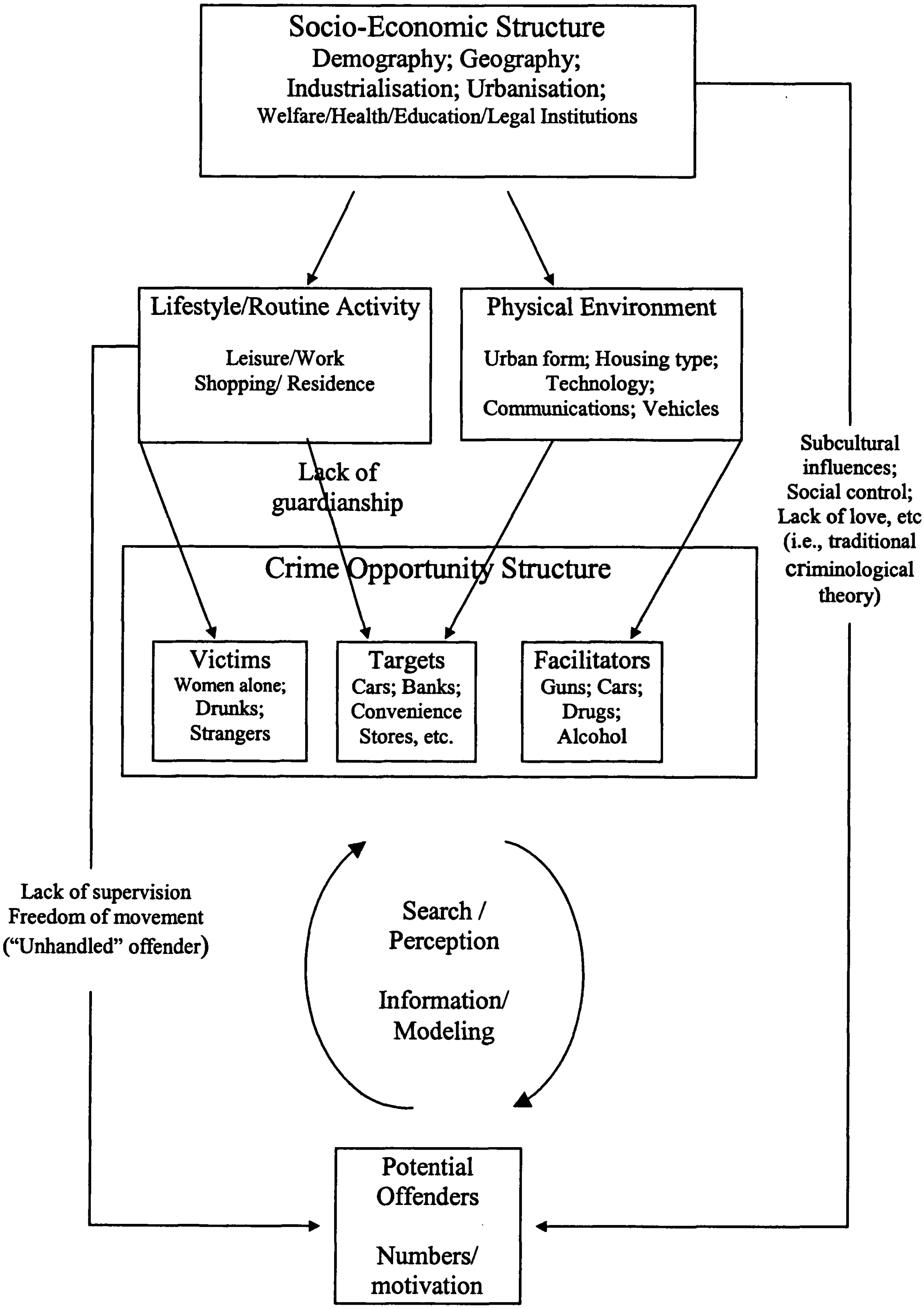
As can be seen from Fig. 1, *targets* and *facilitators* are a result of the *physical environment*. For the former these include cars, banks, and convenience stores; whereas examples of the latter would be get-away cars, guns for armed robberies and drugs likely to loosen inhibitions and thereby lead to the commission of a crime. Targets are also the result of *lifestyle and routine activities* of the population. These patterns relate to work, leisure, residence, and shopping. What is interesting is that these patterns can be seen to either facilitate or hinder guardianship. Facilitators, as per the crime opportunity structure, are provided by the physical environment, whilst lifestyle and routine activities supply the *victims*.

At a more macro level, the *socio-economic structure* determines the lifestyle/routine activities and the physical environment. The former includes demography, geography, industrialisation, urbanisation, welfare/health, education, and legal institutions. The socio-economic structure also partly determines the number of *potential offenders* through sub cultural influences, such as neglect and lack of love, alienation etc. (identified by traditional criminology), and partly through lifestyle and

eg lack of black jobs → crime of blacks.

Fig. 1

Opportunity Structure For Crime



routine activities. These can influence the degree of social control afforded by intimate handlers, leading to a possible *lack of supervision* and *freedom of movement.*

What needs to be stressed here is that the opportunity structure is not simply a physical entity, consisting of the routine activities of the population and the nature of the physical environment. Rather, it comprises interaction between supplies of victims, targets, potential offenders, and facilitators, which determine the nature and scale of the opportunities for crime. These interactions largely take place in the 'action' and subsequently 'awareness' spaces of offenders as indicated by the *search/perception – information modelling* sections of the model and highlighted by environmental criminology. The offender's *perceptions* (highlighted by the rational choice perspective, but also environmental criminology) of the risks, efforts, and rewards associated with such spaces play a crucial role in defining the opportunity structure.

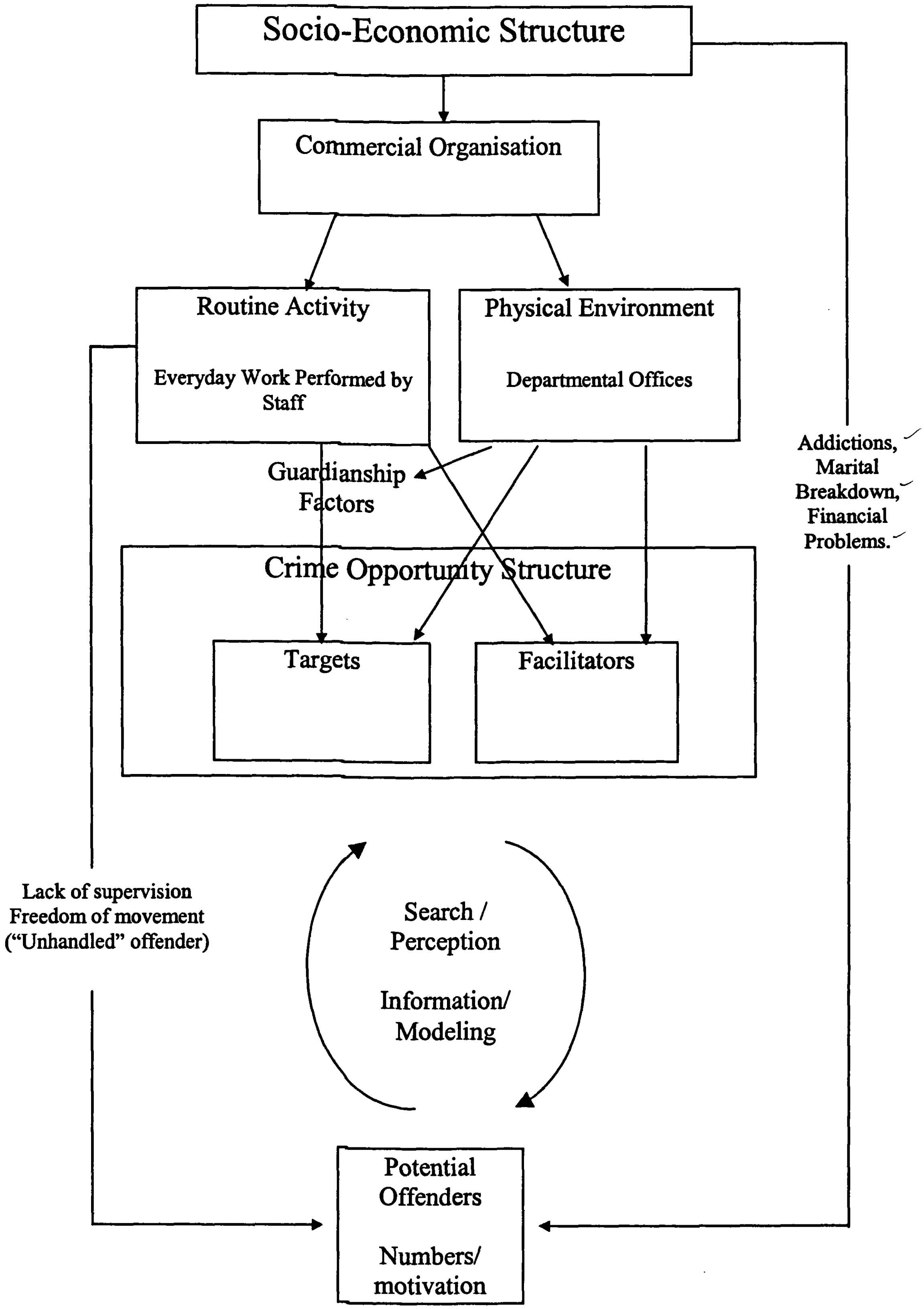
3.7 The 'Crime Specific Opportunity Structure'

The theoretical framework for the current research is based on Clarke's model, albeit, with one major difference. As discussed, SCP is underpinned by a crime specific approach. Although Clarke's model is generic in nature, the central aim of the present study, as mentioned, is to assess the feasibility of an opportunity structure with a crime specific focus. In other words, is it feasible to address opportunities by developing crime specific opportunity structures? Fig. 2 represents the theoretical framework to be 'assessed' with regard to the collapse of Barings Bank. The original model has been modified, given the nature of the crime perpetrated at the bank, and the context in which the crime was enacted.

The 'victims' box has been omitted from Fig. 2. This is not to suggest that organisations are not victims of various forms of computer abuse, but rather that Fig. 1 makes use of the term with respect to how an individual's lifestyle can increase the risks of their own victimisation. Given this, it was felt that this had little relevance to an opportunity structure set in the context of an organisation.

Fig. 2

Crime Specific Opportunity Structure



As with Fig. 1, targets and their nature are the result of the *physical environment*, in this instance, departmental offices. They can also be seen to be the result of *routine activities*, which incorporate patterns of work, and as mentioned earlier, can either hinder or reinforce guardianship. The latter is expressed not as per Fig. 1, in terms of 'lack of guardianship', but as *guardianship factors*, and depending on their nature or even existence they will influence the opportunity structure. So, for example, included in this box could be 'division of duties'. Failure to appropriately segregate working practices (e.g. ensure staff are not responsible for front and back office duties) will afford an absence of guardianship over the work processes and create a potential vulnerability in the respective control system. Other guardianship factors could include, for example, internal/external audit, compliance monitoring etc.

Facilitators, per Fig. 2 are provided not only by the physical environment, but also by the routine activities of staff. Interestingly, the internal threat posed by an organisation's own staff, places a somewhat different spin on the notion of facilitators. The physical environment provides facilitators in the form of standardised systems. If departmental staff use the same type of computers with the same operating systems, then this facilitates the goals of the offender, as knowledge of the working of multiple systems is not required. Moreover, the offender has an in-depth knowledge of the system other people use.

Apart from facilitators which have a physical form, the organisational environment provides a context in which cognitive facilitators can be developed and used by potential offenders (Willison, 2000b). This type of facilitator includes skills and knowledge that a person acquires to perform their job responsibilities. Although such skills and knowledge are, on the whole, used by staff for purely legitimate activities, they can also be used to help perpetrate activities of an illegal nature.

At a more macro level the *socio-economic structure* determines routine activity and physical environment in the form of *commercial organisation*. The socio-economic structure, as per Fig. 1, partly determines the number of *potential offenders*, through sub-cultural influences including alienation, lack of love, etc., or in other words the traditional domain of dispositional theories. While Fig. 2 maintains this element of the model, the focus on specific socio-economic factors shifts. Given that the 'population' to be highlighted in the fall of Barings are bankers and securities staff, more pertinent socio-economic factors which could impact on the numbers and motivations of potential offenders would include addictions in their various guises, marital breakdowns, financial problems and the like.

The number of potential offenders as with Fig. 1 are also partly determined by routine activities in terms of the degree of supervision afforded by managers, leading to either handled, or *unhandled* staff and hence potential offenders. In keeping with the original model, Fig. 2 acknowledges the *search-perception* and *information modelling* activities of potential offenders in their action and awareness spaces.

3.8 Conclusion

The purpose of this chapter is to describe the model assessed in the research. Opening with a discussion of SCP, it is noted how the focus of this school of thought is on the criminal setting. More specifically SCP aims to reduce the opportunities for crime through implementing controls that a) target specific forms of crime; b) impact on the immediate environment via its design, management, or manipulation; and c) aim either to increase the effort and risk of crime, or to render them less rewarding or excusable. The implementation of safeguards into the immediate environment, are designed to impact on the offender's perception about the potential costs and benefits of undertaking a crime. This illustrates the influence that the rational choice perspective has on SCP. The former focuses on the decision making processes of criminals. Another theory that has influenced SCP is that of environmental criminology. Two analytical paths have emerged with regard to this approach in the last decade. One of the paths has focussed on offender decision making and has been generally seen to support the rational choice perspective. The second path has thrown considerable light on the 'search' patterns of offenders, acknowledging how offenders acquire through their everyday pursuits a detailed knowledge of the environment in which such pursuits take place. This knowledge is used to inform criminal decisions.

The chapter further discusses how SCP has been developed by routine activity theory. This theory addresses those elements that are required for certain crime to take place.

Hence, a likely offender, a suitable target, and the absence of a capable guardian would afford a crime commission. The presence of a capable guardian would act as a deterrent.

Closely related to routine activity theory and the final school of thought discussed in the chapter, is lifestyle theory. This body of work asserts that a person's lifestyle has a direct impact on the probability of suffering personal victimisation. Given this, the theory addresses the changes in the patterns of people's behaviour that can be used to avoid the likelihood of victimisation.

The synthesis of the aforementioned theories in the form of the 'Opportunity Structure for Crime' is then described (Clarke, 1995). SCP takes a crime specific focus which stems from a recognition that specific types of crime are unique in their mix of constituent environmental factors. Hence an appreciation and understanding of these unique mixes will afford greater insight for prevention programmes. Given this crime specific focus, the chapter then moves on to describe a number of changes made to Clarke's model, culminating in a description of the 'Crime Specific Opportunity Structure', which acts as the model to be assessed in the current research.

Chapter Four: Research Methodology

As its title states, this chapter describes the methods of the research project. Divided into three main sections, the first examines the philosophical underpinnings of the research, drawing on the interpretive and more precisely hermeneutic tradition. The reasoning behind these choices is discussed. The next section examines the research approach used in this study, namely ethnography. Central characteristics of this approach are discussed, followed by a review of the IS ethnographic literature. The contributions and limitations of the approach are highlighted, followed by a discussion focusing on the reasons why an ethnographic stance was taken for this body of research. The final section describes the data collection and analysis methods used in the study.

4.1 Philosophical Underpinnings

All social scientists approach their research with a certain worldview or paradigm, a set of assumptions or beliefs that guide their inquiries. These assumptions include their perceptions of the nature of reality (their ontological beliefs), and their relationship with the phenomena being studied (their epistemological beliefs) (Creswell, 1998).

Either of two broad positions may be taken when referring to ontology. Adopting a 'nominalist' position signifies a belief that, beyond individual cognition, the social world consists of nothing more than labels, concepts, and names used to structure reality. Advocates of nominalism reject the idea of any 'real' structure to the world to which these concepts, names, and labels refer. The antithesis of nominalism is 'realism'. Realism asserts, that beyond individual cognition, there is a real world of tangible structures. Although we may not be able to perceive these structures, realists assert their existence as empirical entities. They believe the social world exists independently of a person's appreciation of it. The social world in this sense is seen to have a reality of its own.

Closely related to issues of ontology are those concerned with epistemology. Epistemology refers to theories or forms of knowledge. Like ontology, there are two broad positions that can be taken with regard to an individual's epistemological beliefs. Positivism may be used to characterise epistemologies, which in their explanation of the social world, attempt to identify causal relationships and regularities between the constituent elements of the former. This form of epistemology is based upon the traditional approaches of the natural sciences. The second position, that of anti-positivism, rejects the notion of searching for regularities and causal relationships, and, as a consequence, further rejects the idea of an 'observer' – who, positivists maintain, is able (from that vantage point) to understand the social world. Rather, anti-positivists believe the only way to understand the latter is by understanding the points of view of those being studied. The relativist position additionally maintains that understanding can only be achieved by adopting the participant's 'frame of reference'. Hence, it is believed that understanding can only come from inside.

The philosophical assumptions of this research are located within the interpretive tradition. Ontologically, interpretivists reject the notion of a real world beyond human cognition, and with its own reality. Taking a nominalist stance, interpretivists believe the social world is constructed by individuals via negotiating meanings they produce as part of everyday life.

Epistemologically, a central tenet of interpretivism is that there is a fundamental difference between the subject-matter of the social and natural sciences. Interpretivists reject the idea that social world can be explained by identifying causal relationships and regularities between constituent elements. Further, the notion of value-free data is rebuffed, given the researchers role in guiding enquiry and their interactions with human subjects, resulting in altered perceptions of both parties. Consequently, interpretivism:

> Is informed by a concern to understand the world as it is, to understand the fundamental nature of the social world at the level of the subjective experience. It seeks explanation within the realm of individual consciousness and subjectivity, within the frame of reference of the participant as opposed to the observer of the action (Burrell and Morgan, 1979, p. 28)

The reasons why an interpretive position has been taken in this research can be illuminated by a discussion focusing on the nature of IS. Indeed, the mid 1980s to early 90s witnessed a debate that did just this. Writers such as Galliers (1991) and Land (1992) and others (Backhouse *et al.*, 1991) argued that IS are not merely computer systems, but computer systems embedded in a social context. This position was reinforced by work in the 1990's that consistently pointed to how the social and organisational context in terms of IS design, development and application led to the greatest practical problems (Hirscheim and Newman, 1991; Newman and Robey, 1992; Walsham, 1993).

This need to consider the social context of an IS can equally be applied when considering security of the aforementioned. Various writers (Dhillon, 1997; Backhouse, 1997) have argued that if we are to understand the true nature of security problems that IS face, we must be able to examine the whole of the problem and view IS from this socio-technical perspective.

If we accept this position, then insight into the social reality that prevails with the workings of an information system, can be garnered by understanding the existing social reality which is constructed through shared and negotiated meanings. Interpretivism, then seems to be a logical choice, for it is able to help illuminate these meanings, and as a consequence, the countervailing social reality. Indeed, interpretive information systems research is emerging as an acceptable body of inquiry within the IS discipline (Walsham, 1995a, 1995b; Lee *et al*; 1997).

More precisely, this research draws on hermeneutics for its particular interpretive approach. Hermeneutics, which can be defined as the philosophy of the interpretation of meaning, has been used by several members of the IS community (Lee, 1994; Myers, 1997; Introna, 1997). The current research draws on ideas and concepts from the work of Paul Ricoeur (1976, 1981), an established figure in the field of hermeneutic philosophy. The reasons for adopting such an interpretive stance will become clearer during the course of the chapter. Suffice to say, given that the origins of hermeneutics can be found in the interpretation of texts, it seems particularly well suited to the research tradition and methodology used in this study.

4.2 Research Strategy

In conjunction with the debate focussing on the nature of IS, a parallel and closely related debate was being held which addressed the appropriate research approach to be utilised in IS research.

The late 80s and early 90s further saw an increasing dissatisfaction with the existing IS research approaches. At the time, the most common research methods used in IS were laboratory experiments, surveys, and descriptive case studies. Indeed, Orlikowski and Baroudi (1991), in their analysis of research methods used in IS research found a strong preference for positivistic methods, which afforded an acontextual and ahistorical view of IS. IS research was charged with a lack of diversity (Galliers and Land, 1987; Orlikowski and Baroudi, 1991), while other writers claimed IS research to be superficial and faddish in nature (Banville and Landry, 1989).

What emerged was a call for methodological pluralism (Galliers, 1991; Avison and Myers, 1995; Banville and Landry 1989; Hirscheim and Klein, 1989). If we are to view IS as socio-technical systems it was argued, the richness and complexity of organisational settings could not be unearthed by approaches that provide an a-historical/contextual view. In response to this call, qualitative methods have assumed a prominent position in IS research (Yin, 1989; Walsham, 1993, 1995b; Benbasat, Goldstein and Mead, 1987), mainly as a result of their ability to help research social and organisational contexts (Hirscheim and Newman, 1991; Newman and Robey, 1992; Walsham, 1993). More traditional positivist techniques consider context either as a set of interfering variables that need controlling, known as noise in the data, or other controlled variables which are experimentally set up in order to seek cause and effect relationships (Harvey and Myers, 1995). Hence the context is seen as something that should either be factored out or operationalised as a variable.

Those interpretive researchers, however, who take the view that to understand IS you must also address the social context, have increasingly turned to ethnography as a suitable qualitative approach. In recent years a small but growing number of information systems researchers have recognised the value of the ethnographic method for information systems research (Harvey and Myers, 1995; Lee, 1991; Lee, Baskerville and Davis, 1992; Davis and Nielsen, 1992; Pettigrew 1985; Wynn, 1991).

The origins of the ethnographic approach can be traced back to the work of Bronislaw Malinowski and his seminal text *Argonauts of the Western Pacific* (1922). Although he was by no means the first person to collect data from non-Western cultures and societies around the world, what distinguished Malinowski from other anthropologists of his time was the way he was able to contextualise the data. While other researchers had collected material from such cultures, taken out of context, fragments of insights into the cultural practices of the researched groups confused Western onlookers. Rather than presenting the cultural practices in a peacemeal manner, what Malinoski did was to present his findings holistically. In doing so readers of his work were able to see how cultural practices viewed from this perspective made sense. The ethnographic method soon became the preferred form of research for anthropologists. Members of the now celebrated Chicago School of sociology, such as Dewey, Park, and Mead in the 1920s and 1930s used this approach to study the cultures on their doorstep (Bogdan and Biklen, 1992).

Yet what exactly is an ethnography? The following section discusses several central characteristics common to many such studies with the intention of providing the reader with a basic grounding on this research tradition. A useful starting point is to highlight how ethnography refers to far more than just data collection and analytical techniques. As writers including Wolcott (1995) and Frake (1983) assert, ethnography can be seen as a perspective, an approach, a series of procedures and a type of presentation.

Of even greater significance, however, is the major goal of ethnographic research, which predominantly defines this approach. As Wolcott (1987) states:

> If words spoken could appear in neon lights or pyrotechnic displays, my statement would brighten the sky with the carefully chosen words: The purpose of ethnographic research is to describe and interpret cultural behaviour.
> (Wolcott, 1987, p. 43).

Somewhat problematically there is little consensus among ethnographers as to what constitutes this term. However, for the purpose of this research, the following definition advocated by Goodenough (1976) is used.

> The culture of any society is made up of the concepts, beliefs, and principles of action and organization that an ethnographer has found could be attributed successfully to the members of that society in the context of his dealings with them (Goodenough, 1976, p.5).

In line with this definition and additionally echoing the sentiments of Frake (1964) and Wolcott (1987, 1995) is the idea that the major role for the ethnographer is to construct a 'theory' of a specific group/insitution/society's cultural behaviour which can then be attributed to the respective group. As a consequence, culture is not seen as something 'lying about', waiting to be found by the ethnographer (Wolcott, 1987). Rather, through the examination of a specific group's words and actions, beliefs, rituals, myths, artefacts and the like, culture can be inferred and attributed to them by the ethnographer. Hence the ethnographer renders a 'theory' of cultural behaviour to the group under study (Frake, 1964; Goodenough, 1976; Wolcott, 1987). This theory can further be seen as an explicit statement of the actions of a group; but this account has no existence until it is formulated and attributed to the group by the researcher.

For many ethnographers 'thick description' is a central guiding concept in their research (Geertz, 1973). It refers to how an ethnographer develops an understanding of the schemas and sense-making activities of their subjects. Of primary importance, and in keeping with the ontological and epistemological stance taken in this research, is the concept of meaning. The ethnographer is charged with the task of understanding situations with regard to the meaning they hold for individuals. At times a consensual understanding of a situation may imply a shared meaning, while at other times, a situation may hold contradictory and contested meanings. These multiple meanings, and their associated complex connections need to be elicited by the ethnographer to enable a 'thick description' of the subject group. Geertz (1973) drawing on the work of Gilbert Ryle, provides an illustrative example of two boys quickly contracting their right eyelids. An observer perceives the actions as exactly the same, and by providing an account based solely on the acts, affords a 'thin description'. However, by making reference to the meaning of the act - i.e., one boy has an involuntary muscle twitch, while the other is engaged in a conspiratorial signal - a subsequent account would be described as 'thick description'. An ethnographic account can thus present diverse notions of reality due to the diverse interpretations of participants in a given situation.

Another defining characteristic of ethnography is the manner in which the approach privileges local knowledge (Prasad, 1997). It is hence not the goal of ethnographic studies to produce universalistic knowledge or what is sometimes referred to by social scientists as 'grand theory'. Such a type of theory, espoused by for example some Marxists, attempts to perceive and understand human action through a number of universally applicable lenses. The understanding of certain events is therefore mediated by very broad categories and concepts such as class, race, status, etc. This runs counter to the beliefs of almost all ethnographers who give precedence to local knowledge. They critique proponents of grand theory by arguing that in their attempt to construct universalistic knowledge, they neglect rather than reveal those elements that in reality are the basis of such knowledge, i.e., local interpretations and cultural contexts.

For the researcher to be in a position to develop a 'theory' of culture for a particular group, ethnographers normally spend extensive periods of time in the field, drawing on a number of data collection techniques (Hammersley and Atknison, 1995; Fetterman, 1998; Creswell, 1998). Of primary importance to the ethnographer is the technique of 'participant observation'. As is evident by the name, this method involves ethnographers spending considerable time observing the activities of their subjects. There are a number of observatory roles open to the researcher. These include the 'complete participant', 'participant as observer', 'observer as participant' and 'complete observer' (Junker, 1960; Gold 1958). The complete participant for example involves the researcher hiding their true identity through the undertaking of covert research. Groups or organisations studied in this manner have included Alcoholics Anonymous (Lofland and Lejeune, 1960), Army units (Sullivan *et al.*, 1958) Pentecostalists (Homan, 1980), and mental hospitals (Rosenhahn, 1973). At the opposite end of the spectrum is the 'complete observer' who has no contact with the subject being studied. Corsaro (1981), for example, observed nursery children through a one-way mirror, while Karp (1980) observed the 'public sexual scene' in Times Square in New York. It should be noted, however, that the majority of ethnographic studies fall somewhere between the two ends of the spectrum.

In addition to participant observation, a highly popular data collection technique is the interview. It is at times difficult to identify a dividing line between participant observation and interviews, given the often informal and spontaneous nature of the latter. The task is somewhat easier with interviews of a more formal nature, often taking place at specially designated times and locations. Structure to such interviews is often provided through a series of topics, although there are limits to the extent of formalisation as Hammersley and Atkinson (1995) state:

> Ethnographers do not usually decide beforehand the exact questions they want to ask, and do not ask each interviewee exactly the same questions, though they will usually enter the interviews with a list of issues to be covered.
> (Hammersley and Atkinson, 1995, pp. 151-152)

As data-gathering techniques, both participant observation and interviewing can prove highly complementary. Observation can inform the researcher's interpretations of their informant's remarks. In his research into the United States Congress, Dexter (1970) found that observing the activities of the congressional office afforded a degree of 'credibility' when it came to analysing interviews. These interviews, he argues, further acquired meaning as a consequence of the periods of observation. Just as observations may inform interpretations of interview responses, the reverse is also true. Woods' (1981) interviews with secondary school students and their subsequent remarks about the 'boring' nature of particular classes, led him to observe the phenomenon in the class-room setting. As he states:

> The word, I realize now, is onomatopoeic. I could never view the lessons in company with that group again without experiencing that boredom myself. They would occasionally glance my way in the back corner of the room with the same pained expression on their faces, and I knew exactly what they meant.
> (Woods, 1981 p. 22)

Aside from observation and interviews, documents are another important source of data for ethnographers (Cresswell, 1998; Fetterman, 1998; Hammersley and Atkinson, 1995). Admittedly, ethnographic studies have on many occasions researched what are essentially oral cultures. These may take the form of the non-literate type, the focus of much social anthropology, or those settings where there is no conscious attempt to document the activities of the particular group, apart from the efforts of the researcher. Members of the Chicago School provide numerous examples of such cultures where the lives of prostitutes, drug-takers and hobos rarely warranted the production and preservation of documents. That said, many of the contemporary setting in which ethnographers carry out their research are of a literate nature. Apart from the ability of people in these settings to read and write, integral to many of their activities, are the utilisation of these skills.

Hammersley and Atkinson (1995) identify two types of documents that may be drawn on whilst studying literate cultures. These include 'secondary' documents that are produced routinely and may have some relevance to the study at hand, and alternatively, those documents that are produced and used in the actual research setting.

There are a plethora of 'secondary' documentary materials that may be of relevance to a researcher and their study. These range from the 'informal' (e.g. letters, diaries, fictional literature etc.) to the 'formal' or 'official' (e.g. official statistics). Thomas and Znaniecki's (1927) *The Polish Peasant in Europe and America* is an early example of the way 'informal' documents can be used as a source of research data. Now regarded as a classic American sociological text, the study relied heavily on written documents, particularly letters, to construct an ethnographic account.

The other source of documentation is that afforded by the ethnographic setting. Gamst (1980), for example, in his study of locomotive engineers, indicates the number of workplace documents open to his perusal:

> Some documents are published, for example: rule books, time-tables, technical manuals for use of equipment, and instructional, regulating, and investigating publications of many kinds used by railroads, trade unions, government, and other firms. Unpublished documents include; official correspondence, reports in mimeographed and other forms, railroad operating bulletins and circulars, train orders, operating messages, and other sundry items (Gamst, 1980, p. 8).

A number of ethnographers have taken a more pro-active approach by coaxing members of specific cultures to keep personal diaries over a period of time. This was the case with Davies's (Davies and Atkinson, 1991) study of novice midwives. On retrieving the diaries for analysis, Davies found that aside from acting as a valuable source of research data, the midwives had used them as a confessional device, helping them to reveal their anxieties, frustrations and anger.

The importance of documents to ethnographic research should not be underestimated. Hammersley and Atkinson (1995) argue that 'there is nothing to be gained and much to be lost' in portraying literate cultures as essentially oral in tradition. Indeed, developments within anthropology, the mother discipline, and the emergence of historical anthropology and subsequently historical ethnography, have led to the increasing use of archival material, and in some instances such material has acted as the sole source of data. Historical anthropology emerged over the latter half of the last century as a reaction to those anthropological studies which ignored or deliberately avoided issues of dynamic process and history.

There are a number of reasons why anthropologists have become more attuned to historical processes as a result of a plethora of innovations and trends in their field. The post Second World War period witnessed anthropologists examining regimes of colonial domination (Gulliver, 1958; Southall, 1962), and how such regimes impacted on cultural and social institutions including religious practices, patterns of co-operation, and kin/household groups. Anthropologists by the 1950s realised the need to actively address these patterns of change impacting on their subjects, rather than treating them as traditional stable orders. As a consequence of these recent social changes, anthropologists turned their focus on the history of their subjects, and subsequently the related historical documents.

A further development saw the emergence of interest in social process and the dynamism of social life. Rather than assuming that social reproduction merely leads to repetition, anthropologists attuned their studies to appreciate how these elements that constitute social life e.g. patterns of interaction, roles, values and institutions, change through time (Silverman, 1980; Schryer, 1980).

The influence of Marxism in the late 1960s played its role in fashioning anthropology. Original conceptual and empirical vistas emerged for anthropologists through viewing their subjects through the theoretical lens of political economy (drawing on Marxism to varying degrees), leading to various studies, each reaffirming the commitment to historical anthropology (Nash, 1979; Vincent, 1982; Stoler, 1985).

Historical and sociological studies of household composition, social life and family structures in the past were also influencing anthropology. Laslett's (1965) work on domestic domains and kinship, for example, drew the attention of anthropologists who shared a similar focus, but until that time had concentrated on contemporary societies.

Anthropologists have also become more self-reflective and self critical, questioning their role, and recognising how their own discipline has evolved through the last few decades. As Silverman and Gulliver (1992) argue:

> Whether anthropology has simply been a 'child of imperialism' and the degree to which a scholarly discipline has been controlled by the socio-cultural context of its practitioners have been, and are, matters of considerable debate. The point here, however, is that anthropologists have been induced to consider the historical context within which they worked and, therefore and by extension, the historical dimensions of the people they studied (Silverman and Gulliver, 1992, p.15).

Further monographic studies from both sides of the Atlantic during the 1980s have led to the position, where for many anthropologists, through their studies, it is now necessary to look at the past for an understanding of the present. Hence Silverman and Gulliver (1992) describe historical ethnography as:

> A description and analysis of a past era of people of some particular, identifiable locality, using archival sources and, if relevant, local oral history sources. The ethnography may be general, covering many aspects of social life during that era, or it may concentrate on specific features, such as social ecology, politics, or religion ... social anthropologists have been concerned to link past and present, chronologically and processually, in order to explain and understand the present by reference to the past (Silverman and Gulliver, 1992, p. 16).

The concern therefore of historical ethnography has not rested solely on the 'here and now' with regard to contemporary subject groups. There is an additional focus on how past conditions, processes and events have fashioned their modern-day counterparts. As a consequence archival documents have proved an invaluable source of data when constructing historically informed accounts. A variation on this theme has witnessed the undertaking of historical ethnographies covering periods entirely in the past. In such instances archival materials have acted as the sole source of data. For this type of study, their periods of study have been chosen either as a matter of convenience, or dictated by historical conditions. Vincent's (1984) study of religion, marriage and class in Fermanagh during the nineteenth century is an example of the former, while Dening's (1980) research into the Marquesas from the period 1774 to 1880 (where 1880 was the year colonial domination was achieved by France) is an example of the latter.

4.2.1 IS Research and the Ethnographic Tradition

As briefly touched on, ethnography has increasingly been recognised as a valuable research tradition by an ever increasing number of IS researchers. Seminal studies include the work of Wynn (1979), Suchmann (1987), and Zuboff (1988).

Wynn's (1979) research, for example, examines office communication. More precisely, in her study of a telephone sales order-entry organisation, she was interested in understanding whether the social environment at work supports information, as opposed to merely promoting camaraderie and good working relationships. The organisation itself comprised employees who fielded calls from customers who wished to order copier supplies, and another group of staff involved in adjusting customer accounts as a result of billing/shipping errors, returned goods, etc.

Recordings of the conversations between staff members and between staff members and customers, constituted the primary data collection technique. Through her analysis, Wynn discovered how social bonding and task information were 'wound together'. Hence the social environment, Wynn argues, is an important resource for employees. In addition, analysis of the data uncovered a number of information activities occurring regularly through the tape recordings. These included, providing instructions for other employees, engendering social bonding with customers, and clarifying procedural terms and the like.

Wynn contests that in all functions, including those of a routine nature, uncertainty and ambiguity must be overcome before related procedures can continue. This, she argues, was the case with the staff in the telephone sales order company, who continually applied this 'value', made possible as a result of being part of a social group in verbal contact.

The conversations were typically characterised by informality, camaraderie, and co-operation. The following quote is indicative of the types of conversations held between staff members

> Paul: Hello, Jan?
> Jan: Mhmmm?
> Paul: I've got a gal who got some bad – boxes of labels.
> Jan: I hear ya tryin' a talk 'er out of 'em.
> Paul: Yeah, they're curlin up and such, on the sides.
> Jan: Arright – just take the - d' y' have the order number that she ordered 'em on
> Paul: I've got - no. She, I'm getting 'er-she's got the old invoice. It was back in March, 'n this doesn't go back quite-it goes to March, but not when she ordered 'em.
> Jan: Okay, arright.
> Paul: So, I'm gonna get that invoice number that we billed 'er on. And then, uh-
> Jan: Get the supply order number-yeah, get the supply order number off that invoice 'n then I c'n send 'er somp'n.
> (Wynn, 1991, p. 57)

This research, and the work of Zuboff (1988) and Suchmann (1987) helped to lay the foundations for the acceptance of ethnography as a legitimate research approach within the field of IS. Consequently, and more recently, several researchers have utilised this approach to study various aspects of IS. This section hence aims to provide an overview of these ethnographic studies and their application domains.

IS development is one area in which a relatively large number of ethnographic studies have been conducted. This is perhaps not surprising given the insight afforded by ethnography inquiry into the contextual relations of organisations. Wagner (1993), for example, addresses ethical issues with regard to systems development. The context for her research was a surgery clinic located in a large university hospital. The social practices of time management for operations acted as the focus for the study. The ethnographic approach was chosen to give a clear insight into the working practices and any accompanying problems. Such an insight, it was believed, would aid the development of an IS to improve time management. Problems uncovered by the study were primarily non-technical in orientation, with conflicts centering on ethical and political issues. A number of major problems came to light, which had ramifications for the design of the IS.

One of the proposals put forward to help the planning of operations was a networked personal calendar. This, if implemented, would have enabled the relevant individuals (i.e., out-patient nurses, assistant surgeons and anaesthesiologists) the chance to block-out periods of time to indicate non-availability for operations. The current working practice dictated that all nurses and anaesthesiologists be ever-ready for operations during their working-day. Hence, the calendar was viewed by these groups as an attractive proposition. The senior surgeons, on the other hand, kept sections of their working-day private. This, however, was at odds with the need for temporal transparency, if the calendar was to be accepted and implemented.

Another problem related to explicit and hidden priorities with regard to the allocation of operation times. One set of priorities reflected the hierarchy of specialities found in the clinic. At the apex was heart surgery, which took precedence over others. Other priorities revolved around the desire of surgeons to undertake as many complex operations as possible. This was underpinned by a chance for advanced learning and the possibility of future research publications. As a consequence, patient admission was highly selective. While some of these priorities, and others including for example 'emergency' patients, were hidden, proposed computer-support required all priorities to be explicit, unambiguous and decision-relevant in nature. The clinic was therefore faced with the problem of negotiating the legitimacy of priorities and practices.

Wagner further notes that although several parties were involved in an operation, major decisions, such as the postponing or prioritising an operation were taken by senior surgeons. She concludes by advising systems designers to consider a suitable democratic ideal with regard to all the actors who use or are affected by an IS. As she states:

> Participation based on a corporate concept of democracy gives specific weight to the 'voice' of otherwise underrepresented actors (in our case nurses, women, patients). This ensures that minority points of view are given more than token consideration (Wagner, 1993, pp. 100-101).

Another study of IS development, and based in the medical domain, is that of Myers (1997). He cites the development of an IS for a mental health care provider (Sky City Health) in New Zealand. Functions to be supported by the IS covered 'core/administration' duties and included:

- ADT (Administration, Discharge and Transfer)
- Referral Management.
- Registration.
- Waiting lists.
- Scheduling
- Tracking.

As part of the IS development, a project team was assembled with representatives from all the pertinent stakeholder groups. Hence, the team consisted of two project sponsors (clinical director, group manager of mental health), a project leader from the information services group, a project developer from information services, an operative co-ordinator from the group managers office, a medical research officer, a psychiatric district nurse, a clerical staff member, a psychiatrist, one charge nurse, and a clinical psychologist. This team had a regular meeting once a week

In addition to the project team, a user group was formed to represent the opinions and requirements of clinicians and clerical staff and their views of the potential prototypes of the system.

One of the areas of conflict highlighted by Myers (1997) related to the issue of 'time-based' costing. This process would have involved staff noting down the time spent on specific work activities. Senior management were keen to see this implemented as part of the new IS, as this would enable costing reports to be drawn up, and off the back of this, future government funding estimates could be prepared. Such keenness, however, was not shared by doctors and nurses, who regarded the activity as a potential threat to their conditions of employment and professional status. Myers described one meeting of the user group in which time based costing is first introduced as a talking point. While management attempted to underplay its importance, members of the user group reacted strongly, annoyed that they had not been informed about it earlier.

Having said that, the majority of doctors and nurses involved with the project team and user groups were optimistic about the ability of the proposed IS to improve clinical performance. Indeed, one interesting dynamic of the project team emerged during the development of the IS. Although comprised of representatives from the different stakeholder groups, members of the team developed a sense of loyalty both to each other and the project. This was also true of the user group, whose members although charged with the responsibility of representing their peers, actually started to identify more with the other group members, and the development of the system.

Given this insight, Myers argues that the project clinician's concerns related not so much to the implementation of the system and the time-based costing, rather of greater significance and concern to them was the perception of their peers regarding the project and the behaviour of the project members. Through commitment to the project, its members afforded it a degree of legitimacy. If costing was implemented, the legitimacy of the members and the project would be questioned.

Myers points to the effectiveness of the ethnographic approach in uncovering the political nature of IS development. In the case of Sky City Health, he discusses how terms like 'user participation' and 'user involvement' masked the deeper cultural and political processes at work. For example, the user group was successful in side-lining the implementation of the costing systems to a date later than the implementation of the main system. Senior management were under the impression that:

> The user group felt that it was too much to ask the staff to get used to both the implementation of the information system and recording of their statistics in a new way (Myers, 1997, p. 294).

Hence the opposition to the time-based system was perceived in terms of user adjustments to a new system. The 'problem' was therefore shifted from the political hot potato of systems goals to the politically neutral issue of user acceptance.

The study of infrastructures is another IS domain in which ethnographic research has been undertaken. Star and Ruhleder's (1996) study focussed on the use of the Worm Community Systems (WCS), a customised piece of software, designed for linking together geographically dispersed geneticists (approximately 1400 in total). The role of the WCS infrastructural tool was to support collaboration between the biologists involved in researching genetic structure, behaviour, and the biology of a nematode called *c. elegans*. WCS afforded potential users several capabilities including informal/formal communication, data access from a number of sites, graphical representations of the physical structure of the organism, an updated genetic map, research annotations of a formal/informal nature, Worm Breeders Gazette (a quarterly newsletter) and acedb, an independently developed database.

The two authors conducted research at twenty-five laboratories with a collective staff of over one hundred biologists. Working practices were observed and semi-structured interviews were conducted over a three-year period. Star and Ruhleder were particularly interested in addressing the relationship between the WCS infrastructural tool and organisational change. As they state 'who (or what) is changer and who changed'?

The work of Bateson (1978) is drawn on to provide a more formal guide to understand the development of the WCS. He identifies three levels in any communication systems, and these were adapted by Star and Ruhleder. Context is central to these levels. Understanding the relationship between them provides an insight into success or failure factors of communication systems. As Star and Ruhleder assert:

> As with Bateson's levels of communication or learning, the issues become less straightforward as contexts change. This is not an idealization process (i.e. they are not less material and more 'mental') nor even essentially one of scope (some widespread issues may be first order), but rather questions of *context*. Level one statements appear in our study: 'Unix may be used to run WCS'. These statements are of a different character than a level two statement such as 'A system developer may say Unix can be used here, but they don't understand our support situation'. At the third level, the context widens to include theories of technical culture: 'Unix users are evil – we are Mac people'. As these levels appear in developer-user communication, the nature of the gulfs between levels is important (Star and Ruhleder, 1996, p. 117).

There were a number of first-order issues identified by Star and Ruhleder. These included information problems experienced by potential users who needed to find out about the system, its installation and uses. Of those already 'on-line', some faced physical and temporal access restrictions to the system. For others computer literacy was a problem, compounded by a lack of training.

Second-order issues were the result of unforeseeable contextual effects or first order issues combining. The latter necessitates the context of evaluation to be widened. So for example, first order issues of which computer to purchase and how to get the systems running was dependent to a large extent on second order issues. This relationship is evident in terms of user preference. Hence, while the operating system for WCS was UNIX-based, most of the biologists were more comfortable with using Mac computers. Unfortunately for the geneticists, most of the computer scientists who were in charge of IT support in the university environments were also UNIX 'people'.

Third-order issues have the widest context and are present in all scientific communities, given their interdiscipinary nature, their different approaches and their different histories. This plurality impacted on the WCS. Different geneticists with different backgrounds wanted different types of information, something which WCS found difficult to accommodate. However, the flip-side of this - i.e. aligning the WCS to a particular sub-category of work - would have erected barriers to other users. The biologists were also concerned about the 'competition' and issues of 'privacy' when it came to sharing information via the WCS. For some, it posed the threat of becoming a negative externality. In other words, as the tool developed and became central to the community, those labs which did not have access would suffer and be left behind.

IS strategy and management is yet another area in which the ethnographic research approach has been used (Davies, 1991; Davies and Nielsen, 1992). Davies, for example, in her study of the British Army assessed the feasiblity of a theoretical model (drawing on structuration theory) in addressing organisational culture. In particular, Davies is interested in examining the relationship between organisational culture and its implications for IS strategy. Given this, the Army's culture is addressed with regard to their strategy for 'the organisational computing requirements in the 1990s and beyond'.

Davies identified a number of cultural issues with potential consequences for strategy. Of relevance was the degree of importance given by Army personnel to the issue of computing. The latter was considered by many to be of a low priority owing to its affiliation with 'service' activities. These activities on the whole were again seen to be of less importance when compared to the 'fighting' sections. This prejudicial bias was also reflected in the manner by which monies were allocated in the Army. As Davies states:

> ...the internal prejudices of factions within the organisation influence the way budgets are distributed. These prejudices directly link to the belief that those who are in the fighting corps should get money whilst those in the service corps should

> have to put forward stronger cases for financial support. This is noted as 'teeth' corps – at the battle face – and 'tail' corps at the support edge.
> (Davies, 1991, p. 158)

At a socio-structural level, conflicts between the Army as a 'family' and a soldier's own family, were apparent. The support for the Army as an institution from wives and children was assumed as forthcoming, despite the fact that consideration of relative divorce rates (the Army rate was higher than external rates) might have appeared to question this. Despite the Army strategy advocating the need for IT personnel, some of those who were already trained in the requisite skills, viewed the increasing demand from the private sector for such skills as a possible way out, and a means to end the conflict between the two families.

The possible attrition as a consequence of the above was compounded by structural restrictions which made recruitment difficult. Levels of entry and the associated pay increments could not match those of the private sector. With regard to salary we can see how this problem relates back to the prejudicial bias in the allocation of funds.

4.2.2 Contributions

Through this review of IS literature, it has hopefully been demonstrated how ethnography provides a rigorous approach with regard to examining the organisational context of IS practices. Considerable insight into human, social and organisational aspects of IS is offered by the ethnographic method (Harvey and Myers, 1995). Another attraction of the ethnographic approach is that it allows for an appreciation of practices in the real-world setting. This further allows issues to be addressed and frameworks to be developed, aiding both practitioners and researchers. The ability to study practices in their natural setting also avoids having to construct artificial settings for quasi-experimental research.

Ethnographic findings can, in addition, be used to question assumptions, derived on the whole from experimental based studies (Harvey and Myers, 1995). For example, Hughes *et al*'s, (1992) research into systems design questioned widespread assumptions about the process. Their findings enabled a greater understanding of the subject domain, and concluded that accepted 'good design' principles were at times unsuitable when applied to cooperative systems.

The real world setting addressed by ethnography additionally enables an appreciation of the complexity of organisations in terms of their political nature. Canvassing the views of different stakeholders can provide deep insight into points of conflict, which other research methods may fail to uncover.

Finally, ethnographers in a real-world setting are able to pursue avenues of interest, thrown-up in the context. Zuboff (1988) describes how in her research, 'windows of opportunity' opened up potential lines of fruitful study, including where 'people who are working with technology for the first time were ripe with questions and insight regarding the distinct qualities of their experience' (Zuboff, 1988, p.13).

4.2.3 Limitations

Despite the potential benefits, ethnography has been criticised on a number of levels. The major criticism is that, given the privileging of local knowledge and the associated in-depth knowledge of specific contexts and situations, how is generalisable knowledge possible? Here we witness how epistemological issues come to the fore when contemplating the goals of a research project. The issue is addressed by Walsham (1995a) in his discussion of Geertz's study of Jews, Berbers, and the French of Morocco in 1912, which attempted to provide an interpretation in the form of a 'consultable record' (Geertz, 1973). Walsham argues that the goal of Geertz was not the generation of social laws or truths, concluding that Geertz's interpretive approach can clearly be distinguished from the positivist tradition. Although interpretive work can be the basis for generalisations, Walsham maintains that the nature of such generalisations is different per the two traditions. Statistical generalisation is not the goal of interpretive research. This would limit the scope of such research (Walsham, 1993). Instead, benefits can be accrued by generalising at four levels (Walsham, 1995a). The first refers to the development of concepts. Citing the work of Zuboff (1988), Walsham illustrates how she used her ethnographic studies of IT use in American organisations to develop the concept of 'informate'. Extending this example, Walsham indicates how the 'informate' concept can act as a part of a group of propositions, world-views, and concepts, which help to form theories. This generation of theory forms the second generalisation. The drawing of specific implications relating to particular 'domains of action' form the third generalisation. The fourth refers to what Walsham describes as 'rich insight', gained by the reading of other research studies. Such insights, though not easily pigeon-holed as concepts, theories, or implications, may prove equally valuable to the reader, hence, the phrase 'rich-insight'.

Some of the issues discussed by Walsham (1995a) with regard to generalisation are touched on by Golden-Biddle and Locke (1993) in their paper *Appealing Work: An Investigation of how Ethnographic Texts Convince.* They describe the problems of 'legitimating the atypical'. In other words, attempting to secure against an ethnographic text being perceived as 'overly peculiar' and too 'distant' by the reader. To overcome such barriers, Golden-Biddle and Locke cite the strategy of discussing in the text 'common experiences' and 'broader categories', which appeal to and connect with the reader. They cite Adler and Adler (1988) whose ethnographic study of a university basketball team, centres on the issue of loyalty. In an attempt to legitimate the atypical, the authors locate the basketball team as part of a family of similar organisations, and through a discussion of loyalty, describe a concept common to all of them. As they state:

> ...we still know very little about the development of intense loyalty towards organisations (such as Jonestown) or as might be expected for organizations in which members are highly interdependent and in which performance might require unswerving commitments from members. Example of such organization might be combat units, complex and intensive surgical teams, astronaut work groups and high-performing athletic teams, to name but a few.
> (Adler and Adler, 1988, pp. 401- 402)

This attempt to highlight common frames of reference is evident in the Wagner article cited earlier. As she argues:

> Although the social setting of a surgery clinic has given the 'ethical scenarios' of a specific colour, some of the experiences and conclusions are transferable to other problems and organizations. The conflicts addressed here are likely to

> emerge in organizations that depend on a sharing of resources (such as time, personnel, rooms, material), and in which some members enjoy a high degree of time autonomy and decision-making power than the others.
> (Wagner, 1993, p. 100)

At another level IS ethnographic research has been criticised for failing adequately to address the social and historical contexts in which technological developments take place. As noted earlier, this type of criticism was levelled at ethnography's mother discipline, leading to reflection as to the very nature of anthropology. This further led to a concern as to how looking into the past could produce a greater understanding of the present. Tinker (1998) critiques recent AIS ethnographies in three ways. First he argues that they have a myopic perception of 'conflict', addressing it solely at an intra-firm (and often at an interpersonal) level. Consideration of technology as a tool for capital accumulation, and its potential impact - and conflict with labour relations through revolutions in the labour process - 'never enters the picture'.

Secondly, Tinker argues that the AIS ethnographies privilege the 'actor's subjectivity' at the expense of the ethnographer's perspective, leading to what he describes as 'Hamlet without the Prince'. Consequently, by negating the ethnographer's voice, the ability to question the efficacy of technological change is nullified.

The final point relates to the perception of IS history by ethnographers. Viewing it as a 'history of ideas', as opposed to a 'history of social life, work, and technology' recent AIS ethnographies fail to consider lessons from history and their implications for present day developments in AIS. Tinker concludes by arguing that:

> The larger picture is, in part, a historical one that recognises that the current innovations in AIS are not virgin experience but belong to a long lineage of events. The commidification and recommodification of work did not end in the eighteenth century with English cotton, silk and wool workers. Capitalism is 'the unfinished revolution' that continues today with upheavals in the work practices of printers, airline employees, nurses, doctors, teachers, lawyers, accountants, university employees, managers etc ... If ethnographers are to be more than technology's cheerleaders (humanistic or otherwise) they need to give more balanced consideration the impact of their discipline (Tinker, 1998, pp. 24-25).

A final point to be made refers to the length of time needed to conduct an ethnography. As briefly mentioned, this form of research is extremely time intensive and even more so if the process of negotiating access to an organisation is taken into account. It is perhaps best to consider this last point not as a criticism, more as a limitation and the need to consider the pragmatic implications when ethnographic research is proposed.

4.2.4 Reasons for Adopting an Ethnographic Approach

While acknowledging these criticisms, this research can be couched within the ethnographic tradition. More precisely it can be defined as an ethnography based solely on the use of documents as its source of data. The reasons for adopting an ethnographic approach will now be examined followed by a discussion of why a document-based approach was deemed suitable for this body of research.

Orun *et al.* (1991), assert that a lot of quantitative work in the social sciences deals with brief survey questions and answers, and large numbers of what are described as 'disconnected respondents'. One consequence of this is that the 'flesh' and 'bones' of the 'everyday lifeworld' are removed from the research. Smith (1989) argues for the use of appropriate research methods when addressing particular research problems. Or as he describes it 'horses for courses'. Given these views, it is important to consider a suitable approach for the current research. As stated earlier, a growing number of writers in the IS security field assert the need for security to be addressed from a socio-technical perspective (Dhillon and Backhouse, 1996; Willison, 2000a). Backhouse, (1997) for example, when discussing the security domain argues that:

> ... when protecting information, we need to go beyond the technical components to regard the whole ensemble of computers, data and social context as part of what needs to be secured (Backhouse, 1997, p. 33).

A research approach is thus required that respects this perspective and affords the ability to view security practices in a holistic manner. For the majority of organisations, security practices are an inherent part of their everyday working life. An appreciation of these practices (and the associated safeguards) and the interrelationships between them is vital for understanding the IS security domain.

Consequently, particular aspects of security cannot be studied in isolation given their ramifications and impact on other areas.

The ethnographic approach, therefore seems a suitable research approach for the following reasons. First, it allows for a holistic perspective of an organisation to be achieved, or what Creswell describes as a 'cultural portrait' of a group. Insight into the human, social and organisational aspects of an IS are afforded, which mirrors the socio-technical approach. Secondly, an appreciation of working practices in a real-world setting is allowed for. This is in keeping with the assertion that security practices cannot be studied in isolation due to their interrelated nature and their intertwined relationship with working practices. Thirdly, multiple-perspectives, underpinned by the principle of 'thick description' allow for a consideration of potential areas of conflict, ambiguity and mis-understandings.

4.2.5 Document-Based Ethnographic Approach

The reasons for adopting a document-based ethnography are driven by pragmatic criteria and inspired by the methodology of existing literature in the fields of anthropology and ethnography. A mitigating factor that works against gaining access to an organisation is the nature of security research. Achieving access to organisations is difficult enough, but when the research encompasses security issues, the task is made even harder. Companies are particularly sensitive about security matters, especially in terms of how adverse publicity can affect their public reputation. As a consequence, they rather ironically see research of such a nature as a risk in its own right. A document-based ethnography can be seen as a pro-active solution to the challenge of access. To support such an approach, it has been shown that there is an existing body of academic research that advocates, and in doing so, legitimates the methods promoted in this research.

Furthermore, it is important to consider the potential contribution of this method to the IS field. A good starting point is to view the document-based ethnography as a response to Markus and Lee's (1999) call to move beyond the methodological 'tennis' (Scott, 2000) played by competing opponents (positivist v interpretive advocates) and concentrate on the development of what they term 'intensive' research. This research should be viewed as a positive scholarly contribution to this development.

In a recent paper, Scott (2000) drawing on the work of Wieck (1983), cites how 'scholarship' can be stifled due to its dialectic relationship with community. Wieck argues that while there is a need for both 'community' and 'scholarship' to enable a community of scholars to exist and develop, there are potential dangers from both factions. First, although community can support scholarship, it can also smother it. Secondly, scholarship, by emphasising its originality, mitigates against community. Scott argues for a balance to enable original contributions to be allowed into the IS discourse so potential benefits may be shared by the IS community.

Failure to consider new methods such as the one proposed here, could lead to methodological stagnation, and an inward facing stance where legitimacy is achieved through the 'tried' and 'tested' at the expense of the new. With regard to the status quo, Scott argues:

> It is suggested that as members of a 'community of scholars' we may have dampened our experiences and settled for reverse engineered, sanitised methodologies, rather than run the risk that our colleagues might deny us legitimacy on the grounds of either 'method' or 'truth' (Scott, 2000, p. 2).

The research reported here may be viewed as a distinctive contribution and an attempt to advance this methodological practice in the IS field.

4.3 Data Collection and Analysis

4.3.1 Data Sources

Three types of document were used as sources of data for constructing an account of the collapse of Barings Bank. The first was a report especially commissioned by the then Government and undertaken by the Bank of England into the events that led to the downfall of the financial institution. Newspaper articles, ranging from late February 1995 to June 2000 formed the second source of information on Barings. The final types of documents used were books. These were either directly related to the topic (i.e. books about Barings) or indirectly related (i.e. books explaining share trading). Each of these three forms will now be discussed in greater detail.

Barings Report

On the 26th February 1995, the High Court appointed joint administrators to manage the affairs of Barings plc, the parent company of the Barings Group. The following day, the then Chancellor of the Exchequer, Kenneth Clarke QC MP, announced that the Board of Banking Supervision (BoBS), which formed part of the Bank of England (BoE), had been commissioned to write a report in order:

> To establish in detail the events that led to the collapse of Barings: to identify the lessons to be drawn, for institutions, for the Bank's own regulatory and supervisory arrangements, and for the UK system of regulation more generally; and to report to the Chancellor of the Exchequer (BoBS, 1995, p. 1).

The BoBS subsequently reported back on the 13th July, 1995 with a 337 page document entitled, *Report of the Board of Banking Supervision Inquiry into the Circumstances of the Collapse of Barings* (1995). The report is split into two parts. The first part, encompassing sections one to thirteen, covers the events that led to the fall of the bank. The second part, section fourteen, discusses lessons to be learnt.

The full table of contents covers the following chapters:

1. Introduction.
2. Creation and management of Baring Investment Bank (1992-1995).
3. Authorised trading activities on Singaporean and Japanese futures exchanges and relationships with third party customers.
4. Unauthorised trading activities conducted by Barings Futures (Singapore) Pte Limited and their effect.
5. Concealment of trading activities in Baring Futures (Singapore) Pte Limited.
6. Funding of Baring Futures (Singapore) Pte Limited.
7. Internal controls.
8. Impact of unauthorised trading activities on financial reporting of Barings plc.
9. Internal Audit.
10. External Audit.

11. Reporting by Barings to supervisors and regulators.
12. Supervisors and regulators.
13. Conclusions.
14. Lessons arising from the collapse of Barings.
(BoBS, 1995, pp. II)

The report itself takes up 264 pages. The appendix constitutes the remaining section, covering the list of interviewees, glossary, abbreviations, etc. The report acted as one of the two primary sources of secondary data.

Books

The books used to derive an account can be divided into two types. On the one hand are the books that directly address the subject matter i.e., the collapse of Barings; on the other, those that indirectly aid an understanding of the collapse. Of the first category, there were a number of books which could have been used to help construct and account, including *Barings Lost* (Hunt and Heinrich, 1996) and *Rogue Trader* (Leeson and Whitley, 1996). However, *The Collapse of Barings* (Fay, 1996) was chosen to act as the second primary source of data for the following reasons. First, the book drew heavily on the BoBS report, and hence worked well as a complementary source of data. Secondly, compared to the BoBS, the book provided a more in-depth historical account of Baring's business activities. Thirdly, the book afforded a greater insight into the nature of, and relationships between, those people implicated in the collapse. The themes covered in points two and three helped the author to develop a much more contextualised ethnographic account. The BoBS report verged on the over formal and was at times quite dry. Stephen Fay's book acted as a useful counterbalance.

Although other books were available, after initial consultation, they were ignored. The BoBS report and The Collapse of Barings provided more than enough data to work with. Additionally, the researcher was concerned about reaching the point where the wood could not be seen for the trees. Each book on Barings approached the collapse from a different perspective, a different level of analysis or both. Given the nature of business and the number of parties involved, it is perhaps not surprising to learn that the fall of Barings proved to be a fairly complex case study. And, while there was a considerable degree of overlap between the BoBS report and Stephen Fay's account, this was not the case with the other books. The researcher felt that reading additional texts, each with their differing positions, would ultimately lead to confusion when attempting to understand the events that led to the downfall.

The second type of book was in fact used to enhance an understanding, albeit indirectly, of the collapse. The BoBS report does assume *a priori* knowledge of banking practices, and while *The Collapse of Barings* proved more accessible, additional material was drawn on to aid understanding of banking practices. Hence, the text, *Options, Futures, and Other Derivatives* (Hull, 1997) acted as an invaluable reference source.

Newspaper Articles

Fortunately for the author, his university library provided access to CD roms covering English broadsheet newspapers and business magazines. *The Guardian*, *The Independent*, and *The Financial Times* were chosen as suitable publications to form the basis for a literature search.

Before we discuss data analysis, it is worth describing the relationship between the researcher and the texts that constituted the data sources. The intention here is to illustrate that the use of written sources does not mean that the subsequent work based on them (i.e. the ethnographic account of the fall of Barings and the discussion and analysis chapter) is limited by definitive and static meanings that reside in an author's text, and merely allow a reader to assimilate these meanings and regurgitate them parrot fashion.

Indeed, as Boland (1991) argues when discussing the work of Paul Ricoeur:

> He further helps us break the traditional notion that a text represents some well formed idea of its author and that we should try to recover this original meaning through interpretation (Boland, 1991, p. 444).

Ricoeur (1981) argues that there is no need to make reference to the intention of the author, the originally intended audience of the text, or the originating culture.

Through the concept of distanciation, Ricoeur asserts how an intended meaning that writers may hold becomes separated from them in the production of their text. Consequently, when people read the author's text, they themselves actively interpret the material by disclosing meaning in the text. The notion of intransigent meanings associated with a text therefore becomes irrelevant, as the text is made available to the interpretations of readers. Hence there are no definitive meanings produced by an author waiting for assimilation by readers, rather the meaning is disclosed in the process of reading.

There exists a position of asymmetry between a text and the reader. In other words, given that the reader actively discloses meaning to a text through interpretation, the text attains a level of distance (hence the term distanciation) from the author, because different readers of the same text will not necessarily interpret the same meanings the author intended (Ricoeur, 1976). The position of asymmetry emerges therefore owing to the difference in experiences brought to the reading process by different individuals.

Through reading an individual 'appropriates' the text and 'actualises' the meaning. The concept of appropriation further examines the relationship between the author, the text and the reader. Ricoeur (1981) refers to the concept of the non-ostensive reference when discussing this relationship. Lee (1994a) explains this concept by way of example. He first cites how Euclidean geometry, does not, in a physical sense, exist in nature. Rather it may be understood as a fiction. While people who may carry knowledge of this form of geometry in their heads may 'come and go', Euclidean geometry persists. Hence, like a physical object, its form is maintained across different individuals who experience it. Consequently, it can be seen as an objective social reality. Given this Lee explains:

> Furthermore, suppose I am reading a Euclidean research paper. Its meaning is not restricted to the Euclidean argument that its author is making, but also involves the entire socially constructed apparatus that comprises Euclidean geometry – its axioms, theorems, symbols, and logic, all of which transcend what is in the paper and all of which were in existence prior to the writing of the paper. The paper itself is just one possible manifestation or artifact of this apparatus. Upon grasping this socially constructed reality (the paper's non-ostensive reference), I

> become Euclidean myself and I become able to identify inconsistencies and suggest improvements in the paper ... This refers back to Ricoeur's notion of appropriation, which is taken a step further: not only can I appropriate the text or what the author had in mind, but also, the text and the socially constructed world behind it can appropriate me (Lee, 1994a, p. 150).

Hence, even though different readers may bring to the process of reading their own different socially constructed worlds (in my case influenced by criminology), the text will only become meaningful if there is a socially constructed world behind it.

Lee (1994a) gives another example of an office manager reading an e-mail sent by a subordinate about problematic office politics. Through an understanding of the socially constructed world behind the e-mail i.e. the organisation, the office manager who reads the text may have an even better understanding of the problems (the office politics) than the subordinate who wrote it.

As regards the current research, the researcher appropriated the socially constructed world of the banking industry and the activities of Barings bank. Through reading and appropriation, an understanding of the socially constructed world prevailed. Each source of data led to appropriation and increasing insight into the socially constructed world i.e. the non-ostensive reference, which underpins the texts themselves.

4.3.2 Data Analysis

Discussing data collection and data analysis as two phases in the research process can be seen as something of an artificial distinction with regard to ethnographies. Rather their relationship can be seen more as symbiotic. With traditional ethnographies, analysis begins when the researcher enters the field to collect data. The same can be said for the current study. While the researcher did not enter the field, as such, it could easily be argued that analytical processes were at work in the very early stages of data collection e.g. in regard to which books to consult. The next few paragraphs illustrate the interim analytical practices (Scott, 2000) that were used to produce a working body of material from which the ethnographic account of the fall of Baring was produced. The analytical practices are discussed with regard to the three types of data sources.

The BoBS report

With regard to the BoBS report, each chapter of the report was read several times. During each reading sections of the particular chapter were highlighted for the purpose of note taking. After the numerous readings, notes were entered into a word processing file and categorised as per the BoBS text. For example, per the report, the second paragraph of the second chapter would be denoted as section 2.2. Consequently any notes made about that section would also be categorised 2.2. This made sense, given that any ambiguity in my own notes could easily and quickly be checked to the original source. Any notes that were made were typed directly from the original text. Putting the text into the author's own words would have simply taken too long. Sections of a specific part of the report which were deemed to be of particular interest were emboldened as the following example illustrates:

> 2.40 The fact that Leeson was permitted to have first line responsibility for both trading and settlements meant that a crucial ingredient in the matrix organisation of local integrity was absent in BFS. **Therefore, management control was ineffective, in that management believed and relied upon the risk and performance information generated by transactions processed in BFS, apparently without independent investigation (other than might be carried out during the annual external audit), until the internal audit of August 1994.** Although this internal audit failed to identify the unauthorised activities of Leeson, it did highlight the lack of division of responsibilities between trading and settlements; but this fundamental weakness in internal controls was not rectified (BoBS, 1995, p. 26).

Where necessary additional entries were made (signified by N.B.) into the researcher's notes, to aid an understanding of the issues e.g.:

> 2.43 The equity derivatives business comprised the over-the-counter (OTC) proprietary derivatives trading activity in London and the proprietary exchange traded activities businesses in Tokyo and Hong Kong. During what he described as "due diligence" of this business Ron Baker established that within the proprietary volatility book managed by the Tokyo traders was a "switching activity" conducted on behalf of BSJ by **BFS**, which apparently produced, in his estimate, some 65% of the revenues generated by the volatility book. The 'switching' activity is described in Section 3 (BoBS, 1995, p. 27).

> **(N.B. From what I can gather so far, this switching activity is what created most of the losses).**

Making notes from the report helped the researcher to assimilate the information. Reading alone would not have provided a clear understanding of the issues addressed, primarily because of the sheer size of the report and the complexity of the subject matter. The practice of note taking further provided a mental time-out from reading and afforded room for reflection about the issues examined. Note-making also provided the researcher with a sense of achievement, when, after a day's work, several pages of word processing had been created, rather than simply several hours of reading. Importantly, the notes also provided a consultable record, which was referred back to when the ethnographic account was written.

Newspapers

As discussed, the researcher was fortunate to have access to on-line CD roms via his university library. The searches for each newspaper were conducted using the keywords 'Barings Bank'. This term was deliberately broad to enable a 'wide-net' approach, advocated by ethnographers, with regard to the initial stages of data collection (Fetterman, 1998). The search results were shown on-screen as a title and an abstract. If the article was deemed to be of interest, the full text could be easily retrieved. Selected articles were then 'cut and pasted' into a word-processing file for analysis. At this stage 'analysis' meant reading through the articles and further editing out those that were deemed to be of little interest. Certain criteria were adopted to aid this process. It should be pointed out that much of the newspaper coverage was concerned with events post the collapse of Barings e.g. the lengthy extradition process by the Singaporean government of Leeson from Germany, which was of no interest to the researcher.

While the papers did write at length about those factors that brought down the bank, they could not begin to provide the level of detail found in the BoBS report and Stephen Fay's account. Nevertheless, the newspaper articles were useful in a number of ways. First, they identified areas not directly addressed in the report, but whose inclusion would lead to a 'fuller' account. Secondly, for the sake of people reading them (and to the advantage of the author), the newspaper articles provided useful 'layman' accounts of quite complex business activities e.g. derivatives trading. After several rounds of editing down the material, a final body of articles from each newspaper was left. Like the BoBS report, during the editing down process, sections of an article which were thought to be of particular interest, were highlighted in bold text and N.B. notes were sometimes made at the start of an article to indicate its particular strength e.g. the history of derivatives trading.

Books

As with the BoBS report considerable time was spent making notes on *The Collapse of Barings* (Fay , 1996). Similar methods were used. Each chapter of the book was read several times, after which sections, which had been highlighted during this process, formed the basis for note-making. Again, like the BoBS report, specific sections were highlighted in bold text and where necessary N.B. notes were made.

> But the big players in the derivatives markets are no longer local traders, they are the **banks** and **securities** houses. They have clients, and executing clients' orders is part of their business, but they also trade with their own money. This is called **proprietary trading**, and the volume varies (Fay, 1996, p. 47).
>
> **N.B. Note the difference between 'banks' and 'securities' houses.**

Once again, the process of note making helped the researcher to assimilate the information, while providing a timely break from reading the text. As mentioned, the newspaper articles and notes made from the BoBS report and *The Collapse of Barings* were entered into word files. One remarkably effective, but equally simple method was often used to search through this data. This comprised a simple 'Ctrl+F' function. This instruction allowed the researcher to traverse a large body of data very quickly, and afforded the ability of cross-referencing between the three bodies of text.

4.4 Conclusion

The purpose of this chapter is to describe the research methods used in the study. The opening section examines the philosophical underpinnings of the research. An interpretive stance is taken in order to appreciate and afford an insight into the social reality that prevails in the workings of an IS. This position is underpinned by the view that IS are not just merely computer systems, but computer systems embedded in a social context. An appreciation of the social context is equally important when considering IS security. A number of writers have argued that if we are to understand the true nature of security problems that IS face, we must be able to examine the whole of the problems and view IS from a social-technical perspective.

As a complement to the interpretive position taken in this research, an ethnographic approach was adopted for the following reasons. First it allows for an holistic perspective of an organisation to be achieved, which mirrors the security perspective advanced in this research. Secondly, it allows for an appreciation of working practices in a real-world setting. Thirdly, multiple-perspectives, underpinned by the principle of 'thick description', allow for a consideration of potential areas of conflict, ambiguity and mis-understanding.

The document-based ethnography adopted for the current research can be viewed as a pro-active solution to the challenge of access to field research. Such an approach is inspired by developments in the field of anthropology and ethnography, which afford an existing body of literature that advocates and by doing so legitimates the methods used in the research. This approach can be seen as a positive scholarly contribution to the field and a response to Markus and Lee's (1999) call to concentrate on the development of 'intensive research'.

In the 'Data Collection and Analysis' section of the chapter, the sources of text used in the research are described. These sources include the BoBS report, books and newspaper articles. In keeping with the interpretive stance and drawing on the work of Ricoeur (1976, 1981) this section of the chapter discusses how the use of written sources does not imply that the work based on them is limited by definitive and static meaning that reside in an author's text, so allowing only for a regurgitation of those meaning in a parrot like fashion. Rather, each individual reading a text, actively interprets the material by disclosing for themselves meaning in the text.

Chapter Five: Empirical Material

On the 26th February administrators were appointed by the High Court in London to manage the affairs of Barings plc. following the identification of substantial losses incurred by a related overseas subsidiary known as Baring Futures Singapore. The purpose of this chapter is to examine those factors that were instrumental in the collapse of Barings. The first part of the chapter provides a brief history and background to the development of Barings bank. Part of this history encompasses the deregulation of the London Stock Exchange, the so-called Big Bang. In the run up to deregulation, Barings made a modest purchase of a fifteen man trading team which formed the basis of Baring Securities Limited. Although the aforementioned represented Barings' first venture into securities trading, it was to have a profoundly negative impact on the banking activities of Baring Brothers & Co. Section two examines the development of Baring Securities Limited and its volatile relationship with its banking counterpart. This is followed by a focus on the establishment of Baring Investment Bank which came about through the merger of Baring Securities Limited and Baring Brothers and Co. in an attempt to quell the ill-feeling between the two groups.

During the expansion of Baring Securities Limited one of the many subsidiaries opened was Baring Futures Singapore. The fourth part of the chapter examines Baring Futures Singapore's inception and management. Leeson was a key figure in the Far East subsidiary. Specific attention is given to the confusion over job responsibilities and the associated management lines of reporting. The chapter then moves on to address the authorised trading activities on the Singaporean and Japanese exchanges followed by, in section six, the considerable unauthorised trading conducted by Leeson on SIMEX, the Singaporean Exchange. Part seven considers the methods used to conceal his unauthorised trading, followed by an examination of the failings in the control environment which allowed Leeson to draw heavily on the capital base of Baring Securities Limited to fund his illegal activities. Section nine of the chapter addresses how Leeson was in a position to actually undertake the unauthorised trading, through the failings of internal controls at all levels and involving a number of Barings' companies. The internal and external audits of Baring Futures Singapore are discussed in section ten and eleven respectively, with the penultimate part of the chapter highlighting the supervision of the relevant Baring companies by the Bank of England and the Securities Futures Authority. The chapter ends with a summary of the main points raised.

5.1 Factors in the Collapse of Barings Bank

5.1.1 Brief History and Background of Barings Bank

Prior to its collapse, Baring Brothers & Co. had been the oldest merchant bank in the City's square mile. Founded initially as a partnership in 1762, the bank had managed to remain independent and privately controlled. After a near fatal business venture in Argentina, Baring Brothers & Co. was established in 1890 to succeed the partnership. In 1985 the share capital of Baring Brothers & Co. was acquired by Barings plc, which became the parent company of the Barings Group. Apart from Baring Brothers & Co., the other two principal operating companies of Barings plc were Baring Securities Limited (see section 2) and Baring Asset Management, which played no part in the collapse (and hence will not be referred to again in this account).

It was during John Barings' reign as chairman of Barings plc. (1971-1988), that significant changes occurred in the banking world. These changes had a profound impact on Barings. In 1983 the London Stock Exchange struck a deal with the Conservative Government to relax the rules relating to ownership of the securities firms which traded on the Exchange. Restrictive practices, in the form of the Exchange rule book denying majority (let alone whole) ownership of member firms by non-member firms, had traditionally ensured a segregation between the securities houses and the banks. The agreement between the Government and the London Stock Exchange effectively brought this segregation to an end. A three-year grace period was decided on, allowing the Exchange time to implement the necessary changes, which would culminate in the Big Bang of 1986.

In anticipation of these changes, there was a period of frenzied business activity, which saw the sell-out, merger, or auction of the Exchange firms to their counterparts, but, more importantly, to non-member firms. Perhaps not surprisingly, many of these non-member firms were banks. Indeed, many of the deals had an international flavour to them. Banks from the US (Citicorp, Chase Manhattan, Merrill Lynch), Canada (Canadian Imperial Bank of Commerce, Orion Royal Bank), Hong Kong (HSBC), Switzerland (Union Bank of Switzerland, Credit Suisse, Bank Centrade) France (Credit Commercial de France, Paribas) and Ireland (National and City, FBD Insurance) were just some of the international participants.

Barings response was reserved. Unwilling to take part in the frenetic scramble, the one purchase it did make was indeed minor, compared with some of the deals characterising this period. For the price of £6 million Barings purchased, from the stockbrokers Henderson and Crosthwaite, a fifteen-man dealing and research team which specialised in Far East securities. Headed by Christopher Heath, this group, which became known as Baring Securities Limited, was instrumental in shaping a new Barings culture, the ramifications of which were felt up to the collapse. Aside from the traditional business activities carried out by Baring Brothers & Co., Baring Securities Limited represented Barings first involvement in the securities business. The background and development of Baring Securities Limited and its uneasy relationship with Baring Brothers & Co. will now be traced.

5.1.2 Baring Securities Limited

The head of Baring Securities Limited, Christopher Heath, began his career as a stockbroker for Henderson Crosthwaite in the 1970s. His specialism was Far East securities, and when the Japanese stock market bottomed out in 1973-74 as a result of the oil crisis, Heath advised fund mangers to invest heavily in Japanese securities. His advice was sagacious, based on a detailed knowledge of the floated companies, which he himself would visit and report on. The sound advice produced sound rewards and by the 1980s Heath was responsible for approximately 65% of Henderson Crosthwaite's profits. The performance of Heath's team did not go unnoticed by one of its largest clients, Barings. After protracted negotiations, Barings were able to persuade Heath and his colleagues to leave Henderson Crosthwaite in 1984 and start afresh as Baring Securities Limited.

Baring Securities Limited's business empire expanded rapidly. New offices were opened in 1985 (Tokyo and Hong Kong), 1986 (New York), 1987 (Frankfurt and Singapore), 1988 (Geneva, Los Angeles, Melbourne, Sydney, T'ai-Pei, and Bangkok) and 1989 (Osaka, Kuala Lumpur, Manila, Jakarta, Paris, Karachi, and Seoul). Hence, in the first five years of business Baring Securities Limited opened nineteen offices. One office worthy a special mention, which housed key personnel implicated in the collapse of Barings, was Baring Securities Singapore. This Baring Securities Limited subsidiary was followed some five years later by Baring Futures Singapore. Like Baring Securities Singapore, Baring Futures Singapore employed personnel who played a role in the downfall. Indeed, one of the staff on Baring Futures Singapore's books was Nick Leeson.

Company profits also reflected the expansion of Baring Securities Limited. Sir John Baring in the annual report of 1985 stated: 'I am happy to say that the results of the first eighteen months have greatly exceeded our expectations'. They also exceeded Heath's. The eighteen-month profits were initially calculated to be achievable in the first seven years of Baring Securities Limited's business. The following two years' profits (1986-1987) merited further praise by Sir John in the respective annual reports; and in 1988 he announced that Baring Securities Limited had been awarded the Queen's Award for Export.

The formation of Baring Securities Limited, and its business activities and subsequent success, did, however, create major unrest in the Barings Group as a whole. To understand why, it is worth examining the differences in the types of business conducted by Baring Brothers & Co. and Baring Securities Limited, as well as the people who worked for the respective groups. Banking and securities trading essentially hold different philosophies and strategies with regard to profit accumulation. As Andrew Tuckey (who at the time was Chairman of Baring Brothers & Co. and later Chairman of Baring Investment Bank - see section three), a key figure in the collapse, explains:

> I knew that their culture [Baring Securities Limited] was different, as indeed brokers are generally from corporate financiers [i.e. bankers] anywhere you find them in an organisation. I saw that difference...in time scale. Everything in the broker's world is today and tomorrow ... whereas when you talk to a corporate financier person he is interested in what his clients are going to be doing next year (BoBs, 1995, p.21).

This assertion was supported by Andrew Bayliss (Vice-Chairman of Baring Securities Limited), who argued:

> It wasn't so much an intellectual failure as a psychological one. It was a matter of differences in attitude between bankers and brokers. Broking is essentially a short-term activity, and brokers are more gung-ho, wanting to get something done today. The banker is, by nature, more cautious, more measured, more conservative (Fay, 1996, p. 32).

These business differences acted as a source of tension between the two groups leading to an 'us' versus 'them' mentality. This tension was compounded by the respective profits and subsequent bonuses of Baring Securities Limited and Baring Brothers & Co. With the phenomenal growth of Baring Securities Limited, the brokers fared much better than their banking counterparts, who were well aware of this. The bonus system is central to the securities business. In some respects the profits acquired through such business can be seen very much as a means to an end, with the 'end' in this case being bonuses. Baring Securities Limited was no exception, and the bonus system was seen as sacrosanct. Any attempt to change or interfere with the allocation of profits to the bonus fund was met with fierce resistance from the securities staff, who were driven by the goal of their yearly bonus in their day-to-day activities.

One other notable area of divergence between Baring Securities Limited and Baring Brothers & Co. was their management systems. Though nineteen offices opened in the first five years of Baring Securities Limited's operations, the requisite control environments had not correspondingly developed. This did not bode well for the running of the overseas operations, one of which was Baring Futures Singapore, the subsidiary in which Nick Leeson worked. Andrew Bayliss asserts:

> We had grown very rapidly, and it is an utterly fair criticism that our management and control structure had probably not evolved at the same rate as the business. We still believed as though we were a small firm, and had fingers in too many pies (Fay, 1996, p. 60).

Another adverse affect of rapid growth was the strain it placed on Baring Securities Limited's capital base. With business on the ascent, this was not such a worry for Heath, but the Japanese stock market boom, which had lasted for fifteen years, came to an end. In January 1990, the market suffered severe falls and two months later it collapsed. Profits from commissions fell, while still leaving overheads to be paid. By 1991, there were twenty-one Baring Securities Limited's subsidiary offices in nineteen countries, with an accumulated staff of over 1300. This was far from the figure of fifteen staff which Heath had brought with him from Henderson Crosthwaite. These staff had grown used to the large bonuses, which, as discussed, they perceived as sacrosanct. Any attempt to deprive employees of their bonuses would simply have meant the exodus of staff to their competitors. Yet it was this very bonus system which had led to the relative paucity of capital with which Baring Securities Limited could conduct business. Rather than ploughing profits back into the business, they were used to pay staff large bonuses.

Yet clients were voicing their concern about Baring Securities Limited's capital base, listed in the company's balance sheet. In an attempt to stabilise the situation, a related company called Baring Securities International Holdings Ltd took out short-term bank loans to subsidise the subsidiary offices. The problem with this was that there was always the associated worry that the lending banks, which reviewed the short-term loans on an annual basis, would call them in. Baring Securities Limited further recognised that using short-term loans to provide long-term capital could hardly be equated with sound business sense. The precarious position of Baring Singapore Limited was not helped by business profits - or rather the lack of them. Monthly losses were being reported in 1992.

The finance director of Baring Securities Limited, Ian Martin, calculated that a capital injection of £50-£60 million was required to stabilise the group's position. Senior management, however, were incensed when Baring Brothers & Co. spent £75 million on a 40% stake in Dhillon Read, an American investment house. This was seen by Heath and his colleagues as strategically inept.

With monthly losses occurring, Tuckey told Heath in June 1992 that capital would only be loaned to Baring Securities Limited if overheads were drastically reduced. A review of Baring Securities Limited's operations was subsequently undertaken by Richard Greer (a Baring Securities Limited Tokyo employee) and Peter Norris (who had recently returned from a senior Baring Brothers & Co. position in Asia). Norris believed that:

> By 1992 it [Baring Securities Limited] had become a deeply troubled and divided group, missing many of the management disciplines that you would expect to find in a multinational trading and broking operation (BoBS, 1995, p. 20).

The review recommended a 15% cut in staff, the closing or curtailing of certain business activities, delegation of management authority to a number of regional centres (Tokyo, Hong Kong, Singapore, and New York) and the imposition of stronger systems of control.

By accepting the capital loaned by Baring Brothers & Co., Baring Securities Limited lost its independence and a great number of staff on 26th September 1992, when the recommendations were implemented. Barings Securities was loaned £50 million by Baring Brothers & Co. to shore up its capital base. The loan was accompanied by senior staff changes, with Heath elevated to the position of Executive Chairman and Peter Norris assuming the position of Chief Operating Officer.

Their relationship was never amicable, and on Monday 24th March 1993 Heath was sacked. Norris assumed the position of Chief Executive Officer.

5.1.3 Creation and Management of Baring Investment Bank

Towards the end of 1992, Andrew Tuckey and Peter Baring, who had succeeded John Baring in 1988 as chairman of Barings plc., had come up with the idea of merging Baring Brothers & Co. with Baring Securities Limited. The hope was that by doing so, the obvious divergences between the two groups would be lessened, affording a business environment characterised by co-operation rather than conflict. This idea was met with approval from the board of directors in the second half of 1993 (following the sacking of Heath in March) and in December of that year Tuckey had issued a memorandum explaining the changes. He concluded by asserting:

> I am convinced that, by combining our merchant banking and securities businesses ... we shall be in a position to make the most of all the talents employed in the two businesses and of the opportunities which are now in front of us (BoBS, 1995, p. 21).

A new organisation called Baring Investment Bank was established. With Norris acting as CEO, the organisation encompassed four groups, these being the Equity Broking and Trading Group, the Bank Group, the Corporate Finance Group and the Emerging Markets and Corporate Finance Group. Of particular relevance to the account of the fall of Barings is the Bank Group headed by George Maclean, which further incorporated the Financial Products Group headed by Ron Baker.

The ensuing months, which witnessed the formation of Baring Investment Bank, unfortunately proved a difficult time for Barings. The brokers found it difficult to come to terms with the more bureaucratic and formal environment traditionally found in the realm of banking. As Maclean argues:

> I believe the seeds of this [the collapse] were sown when we went into Baring Securities Limited to bring the two companies together and made the assumption that the quality controls that we [Baring Brothers & Co.] had could quickly get installed there [Baring Securities Limited]. As it turns out, that appears not to be true (BoBS, 1995, p. 21).

Central to the restructuring of Baring Securities Limited, and later the formation of Baring Investment Bank, was the development of a matrix reporting structure. This method of management views profit responsibility to be the domain of bank products, while at the same time acknowledging the importance of local management in controlling the office infrastructure which includes systems, controls, accounting, settlements, and administration. The matrix system of management was deemed by senior Barings staff as essential to allowing the coordination of a bank's products (e.g., futures and options) on a global basis, with concurrent decentralised management at a local level. Norris describes this form of management as:

> Each of our business lines [was described] as global products which were the columns in the management structure, and each of our offices and regional centres as floors in the structure. Anybody who ran a business in any location related both to the person who managed that location and to the product manager who might be in the vicinity or who might be 10,000 miles away. It was only in that way that you could really ensure the integrity of the management process.
> (BoBS, 1995, p. 22)

For some members of Barings the matrix structure created ambiguity rather than clarity. Although Norris and Peter Baring perceived the reporting lines as perfectly clear, this was not a view shared by Maclean. Such ambiguity was to some extent reinforced by the failure to create and disseminate an organisational chart during the formation of Baring Investment Bank. In regard to reporting lines the BoBS report states:

> It appears from out interviews that reporting lines and responsibilities were not fully understood by a number of individuals especially concerning Financial Products Group, headed by Ron Baker, and Baring Futures Singapore of which Leeson was general manager (BoBS, 1995, p. 22).

5.1.4 Creation and Management of Baring Futures Singapore

The confusion over reporting lines thus did not stop at Baring Futures Singapore's door; rather it increased. Given the matrix structure of reporting lines used in Barings, the management structure of Baring Futures Singapore cannot be examined on a separate basis, but must also be considered with regard to those bank products traded under its name and on behalf of other Barings subsidiaries. Confusion was apparent over reporting lines in Baring Futures Singapore from its formation and it is to this period that we now turn.

As discussed, Baring Futures Singapore was one of the new offices that opened during the expansion of Baring Securities Limited, and was formed to specialise in exchange-traded futures and options (i.e. these were Baring Futures Singapore's bank products). More precisely, Baring Futures Singapore would execute client business on the Singaporean Stock Exchange (SIMEX) on behalf of Baring Securities Limited and Baring Securities Japan. This client business, also referred to as 'agency' business, was managed by Mike Killian (Head of Global Equity Futures and Options Sales) in Tokyo. Ideally Baring Futures Singapore would accumulate profits through commission charged to clients. It also made further economic sense, as Chase Manhattan had previously charged Baring Securities Limited and Baring Securities Japan for executing SIMEX trades on their behalf. With three new Baring Futures Singapore trading seats on the Singaporean exchange, the services of what was, after all, one of their competitors, were no longer required.

As Killian would be working closely with Baring Futures Singapore, he wanted a reliable figure who could speak fluent English and would have a sound knowledge of back office operations. Thus Nick Leeson was asked by Killian to apply for the post of settlements manager. Leeson had acquired the necessary experience through working in the settlements section of a Baring Securities Limited department, which specialised in Japanese futures and options. He accepted the offer, and his name, once submitted to the Management Committee, was approved.

Previously in 1987, Baring Securities had opened their first Singaporean office in the form of Baring Securities Singapore. The managing director of Baring Securities Singapore was James Bax. He oversaw a business which traded equities (but not derivatives) on SIMEX. Bax was extremely defensive of Baring Securities Singapore's business territory, but on the whole was well-regarded by the financial establishment in the Far East.

Bax's second-in-command was Simon Jones, who acted as the Chief Operating Officer of Baring Securities Singapore. This position included responsibility for the back office, which settled Baring Securities Singapore's equity trading. Jones' volatile temper was legendary, as were his disputes with other employees. He disliked dealing with the head office in London, and treated visiting Baring Securities Limited senior staff accordingly.

Although Bax was in charge of Baring Securities Singapore, he had little knowledge of settlements, and was therefore heavily dependent on Jones. This dependency was recognised by Jones, who, whenever office politics required it, relied on Bax to side with him. Hence, Bax and Jones had a close-knit working relationship, epitomised by the nickname 'Fortress Singapore', given to Baring Securities Singapore by Baring Securities Limited staff.

The opening of Baring Futures Singapore, however, was to create additional friction between head office and Bax and Jones. The initial major problems were a lack of consensus over who would manage Leeson, coupled with an equal failure to agree on his work responsibilities.

Leeson moved to Singapore in early March 1992. Despite the fact that Mike Killian had asked Leeson to run the back office (i.e., the settlements section) of Baring Futures Singapore, the picture began to blur when Ian Martin (Baring Securities Limited's Finance Director) sent a fax on the 24 March 1992 to Jones and Killian, stating that Leeson would:

> ... head up our SIMEX operation and also act as floor manager ... he will report to Simon Jones and Gordon Bowser (BoBS, 1995, p. 31).

At the time Bowser was in charge of future and options settlements in London. But what was remarkable about this fax was Martin effectively putting Leeson in charge of both front and back office operations. This was traditionally unheard of in the securities business, as one of the golden rules of management is that there should be a strict segregation of duties between trading and settlements. By putting Leeson in charge of these two businesses, Martin essentially negated the validity of the associated accounting controls.

This caused great concern for Bax, who firmly believed that Leeson had been appointed solely to run the settlements section of Baring Futures Singapore. His response was to send a memo to Andrew Fraser (Head of Equity Broking at Baring Securities Limited), which stated:

> My concern is that once again [reference to the previous problems experienced by Baring Securities Limited in Bangkok, Singapore, Kuala Lumpur, and Jakarta] we are in danger of setting up a structure which will subsequently prove disastrous and with which we will succeed in losing either a lot of money or client goodwill or both ... (BoBS, 1995, p. 31).

Bax further argued in the same memo:

> In my view it is critical that we should keep clear reporting lines and if this office is involved in SIMEX at all then [Nick Leeson] should report to Simon [Jones] and then be ultimately responsible for the operations side (BoBS, 1995, p. 31).

Jones did not warm to the idea of co-managing Baring Futures Singapore staff; indeed, he was offended by the idea. As a consequence, he took little interest in the new subsidiary, despite the fact that both himself and Bax were, on paper at least, responsible for Leeson at a regional level. This is confirmed by the BoBS report:

> Baring Futures Singapore was run as a separate operation from Baring Securities Singapore although Bax and Jones had, we consider, local responsibility for operational matters and both were directors of the company. There was clearly communication and contact between Leeson and Bax, and between Leeson and Jones; however, it is equally clear that Bax and Jones were much more focussed on Baring Securities Singapore than Baring Futures Singapore.
> (BoBS, 1995, p. 32)

Although Mike Killian managed the agency business that was sent from London (Baring Securities Limited) and Tokyo (Baring Securities Japan), and executed by Baring Futures Singapore, he rejected the idea that there was a reporting line between himself and Leeson. Yet this runs contrary to what Leeson argues, who cites Killian as one of the people who managed him in 1992. Hence from the very start of Leeson's employment at Baring Futures Singapore, there was considerable confusion over two key areas: first, what his job responsibilities were, and secondly, who managed him.

In early 1993 Leeson started trading on SIMEX in conjunction with Baring Securities Japan's Tokyo traders who (since the collapse of the Japanese stock market in 1990) made their money through a type of trading called 'arbitrage', otherwise known as 'switching'. This section of Baring's business was known as equity derivatives. Unlike Killian's business, the trading undertaken by the Baring Securities Japan traders and Leeson was conducted solely to make profits for Barings and not clients, and can therefore be classified as proprietary trading (see section 5). The manager in charge of the switching business was Fernado Gueller, based in Japan.

When Peter Norris became CEO of Baring Securities Limited in March 1993, after the dismissal of Heath, one of his first decisions was to make the Financial Products Group of Baring Brothers & Co. responsible for the equity derivatives business (i.e., switching). The actual hand-over of this business did not take place until late 1993. The manager in charge of the Financial Products Group was Ron Baker. Until October 1994 all switching continued to be overseen by Gueller, although he maintains he was never in direct charge of the SIMEX switching, which, he argues, was managed solely by Leeson. After October 1994, the management of the switching was delegated to Mary Walz (who reported directly to Baker) with Gueller reporting functionally up through her to Baker.

When the Financial Products Group took over switching, this had further implications regarding the person to whom Leeson reported at a product level. However, the BoBS cites considerable confusion over when and to whom Leeson should have reported as a consequence of these changes. According to the report:

> Ron Baker continued: 'There is a lot of ambiguity about where Nick [Leeson] sat during 1994 ... De Facto without knowing it, I inherited the income stream and the trading strategy that Nick [Leeson] was pursuing from 1 January 1994 ... I did not feel that Nick [Leeson] reported to me or that I had any real organisational control over him until the second half of 1994 ... Killian told the inquiry: 'We were informed by London that he [Ron Baker] had now taken on all the responsibility for arbitrage for Nick Leeson and for the proprietary people in Tokyo ... This would have been in 1993 ... the third/fourth quarterish'. Norris told us that Ron Baker took full management responsibility for the equity derivatives business from October 1993, including the 'switching' business managed by Baring Futures Singapore (BoBS, 1995, p. 23).

The issue of Baker's management over equity derivatives was hindered by two factors. First, there was additional confusion as to whom Baker reported in the matrix structure, and secondly, questions were raised over his ability to manage equity derivatives. While he had experience of derivatives, these were of the 'over-the-counter' (OTC) variety which are not sold on exchanges. Baker, therefore, had little knowledge or experience of the Exchange-traded derivatives, which formed the basis of the business undertaken by Leeson in conjunction with Gueller. He admits in the BoBS report that his relative inexperience was a contributing factor in the collapse of Barings.

To conclude this section on the management structure it is again worth citing the BoBS report:

> One of the consequences of the ambiguities in the ... organisational structure was that some of the members of management believed that responsibility for certain activities (e.g. equity derivatives, Baring Futures Singapore) rested with other managers, who deny they had such responsibility. This resulted in confusion and a pervasive lack of management control over these activities (BoBS, 1995, p. 23).

5.1.5 Authorised Trading Activities on Singaporean and Japanese Exchanges

The preceding section highlighted the management problems experienced with the creation of Baring Futures Singapore. This present section addresses the actual authorised trading on the Singaporean and Japanese exchanges by the Barings subsidiaries implicated in the collapse of the bank. Although the central focus for this chapter is Baring Futures Singapore (as is illustrated in the issue of management in the preceding section), the activities of this company cannot be discussed in isolation, owing to the very nature of the business it undertook, and the trading relationships that existed as a consequence. Hence, reference is made to other local subsidiaries, the exchanges on which the trading took place, and the London-based Barings companies which supplied considerable business for their Far East counterparts.

A description of the products that formed the basis of trading (namely derivatives), and the basis of the aforementioned relationships, can be found in 'Appendix One'.

Baring Futures Singapore's Agency Trading

As mentioned in the previous section, Baring Futures Singapore was formed to specialise in exchange-traded futures and options. In particular, Baring Futures Singapore would execute on the Singaporean Stock Exchange (SIMEX) client business on behalf of Baring Securities Limited and Baring Securities Japan. Acting in an agency capacity, Baring Futures Singapore had the capability to trade in any of the futures and options contracts traded on SIMEX. Baring Futures Singapore's and Baring Securities Japan's agency business was managed at a product level by Mike Killian, who was based in Baring Securities Japan's Tokyo office until March 1994, whereupon he was relocated to Portland, but continued to manage this business area.

Baring Securities Japan's Agency Business

While Baring Securities Limited was the primary booking entity for the majority of agency clients for Baring Futures Singapore and Baring Security Japan, the latter did have their own clients. Much of the agency business was undertaken by traders located in Baring Securities Japan's Osaka and Tokyo offices. Furthermore, these traders executed business on the local Japanese exchanges, which included the Osaka Stock Exchage (OSE), the Tokyo Stock Exchange (TSE), and the Tokyo International Financial Futures Exchange (TIFFE).

Baring Securities Japan's Proprietary Trading

Aside from Baring Securities Limited supplying agency clients for Baring Futures Singapore and Baring Securities Japan, another London subsidiary called Baring Securities London Limited also supplied trade for Baring Securities Japan, but the nature of this business was proprietary. Hence, Baring Securities Japan's traders in Tokyo took positions on the books of Baring Securities London Limited in the various contracts in Japan and Singapore, aiming for outright trading profits. This business was correctly registered as 'house' business (i.e., proprietary) with the various exchanges.

Baring Futures Singapore's and Baring Securities Japan's Proprietary Arbitrage (Switching) Trading

In addition to the above proprietary trading (and as noted in the preceding section), Baring Futures Singapore also undertook proprietary trading in conjunction with

Baring Securities Japan, for which Leeson was a key figure. The form of arbitrage trading undertaken commenced mid-1993, when Baring Futures Singapore traders identified price differences in Nikkei 225 contracts sold on SIMEX and OSE. The Nikkei 225 is a share index, like the FTSE 100. A futures contract based on the Nikkei is offered on the three Japanese exchanges and SIMEX. Traders realised that price differences arose between Singapore and Osaka, affording arbitrage profits to be made. Baring Futures Singapore traders subsequently took Nikkei 225 futures contracts (bought for hedging purposes) initiated by their Baring Securities Japan colleagues, and 'switched' them between Singapore and Osaka. In effect the Baring Futures Singapore traders would buy the cheaper contract and sell the more expensive. These trades would be reversed in less volatile markets or when the price differences had closed to a level of parity. The price differences between the two exchanges existed for two reasons. First, the OSE is an electronic exchange and tends to process trades more slowly compared to the open out-cry trading-pit found at SIMEX. Secondly, the OSE attracts more business than its Singaporean counterpart, leading to different market forces at work in the two exchanges. The Nikkei 225 market could move off the back of a large order in Osaka, leading to a temporary price difference with the SIMEX Nikkei 225 contract.

The Nikkei 225 was not the only contract on which arbitrage trading was conducted by Baring Futures Singapore on behalf of Baring Securities Japan. The ten-year Japanese Government Bond (JGB) was also a target for traders, with switching taking place between SIMEX and TSE. From May 1994 the three-month Euroyen contract also began to be switched between SIMEX and TIFFE.

It is worth mentioning here that, for some reason (no answer is provided in the BoBS report), Baring Securities Japan reported this proprietary business as 'client' rather than 'house' business with SIMEX. Of further importance is the fact that Baring Futures Singapore recorded details of 'switching' in their account number '92000'. As we shall see later, Leeson used this account (in conjunction with account 88888) for false accounting purposes.

5.1.6 Unauthorised Trading Activities Conducted by Baring Futures Singapore

The trading described in the previous section encompassed the authorised activities of Baring Futures Singapore. It was noted how Leeson, in conjunction with other Baring Futures Singapore traders, was authorised to take proprietary positions with regard to the switching business. However, Leeson was also engaged in substantial unauthorised trading on SIMEX through the taking of proprietary positions in futures and options. A number of methods were used to conceal this trading, and these are discussed in the next section. This section addresses the unauthorised trading through the examination of the history of the account (88888) used to book and record the deals. Through such an examination, the risk positions and the profits and losses that occurred from the trades are described. Details of the unauthorised trades are limited, owing to essential documentation not being made available to the compilers of the BoBS report. However, sufficient information exists to cite which derivatives were traded, over what period, and the subsequent losses accrued. It should be noted that Leeson was never authorised to take proprietary positions. He was only allowed to trade in the Nikkei 225, the JGB and the Euroyen with regard to the arbitrage business.

Account 88888

Prior to any discussion of the trades, it is worth noting that the BoBS report attributes the responsibility for trading on, and accounting for, account 88888 to Nick Leeson, for the following reasons:

1. He was the senior floor trader throughout the period examined.
2. He was the general manager of Baring Futures Singapore responsible for the back office.
3. Account '88888' was opened shortly before he began to use it for trading.
4. He took responsibility for arranging funding.
5. Staff in the Singapore office (so far as we have been able to obtain their views) attribute responsibility to him.
6. He represented himself to London as the person who could answer all the queries relating to the trading accounts.

7. SIMEX expressed concern in their letter to Baring Futures Singapore of 11th January 1995 that information required by the Exchange could not be provided in his absence.

(BoBS, 1995, p. 53)

Unauthorised trading of futures commenced very shortly after the opening of 88888 and carried on until the collapse in late February of 1995. This trading went largely unnoticed for almost two years and eight months. The only capacity in which Baring Futures Singapore was authorised to transact options was with regard to agency trading (see section 5). However, in October 1992 Leeson started to sell options, and continued to do so until 23rd February, 1995. The actual derivatives that were traded by Leeson included the following:

Futures

- Nikkei 225
- JGB
- Euroyen

Options

- Nikkei 225 futures contract.

At the year-end 1992, losses incurred through the unauthorised trading were relatively minor, standing at £2 million. One year later, they had grown to £23 million, and by 31st December 1994, the figure amounted to £208 million. In the space of the following three months, however, this figure had almost quadrupled to a staggering £827 million. The BoBS report acknowledges that if the unauthorised trading had been discovered at the end of 1994, Barings could feasibly have survived, albeit in a considerably weakened financial position. But the spiralling losses in the subsequent trading quarter ensured the fall of the bank.

5.1.7 Concealment of Trading Activities in Baring Futures Singapore

As noted, account 88888 was used for over two and a half years to facilitate unauthorised trading by Leeson. The very fact that he was able to conceal the positions and subsequent losses was instrumental in bringing down Barings on the 26th February 1995.

The account was originally opened as a Baring Futures Singapore client account on the 3rd July 1992. As with other accounts, the daily trading details were sent by Baring Futures Singapore to London in the form of four reports, which included: a trade file, which gave details of the day's trading activity; a price file, which reported on closing settlement prices; a margin file, listing the initial and maintenance margin details of each account; and the London gross file, which provided details of Baring Futures Singapore's trading positions.

Five days later after the inception of account 88888, however, Dr. Edmund Wong, a computer consultant, was instructed by Leeson to alter Baring Futures Singpore's computerised reporting system, so that details of the account were omitted from all the daily reports, except for the margin file. Understanding London-office procedures, Leeson knew that to conceal his trading activities, any information relating to 88888 had to be excluded from the other three reports. Furthermore, he knew the margin file was of little relevance, as staff in London never bothered to review the information it contained.

These machinations had the desired effect. The BoBS report cites how management and other personnel in London had no idea of the existence of the 88888 account until the 23rd February 1995. As Leeson had correctly surmised, despite the fact that the account details were maintained in the margin file, it was of no consequence, as this information was continually overlooked by the staff in London.

Yet within Baring Futures Singapore, settlements (back office) staff were aware of account 88888's existence, as their daily routines often led them to booking, and making adjustments to trades in account. Additionally, the BoBS report indicates that the Baring Futures Singapore floor traders were 'likely' to know of the account, as they were involved in preparing a 'daily blotter' which summarised the trading activities. Even though the front and back office instructions from Leeson may have been considered unusual, particularly during the final months which preceded the collapse, none of the aforementioned staff raised any concerns with senior managers.

Manipulation of Trade Prices

Despite the losses he incurred through unauthorised trading, Leeson needed to maintain the profitability reported with regard to authorised inter-exchange arbitrage (see section 5). This was conducted by Baring Futures Singapore (primarily Leeson) between SIMEX and the three Japanese exchanges (OSE for Nikkei 225, TSE for JGB and TIFFE for Euroyen). Leeson made this possible through unauthorised adjustments to the price of trades conducted on the SIMEX floor. As a consequence details of fictitious trades were recorded in the books of Baring Futures Singapore. These unauthorised adjustments were made through cross-trades, which the BoBS report defines as:

> .....a transaction concluded across the floor of the Exchange by a member who has matching buy and sell orders for the same contract and at the same price for two different customer accounts. Under SIMEX rules, the bid and offer of a cross trade must be declared three times by open outcry in the pit. If the bid or offer is not taken up, the member is allowed to cross the transactions at the stated price between the two accounts. Generally, a cross trade involves two floor traders of the same firm taking either side of the trade thereby transferring a position through the Exchange between two customer accounts of the same member firm. (BoBS, 1995, p. 80)

A significant number of cross-trades were made by Baring Futures Singapore between account 88888 and 92000. Cross-trades are supposed to be executed at the market price and during the trading-pit hours, although a 'post-settlement period' exists to allow traders to conclude unfinished business while still trading at official settlement prices. Leeson chose the post-settlement period to undertake many of the cross-trades. The reason, the BoBS report asserts, is that other firms' floor-traders were less inclined to trade during this time.

Leeson would then instruct settlement staff to take the cross-trades and change their prices, thereby creating 'profits' which were credited to account 92000, while losses were charged to the 88888 account. Hence, while the cross-trades appeared legitimate and within the rules espoused by the exchange, and while the Baring Futures Singapore's records listed the actual number of contracts cross-traded, their recorded prices bore no similarity to the real trading prices found on the floor of SIMEX. For

Leeson the cross-trades and manipulation of prices had the desired effect of inflating the reported profits in the arbitrage 92000 account while maintaining the losses in the concealed 88888.

Manipulation of the Books and Records of Baring Futures Singapore

When discussing the unauthorised trading undertaken by Leeson, it was noted that such trading resulted in losses accrued to account 88888. Leeson had to find a way to hide these losses, and he did so by creating false journal entries, creating fictitious transactions, and writing options. From February 1993 he masked the month-end balance on the account by making a journal adjustment, crediting 88888 with a sum which would leave the balance at zero, and making an additional journal adjustment by debiting the exact same amount to the SIMEX clearing bank account, maintained by Baring Futures Singapore. Following the traditional month-end reconciliation the trade was simply reversed. From the period February 1993 to January 1995 (24 months) this technique was used sixteen times. In the months when this method was not used, the balance on account 88888 amounted to zero. The BoBS report asserts this to be an 'unlikely coincidence' and indicates how, through the writing of options, the true balance continued to be manipulated. Leeson achieved this by taking the premiums collected through the selling of options, and offsetting this amount against the losses residing in account 88888.

The effect of these aforementioned methods of concealment is neatly summarised in the BoBS report which states:

> The effects of the methods applied to conceal the activity, balances and losses on account '88888' is that since its inception the account would not have featured within the management or financial accounts of Baring Futures Singapore, and would not have appeared on any management exception report.
> (BoBS, 1995, p. 91)

5.1.8 Funding of Baring Futures Singapore

The funding of Baring Futures Singapore proved to be another piece in the jigsaw of Barings' downfall. Mismanagement in the controls of funds from London (Baring

Securities Limited) to Singapore commenced with the inception of Baring Futures Singapore.

As stated, when Leeson started his new job, Ian Martin had requested he report to Gordon Bowser, who was in charge of futures and options settlements in London, and Simon Jones. Bowser had recommended that a reconciliation function, which tied funding requests to specific accounts, be carried out regularly in Baring Futures Singapore. He further advocated that this function be kept separate from Leeson's settlement department - i.e. independent. Finally, Bowser recommended that the creation of a routine reconciliation be agreed between Simon Jones (Baring Securities Singapore) and Tony Dickel (a member of Baring Securities Limited, which was instrumental in moving Leeson out to Singapore). Unknown to Bowser, who believed it to be a formality, no agreement was ever reached, and the reconciliation function in Singapore never came to fruition. This mismanagement was additionally reinforced by Bowser who, believing regular reconciliations were taking place in Baring Futures Singapore, saw little point in performing the same function in London, which he viewed as a duplication of effort and a waste of resources.

To compound these errors Bowser had also acquiesced to a request from Leeson with regard to funding. Leeson had argued that, owing to the way in which SIMEX called for margin, it was sometimes difficult to raise in time the appropriate monies to meet the requests. Hence, he argued that it would be easier, if, prior to the announcement of margin requests from SIMEX, advance funds could be made available from London (Baring Securities Limited) to Singapore. Bowser subsequently agreed. What this meant for Leeson was that he could call for funds from London without having to provide details about the accounts to which the funding requests related. In effect he had a free rein with regard to funds.

5.1.9 Failure of Internal Controls

The ability of Leeson to establish substantial unauthorised trading positions on SIMEX was afforded by failures in the management, financial, and operating controls in Barings. These failures were evident in Singapore, Tokyo, and London, and encompassed all levels of control ranging from the management controls of Baring

Investment Bank (ALCO and MANCO see below), the business functions and associated organisational units, and the actual day-to-day operating controls. This section reviews these controls and their failures.

Absence of Managerial Supervision Over Leeson

Failures in the management of Baring Futures Singapore has already been noted (see section 4). Suffice to say, they existed at both a product and a local office-operation level. This lack of management supervision on its own may not have afforded Leeson the chance to establish the massive unauthorised trading positions. What contributed significantly, however, were the failure of other control functions, which collectively meant that the trading positions went unnoticed until the 24th February 1995, and by which time Barings' losses were so large that survival was not an option. These other control functions included:

Lack of Segregation

The very fact that Leeson was in charge of Baring Futures Singapore's front and back office operations, negated the effectiveness of reconciliations and other accounting controls. The inherent associated risks were cited in the 1994 internal audit report (see section 10), which recommended a departmental reorganisation, relieving Leeson of direct responsibility for the back office. Unfortunately, this recommendation failed to be implemented. In hindsight, Norris recognised this to be a crucial error.

> I accept that the combination of Leeson's positions in front and back offices constituted a most serious failing in the context of the failure to implement the recommendations of the internal audit report to segregate front and back office duties and to reinforce the independent supervision in Singapore of Baring Futures Singapore's activities (BoBS, 1995, p. 121).

Insufficient Action Taken In Response to Warning Signals

As illustrated in the above example, one of the perennial features of Baring's management (see below regarding the role of MANCO and ALCO) was their failure to take appropriate and timely action with regard to Baring Futures Singapore, despite numerous warning signs.

No Risk Management Function In Singapore

In 1994 risk controllers were appointed for the first time in the London, Tokyo, and Hong Kong offices of Barings. Singapore was the exception. Agreement was reached in November 1994 that Rachel Yong, who had acted as Baring Futures Singapore's financial controller, would change jobs, assuming the risk management and compliance officer (see below) duties. This course of action proved untimely, for when the bank collapsed in late February 1995, Yong had still to commence her new responsibilities.

Weak Financial and Operational Control Over the Activities and Funding of Baring Futures Singapore at Group Level

It has already been noted how an independent reconciliation function failed to be inaugurated in Baring Futures Singapore. This, coupled with the ability of Leeson to request funds from London without having to provide details about the relevant accounts, represented weak financial and operational controls over this area. To some extent the control system that addressed the funding activities should have been strengthened by a constant dialogue between the Group Financial Controller in London, Geoffrey Broadhurst, and the Chief Operating Officer in Singapore, Simon Jones. But office politics and antipathy undermined the effectiveness of this safeguard. From May 1994 to the collapse, dialogue between the two was virtually non-existent because of the poor working relationship. That relationship had soured over a disagreement concerning Rachel Yong. Broadhurst had wanted Yong to attend a conference for all the financial controllers. Jones initially blocked the move and had only acquiesced after a considerable period of time. Unfortunately, after May 1994, any communication between the two was made via Bax.

Ineffective Compliance Function of Baring Futures Singapore

As with risk management, there was no compliance function in Baring Futures Singapore at the time of the bank's collapse. Once again, management intransigence is partly to blame, given that the 1994 internal audit advised the establishment of compliance monitoring. The BoBs report refers to the fact that with regard to compliance arrangements, overseas subsidiaries received little attention in London. Although there was a Baring Investment Bank Compliance Officer (Valerie Thomas) who ostensibly had a global role, that role did not encompass examining the capability of the compliance arrangements for the overseas offices. An agreement was, however, reached in November 1994, that Rachel Yong (see above section on Risk Management) would move from acting Financial Controller to the dual role of Risk Manager and Compliance Officer. Unfortunately, given the delay in agreement, Yong had not even begun her new duties at the time of the collapse.

Inaccurate Reporting to Regulators

Although Barings did produce regulatory reports, which contained some pertinent information relating to Baring Futures Singapore's precarious financial position, of greater importance was the information omitted, information that would have alerted the bank's regulators, (see section 12).

The Role of ALCO and MANCO

Central elements in the control structure of Barings were the Asset and Liability Committee (ALCO) and the Management Committee (MANCO). These were responsible for providing an oversight role. ALCO was created through a merger of Baring Securities Limited's Risk Committee and Baring Brothers & Co.'s Treasury Committee in November 1994. Members of ALCO met daily to discuss the previous day's trading, credit issues, market risk and the like. MANCO had been formed in May 1994. Its members comprised executive management from both the securities and banking arms of Baring's business. Chaired by Tuckey, and convened on a weekly basis, MANCO acted as the decision-making forum for Baring Investment Bank.

The BoBS report indicates how during 1994 and 1995, both committees discussed issues relating to Baring Futures Singapore's switching business. More precisely, up to the 24th January 1995 both ALCO and MANCO expressed little concern with regard to the arbitrage activity, although some doubts were beginning to be raised about the levels of funding. From the 24th January 1995 ALCO members were increasingly worried about market positions, the associated risk profiles, market rumour, and the integrity of the information purporting to provide accurate margin details. This period also witnessed some alarm by MANCO members in terms of the funding and profitability of the arbitrage business. Unfortunately, these concerns did not translate into management action aimed at addressing quickly and rigorously those factors which formed the basis for alarm. As a consequence, when the unauthorised trading was finally discovered, considerable losses had already been incurred and a salvage operation was no longer an option.

5.1.10 Internal Audit

Baring Futures Singapore was subject to its first and only internal audit in August 1994. It was undertaken by James Baker (no relation to Ron Baker) who was a member, but not the head, of the Baring Securities Limited's audit team. This Baring Securities Limited function was only created towards the end of 1992, compared with Baring Brothers & Co. who established their audit department in the mid -1980s. This disparity to some extent reflects the priority given to constructing sound control environments in the respective business units. The Singapore audit was the last undertaken by the Baring Securities Limited team, which, as a result of the merging of Baring Securities Limited and Baring Brothers & Co, was similarly merged with its banking counterpart to form the Baring Investment Bank internal audit group.

Prior to leaving for the Far East, James Baker had met with Tony Hawes (Baring Securities Limited's Treasurer) to ascertain if there were any issues he would like investigating with regard to Baring Futures Singapore. Baker noted the following:

> A major concern is the Futures company. Nick Leeson has too dominant a role looking after both trading (agency and proprietary) and settlements aspects of the business; there is no deputy to challenge him. The amounts of money involved are vast and this is a very fast-moving and complex market. TH [Tony Hawes] believes that SJ [Simon Jones] basically leaves NL [Nick Leeson] to his own devices. While he has no evidence to suggest that NL has indeed abused his position, the potential for his doing so needs examining (BoBS, 1995, p. 143).

The actual audit was due to take place in early 1994, but as a consequence of delaying tactics employed by Jones, did not commence until July of that year. Baker spent two weeks in Singapore, interviewing, amongst others, both Leeson and Jones.

During this period, Baker drafted several versions of the Baring Futures Singapore audit report. The first draft included a recommendation that a regular reconciliation be made between Baring Futures Singapore's funding requests to London and the actual accounts to which they related. As noted, Bowser believed that this specific reconciliation had been taking place since the formation of Baring Futures Singapore, but, as an agreement was never reached, the function was never introduced.

Leeson strongly opposed this recommendation, citing how the reconciliation was unnecessary and would tie up scarce resources which could be put to better use elsewhere. Although Baker argued that the reconciliation need not take place daily and could rather be undertaken on a weekly or even monthly basis, Leeson continued his entrenchment. Baker eventually acquiesced, and no further mention was made about the reconciliation in subsequent drafts of the audit report.

At the end of the two-week stay, Baker completed his final report. The major recommendations were:

- Reorganisation of Baring Futures Singapore, relieving Leeson of direct responsibility for the settlements section, affording appropriate segregation of duties between front and back offices.
- As a consequence of the growth in Baring Futures Singapore's trading, its size now warranted the employment of a full-time Risk Manager and Compliance Officer.
- A review of Baring Futures Singapore's funding, to be undertaken by the London Group Treasury department.

With regard to the first point both Leeson and Jones stated that the proposed recommendations would be implemented. Jones went as far as giving his own personal assurance that the settlements section would be appropriately supervised once the necessary changes had been implemented. In the end no action was taken. Leeson continued to have direct control over the front and back offices with the full knowledge of Jones, who made no attempt to implement the audit recommendation.

Some action was taken with regard to the employment of a Compliance Officer and Risk Manager. But, as has already been noted, at the time of the collapse, Rachel Yong had not even commenced her new duties.

Although the audit report recommended a review by the London Group Treasury Department of the way Baring Futures Singapore was funded, this failed to take place prior to the collapse.

5.1.11 External Audit

In London Coopers & Lybrand had acted as Barings plc's external auditors for many years. Coopers & Lybrand further audited all the other Barings subsidiaries, both through its London offices and overseas branches. There was, however, one exception, namely Baring Futures Singapore. The 1992 and 1993 Baring Futures Singapore's external audits were performed by Deloitte & Touche. As part of this undertaking Deloitte & Touche reported their findings to Coopers & Lybrand, who were responsible for producing Baring plc's consolidated financial statements. For Baring Futures Singapore's 1994 audit, however, Deloitte and Touche were replaced by Coopers & Lybrand Singapore.

When examining the external audit function with regard to Baring Futures Singapore, the compilers of the BoBS report were severely hindered by the stance taken by Coopers & Lybrand Singapore and Deloitte & Touche. Both these companies refused access to the relevant working papers and denied the BoBS team the opportunity to interview their respective members of staff, who conducted the Baring Futures Singapore's audits. Coopers & Lybrand did provide some access to pertinent material. Despite the lack of information, a number of points can be raised which cast doubt over the efficacy of the external audits undertaken at Baring Futures Singapore.

Baring Futures Singapore's 1992 Audit

There is little mention in the BoBs report of the 1992 external audit by Deloitte & Touche. Importantly though it does make reference to the Deloitte & Touche management letter, prepared at the end of the 1992 audit, in which 'no significant matters were raised'. Leeson commenced work at Baring Futures Singapore in March 1992. Given that from the very start of his employment he had control of the front and back office, it seems strange that in the 1992 audit, Deloitte & Touche did not perceive this, for example, to be a significant matter.

Baring Futures Singapore's 1993 Audit

On the 28th January 1994 Deloitte & Touche presented Coopers & Lybrand with the Baring Futures Singapore's audit report for the year ending 31st December 1993. As with such information from the other Barings audits, Coopers & Lybrand used the data to produce the consolidated financial statements of Barings plc. Deloitte & Touche had stated that the 1993 audit had been conducted and produced in accordance with the UK Auditing Standard. The Deloitte & Touche report cited a Baring Futures Singapore profit for the year-end 31st December 1993 of £9 million. After adjustments, due to the unauthorised trading, the BoBS report states the real figure was more likely to be in the region of a £10 million loss.

As Coopers & Lybrand were acting as the parent company auditor, they had asked Deloitte & Touche to provide a summary of the audit approach taken regarding the Baring Futures Singapore's 1993 audit. Once again Deloitte & Touche's response can be considered surprising for as the BoBS report states:

> D&T confirmed: that they had evaluated the adequacy of controls within the accounting system and identified that reliance could be placed on these controls: that they had performed sufficient testing to provide audit evidence that internal control procedures were in place and were effective; and that there were no weaknesses in the company's systems which were of sufficient significance to bring to C&L's attention (BoBS, 1995, p. 155).

Status of the 1994 Baring Futures Singapore's Audit

The board of directors of Barings plc met on the 22nd February 1995 to approve their accounts (produced by Coopers & Lybrand) for the year ending 31st December 1994. These accounts incorporated the financial position of Baring Futures Singapore, which had been audited by Coopers & Lybrand Singapore. The audit had commenced early in October 1994 and concluded with the sending of Baring Futures Singapore's financial statements to Coopers & Lybrand on the 3rd February 1995. As the BoBS team did not have recourse to those members of Coopers & Lybrand Singapore who conducted the audit, their working papers, or the subsequent report that was produced, it is difficult to pass comment on the way the audit was performed and the findings it produced. The fact, however, that Baring Futures Singapore's stated financial position per the accounts bore no relation to the reality, draws into question the methods and findings of the Coopers & Lybrand Singapore audit group.

Lack of Dialogue Between Internal and External Auditors

One final point to make in this section concerns the lack of dialogue between the audit groups. Despite receiving the yearly internal reports of the Baring Brothers & Co. audit team, Coopers & Lybrand had not made similar arrangements with the Baring Securities Limited's internal audit group. Two partners and a manager of Coopers & Lybrand all confessed that they had not seen the Baring Futures Singapore's internal audit report. As a consequence, they were not aware of the concerns raised over the segregation of duties, risk, and compliance monitoring, and the funding of Baring Futures Singapore from London.

5.1.12 Supervision of the Barings Group by the Bank of England and the Securities and Futures Authority

By discussing the Barings Group and its supervisory relationship with the Bank of England and the Securities and Futures Authority, the aim in this part of the chapter is to address those aspects of these relationships, which enabled Leeson to undertake the unauthorised trading in Baring Futures Singapore and remain undetected for over two and a half years. The regulatory relationship between Baring Futures Singapore and SIMEX would also have been addressed in this section were it not for the fact that SIMEX officials refused to be interviewed for the BoBS inquiry. Members of the latter were also unable to review the relevant SIMEX correspondence and documentation.

Supervision of the Barings Group by the Bank of England

The role of the Bank of England with regard to the banks they supervise is to help such banks maintain degrees of solvency and stability. This is achieved through the imposition of regulations. The mathematical formulas that underpin the regulations are complex but the associated principle is simple. A bank should never place itself in a position where it risks a sum of money that it could not afford to lose. More precisely, a bank's business is backed by its capital. In the course of trading the sum of money at risk should never exceed its total sum of capital.

When Leeson joined Baring Futures Singapore in March 1992, the Barings Group was under the consolidated supervision of the Bank of England. This type of supervision involved the assessment of risks to the bank (Baring Brothers & Co.) with regard to the business activities of other companies (e.g. Baring Securities Limited) in the Barings Group. This assessment was facilitated by Baring Brothers & Co., which collated information from all the companies that constituted the Barings Group, and passed this information (which was known as 'consolidated returns') on a regular basis to the Bank of England.

Although the Bank of England acted as the consolidated supervisor of the Barings Group, this did not mean that all the companies in the Group were under its direct supervision. As the BoBS states:

> ... the Bank of England was not responsible for the supervision of any individual Barings entities other than Baring Brothers & Co. ... The supervision of other Baring entities (including their capital adequacy and the effectiveness of their systems and controls) remained the primary responsibility of the relevant regulator in the country or business sector in which the Group company operated (including, where relevant, other UK regulators e.g. the Securities and Futures Authority). The Bank of England is under no duty, indeed has no statutory power, to supervise other companies in a group to which a bank belongs. However, the Bank of England is required under the Act [the Banking Act of 1987] to take into account risks elsewhere in a group which might affect the authorised institution. Accordingly, Bank of England supervision was primarily focused on Baring Brothers &Co., but the Bank of England was required to take into account the activities of other parts of the Barings Group insofar as they might affect the reputation and financial soundness of Baring Brothers &Co. (BoBS, 1995, p. 193).

The UK Banks Supervision Division was the Bank of England department in which the Barings Group was monitored. Carol Sargeant was the head of this section from March 1993. Reporting directly to her was Christopher Thompson, a senior manager in the department, whose specific responsibilities included the supervision of the UK Merchant Banks (one of which was Baring Brothers &Co.).

Solo Consolidation

The early 1990s had proved to be a difficult time for Baring Securities Limited. Its rapid expansion was impeded by the end of the Japanese stock market boom. By 1991 there were twenty one Baring Securities Limited subsidiary offices employing approximately 1300 staff. Rising overheads and falling profits (reported monthly in 1992) placed excessive strain on Baring Securities Limited's capital. Baring Brothers & Co. came to the rescue with a £50 million loan, but this was only possible because it had received what is known as a 'treasury concession' by the Bank of England. If a bank wants to lend to a group company a sum of money, and if that sum is more than 25% of the bank's capital base, then it must get permission (hence the treasury concession) to do so. Although the £50 million did not amount to 25% of Baring Brothers & Co's capital, the bank had asked for a concession amounting to £150 million, which did exceed a quarter of their capital.

Despite the concession, management in Baring Brothers & Co. found the limit of £150 million too restricting, and, as a consequence, began to consider the solo-consolidation of Baring Brothers & Co. and Baring Securities Limited. This form of consolidation is defined in the BoBS report as follows:

> If the linkage between an authorised institution and one of its subsidiaries is sufficiently strong, and certain other criteria are met, the Bank may permit the subsidiary to be treated effectively as a division of the institution and included in the institution's unconsolidated prudential returns filed with the Bank. This is known as 'solo consolidation'. Where this occurs the subsidiary is monitored for capital adequacy ... as if it were part of the institution (BoBS, 1995, p. 163).

Tony Hawes commenced a review in mid-1993 to assess the feasibility for solo consolidation of Baring Brothers & Co. and Baring Securities Limited. If solo consolidation was deemed appropriate (and agreed with the Bank of England), then Baring Securities Limited would be in a position to access the capital of Baring Brothers & Co. to a sum far exceeding the £150 million limit imposed by the Bank of England.

Indeed, several meetings took place between Baring Brothers & Co. and the Bank of England to discuss the issue. The BoBS cites how Sergeant and Thompson were in a state of 'disarray' with regard to the proposal. Sergeant was particularly concerned about the lack of information to which her department would have access as regards the financial positions of the Baring Securities Limited's subsidiaries and the associated risks. Nevertheless on the 4th November 1993 Thompson gave provisional acceptance to solo consolidation 'pending further consideration'. No further 'consideration' was, however, given to the issue, and for all intents and purposes, Baring Brothers & Co. and Baring Securities Limited were solo consolidated from November 1993. Perhaps not surprisingly, solo-consolidation between the two groups was very much the driving force between their eventual merger.

Crucially for Leeson, solo-consolidation meant access to Baring Brothers & Co's capital base via Baring Securities Limited, which in turn financed Baring Futures Singapore. Owing to poor accounting controls Leeson was now able to draw on not only Baring Securities Limited's capital base, but also Baring Brothers & Co's. This was helped by the fact that Baring Securities Limited was funded without limits by Baring Brothers & Co.

As Maclean states in the BoBS report:

> I was involved in the setting up of the process which became known as solo consolidation, which in my view, is one of the factors at the heart of this problem, this crisis ... That amount of cash could not have got to where it did if it had only been in Baring Brothers & Co. The principle of solo consolidation is that the bridge between Baring Brothers & Co. and Baring Securities Limited was taken away and the two were pushed together, so that any amount of cash ... could go from Baring Brothers & Co. to Baring Securities Limited (BoBS, 1995, p. 169).

Supervision of Barings Group Companies by the Securities and Futures Authority

Baring Securities Limited, Baring Securities London Limited and Baring Brothers & Co. were all members of the Securities and Futures Authority. Of the three companies, Baring Securities Limited and Baring Securities London Limited were authorised by the Securities and Futures Authority to conduct investment business in the UK. The Securities and Futures Authority reached agreement with the Bank of England in a memorandum of understanding that the latter would regulate the business activities of Baring Brothers & Co. Even though Baring Brothers & Co. and

Baring Securities Limited solo-consolidated in November 1993, Baring Securities Limited continued to maintain regulatory capital in accordance with the Securities and Futures Authority's rules.

The Securities and Futures Authority was created to ensure that its members maintain adequate financial resources to remain solvent and stable, while protecting their customer's assets. The extent to which the Securities and Futures Authority should monitor the business activities of member firms' subsidiaries is something of a grey area. As the BoBs report states:

> The extent to which the Securities and Futures Authority is required to concern itself with the operations in and financial affairs of subsidiaries is ill-defined by the Financial Services Act [1986] ... the Securities and Futures Authority has rules which relate, in part to the financial position of subsidiaries of a member firm. Nevertheless, the Securities and Futures Authority has stated that it does not regard itself as having obligations with regard to subsidiaries (whether UK or foreign) other than those which apply to ordinary counterparties who might expose the member firm to risk; and that it has no further power with regard to subsidiaries other than the notification of obligations expressly set out in its rules. Accordingly the Securities and Futures Authority does not undertake consolidated supervision of a member firm and its subsidiaries in the way the Bank of England does. However, BoBS is advised that in monitoring the financial resources of Baring Securities Limited, the Securities and Futures Authority should have had regard to the financial soundness of Baring Securities Limited's subsidiaries including Baring Securities Japan and Baring Futures Singapore insofar as the operations of the subsidiaries were capable of affecting the financial integrity of Baring Securities Limited (BoBS, 1995, p. 217).

The BoBS report, however, recognises that the Securities and Futures Authority does not have any power to regulate the subsidiaries of a member firm. Furthermore the report stresses that the Securities and Futures Authority's concern is solely with the investment business activities of their members.

Within the Securities and Futures Authority, the Surveillance Division was responsible for the regulation of Baring Securities Limited and Baring Securities London Limited. More specifically, Rupert Armistead was the team manager who oversaw the activities of the two groups for the period January 1992 to August 1994. He was succeeded by Carol Sergeant. Stephanie James, who reported directly to Sergeant, was the team member who had the most daily contact with both Baring Securities Limited and Baring Securities London Limited.

As noted, Leeson was able to extricate funds from Baring Securities Limited and (after solo consolidation) Baring Brothers & Co. The supervisory role of the Securities and Futures Authority with regard to the monitoring of this funding was flawed on two levels:

1. The Securities and Futures Authority did not believe it was responsible for assessing the inherent risks associated with member firms' subsidiaries.
2. Baring Securities Limited failed to provide the Securities and Futures Authority with precise details regarding the Baring Futures Singapore's funding.

In terms of point one, it has been noted how the Securities and Futures Authority did not view the monitoring of member firm subsidiaries as part of its remit. This is confirmed by Securities and Futures Authority's staff, who were interviewed as part of the BoBS inquiry. Armistead, for example, argued:

> I do not know if we would have specifically looked at Singapore as an operation ... we are looking at the one particular entity. That was the member and we were actually looking at the regulation I guess ... As you can imagine, where you have 80 members and a team of five, you do not necessarily have the chance to sort of look at subsidiaries (BoBS, 1995, p. 226).

This view was supported by James who believed:

> Baring Securities Limited had a lot of subsidiaries, most of which were trading overseas in various different markets ... The assumptions would have been made at this end that those subsidiaries in those foreign countries were being looked after and regulated by another institution overseas. They are not our responsibility. Our responsibility is purely to our members (BoBS, 1995, p. 226).

With regard to the second point, one of the methods through which the Securities and Futures Authority undertake their supervisory role is through the monitoring of financial returns which it receives on a routine basis from its members. The returns are submitted in electronic format and reviewed on-screen by Securities and Futures Authority staff. As with other Securities and Futures Authority members, part of the Baring Securities Limited financial information sent on a monthly basis were the balance sheets. Included in the balance sheet is a section entitled 'Trade Debtors'. This further included details of amounts due from 'affiliates'. The Baring Securities Limited balance sheet indicated significant amounts of money were due from these affiliates. For example, at the 31st December 1993, the amount came to £254 million and by the same date the following year it totalled £540million. What Baring Securities Limited crucially failed to mention was that these affiliates were actually Baring Futures Singapore and Baring Securities Japan. Of course, unbeknown to Baring Securities Limited, a large proportion of this money represented funds requested to pay for the unauthorised trading conducted by Leeson. If Baring Securities Limited had named Baring Futures Singapore and Baring Securities Japan and cited the actual amounts that were funded to them, then the Securities and Futures Authority may have had cause for concern and acted appropriately. Unfortunately, this error was reinforced by the Securities and Futures Authority, who at no time asked for a listing of the affiliates, or the amounts they owed.

5.2 Conclusion

This chapter examines those factors that were instrumental in the collapse of Barings. It is noted how initial problems were created through the formation and development of Baring Securities Limited. Although in its early years Baring Securities Limited proved to be a spectacular business success, the company did not sit easily with its banking counterpart, Baring Brothers & Co. The conflict between the two groups was one of the factors that led to their eventual merger, leading to the formation of Baring Investment Bank.

One of the many subsidiaries opened during the expansion of Baring Securities Limited was Baring Futures Singapore. A central figure in this company was Leeson around whom there was considerable confusion over his management reporting lines and employment responsibilities. While Leeson undertook authorised trading on the Singaporean and Japanese exchanges, he additionally carried out unauthorised trading on SIMEX for over two and a half years. Leeson used several methods to conceal the unauthorised trading including, for example, omitting details of account 88888 from the daily trading reports sent to London. Leeson was able to finance the unauthorised trading as a result of mismanagement in the control of funds from London to Singapore. Furthermore, his ability to establish substantial unauthorised trading positions was afforded by failures in the financial, management and operating controls in Barings.

The first and only internal audit in August 1994 had little impact on reinforcing the control environment at Baring Futures Singapore, Similarly, questions were raised in the BoBS report over the effectiveness of the three external audits. Finally with regard to the supervision of the Barings Group by the Bank of England and the Securities and Futures Authority, it was noted how the solo-consolidation of Baring Brothers & Co. and Baring Securities Limited allowed Leeson access to the former's capital base. Additionally, it was noted how the supervisory role of the Securities and Futures Authority was flawed, given that the regulating body did not believe it was responsible for assessing the risks associated with member firms' subsidiaries and, furthermore, Baring Securities Limited failed to provide the Securities and Futures Authority with precise funding details regarding Baring Futures Singapore.

Chapter Six: Discussion and Analysis

In attempting to assess the feasibility of a crime specific opportunity structure, the first section of the 'Discussion and Analysis' chapter will address the theoretical coherence of the model with regard to using the Barings case as a 'test bed'. Do the propositions and concepts inscribed in the model hold 'theoretical water' when applied to the case study? Using data from the case study each element of the model will be duly assessed, and where relevant the theoretical relationships between the elements will also be examined.

After a discussion of the elements that constitute the model, the next section of the chapter examines related themes. For example, one of the themes concerns the holistic nature of the model. Unlike the vast majority of writings in the IS Security field, one advantage of the crime specific opportunity structure is that it is able to consider the elements that afford security as an 'in-progress' phenomenon. Hence it is able to view the elements in an interactive relationship. The chapter ends with a summary and conclusions.

Before the specifics of the model are discussed, the following should be noted regarding the relationship between the model and the case study data. The crime specific opportunity structure addresses the activities of a potential offender up to the point of a crime commission. However, the majority of the data in the Barings' case relates to a period during which Leeson was actually undertaking the fraud. This does not mean that the data cannot be used to assess the theoretical propositions in the model, although this feature of the crime specific opportunity structure should be recognised.

For easy reference, the Opportunity Structure for Crime and the Crime Specific Opportunity Structure diagrams are now reprinted under the headings Fig.3 and Fig.4.

Fig. 3

Opportunity Structure For Crime

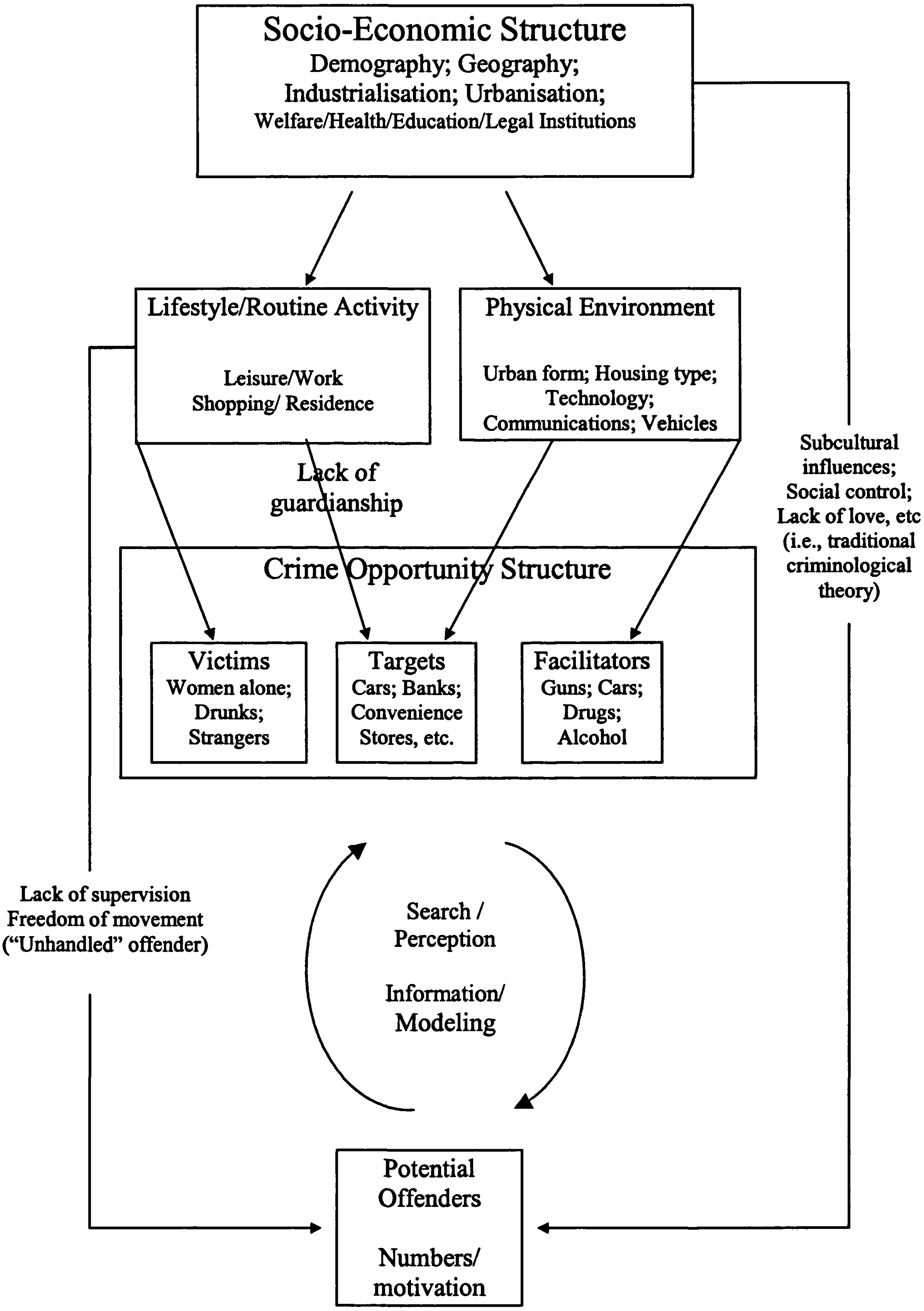
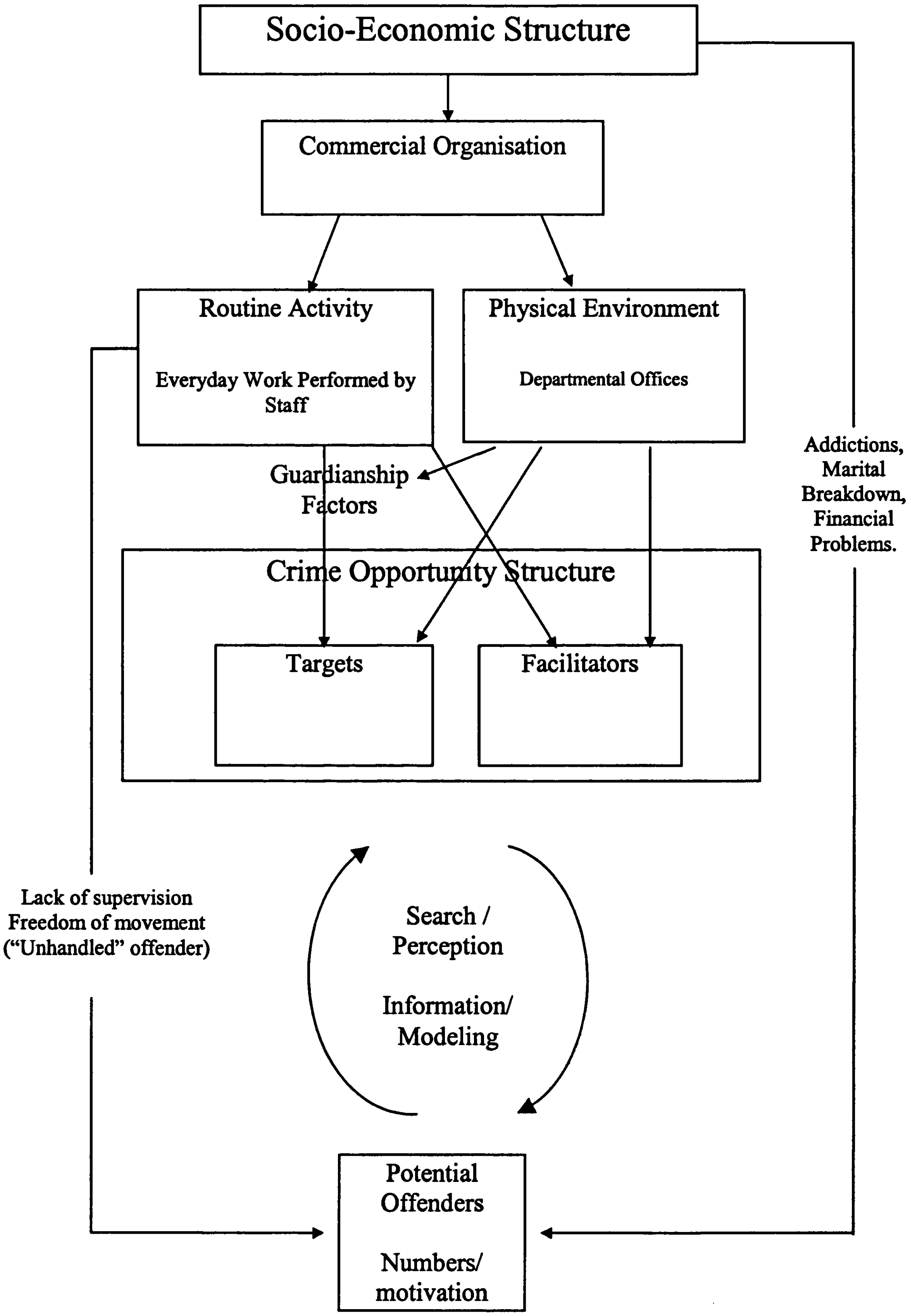


Fig. 4

Crime Specific Opportunity Structure



6.1 Theoretical Coherence of the Model

6.1.1 Unhandled Offender

The crime specific opportunity structure depicts the number of potential offenders as partly determined by routine activities which impact on the nature of social control afforded by 'intimate handlers'. Advocates of routine activity theory (Cohen and Felson, 1979) argue that for a crime to occur, three elements must meet in time and space: a potential offender, a target and the absence of a capable guardian. In an attempt to accommodate Hirschi's (1969) social control theory, Felson (1986) proposed the incorporation of another element, that of the intimate handler, to illustrate how people can act as a 'brake' on the activities of offenders. In his book *Causes of Delinquency*, Hirschi (1969) argues that there are four factors that constitute a social bond between an individual and society. These include commitments, attachments, involvements and beliefs. So, for example, with regard to 'commitments':

> the person invests time, energy, himself, in a certain line of activity, say, getting an education, building up a business, acquiring a reputation for virtue. When or whenever, he considers deviant behaviour, he must consider the costs of this deviant behaviour, the risk he runs of losing the investment he has made in conventional behaviour ... Most people, simply by the process of living in an organised society, acquire goods, reputations, prospects that they do not want to risk losing. These accumulations are society's insurance, that they will abide by the rules (Hirschi, 1969, pp. 20-21).

Felson (1986) uses the word 'handle' to summarise the four elements that help to create a social bond. By doing so he argues that the social bond (and hence handle) is a key element in informal social control. Another important factor in this equation is the 'intimate handler' who is able to exert this form of control. The handler is normally someone who is recognised by, and has sufficient knowledge of, the potential offender. Hence the mere presence of a person known to the potential offender may act as a form of handling, and consequently a deterrent, by reminding the offender of their social bonds. Felson cites the example of a mother and son living in a flat. Their neighbour owns a state of the art television set. The son, who has some criminal inclinations, is tempted by the television, but such inclinations are mitigated by his mother's presence, and the fact that she knows the neighbour and recognises the television.

Incorporating the concepts of the handled offender and the intimate handler into routine activity theory, Felson argues that just as a target must be lacking a capable guardian for the commission of a crime, so too must the offender be lacking an intimate handler. Furthermore, as Felson notes (1986), routine activities can impact on the ability of individuals to act as an intimate handler:

> As daily activity patterns disperse people away from family and household situations, it is more likely that criminogenic conditions will apply. Not only will offenders find targets with guardians absent, but they will be able to get away from their handlers ... It is not that urbanites lack friends or family ties, or that they are unhandled, but merely that their handlers are scattered and segregated from the suitable targets and capable guardians (Felson, 1986, pp. 124-125).

Routine activity theory (Felson, 1986) and the concepts of the 'intimate handler' and the 'handled offender', underpinned by Hirschi's (1969) social control theory, offer some insight into the management problems experienced by Baring Futures Singapore. However, as we shall see, the aforementioned theoretical concepts lack the necessary sophistication to provide a comprehensive explanation of the supervisory failings in the Far East subsidiary. As noted, an intimate handler is usually someone known to the offender, and whose mere physical presence is enough to deter criminal activities. Felson (1986) further argues that a potential offender must be lacking an intimate handler to afford the freedom to perpetrate a crime. To some extent these theoretical propositions are mirrored in the collapse of Barings.

Initial management problems were created at the inception of Baring Futures Singapore. The BoBS report cites how despite the fact that James Bax (Head of Baring Securities Singapore) and his second in command, Simon Jones (Chief Operating Officer of Baring Securities Singapore) had, on paper at least, regional responsibility for Leeson, neither spent much time overseeing his activities. Although the BoBS report acknowledges there was some contact between the two 'managers' and Leeson, it further contends that both Bax and Jones preferred to focus their energies on Baring Securities Singapore. Additionally, Mike Killian, who managed the agency business sent from London and Tokyo, and executed by Baring Futures Singapore, rejected the idea of a reporting line between himself and Leeson. Hence, from the start of Leeson's employment at Baring Futures Singapore, there was confusion over who actually managed him. This confusion manifested itself in a paucity of oversight from senior management. There is some overlap here with the theoretical concepts of the intimate handler and the handled offender. The fact that, on the whole, there was an absence of an intimate handler in the form of senior management, provided Leeson with the freedom to undertake his unauthorised trading.

However, there is a divergence between theory and data with regard to how supervision is actually enacted. With regard to the intimate handler, their presence is enough to act as a deterrent. But it was not just the mere physical absence of a manager, which aided Leeson in perpetrating his criminal activities. When Leeson was afforded some supervision, the evidence suggests that the management problem was compounded by the fact that Bax, Jones and Ron Baker (who was later responsible for managing Leeson at a product level) had very little understanding of the products (futures and options) he dealt in and the trading processes which underpinned this business. In this sense, supervision could not be executed properly owing to the ignorance of managers regarding the nature of business undertaken by Leeson and not, in the case of intimate handlers, owing to their absence.

Readying

With regard to Barings and organisations generally, it is important to note how the setting in which the associated routine activities take place, may additionally impact on the number of potential offenders. The work of Wortley (1997) offers a good starting point for this discussion. He contends that the concept of opportunity, when used with regard to SCP, is myopic, and does not fully appreciate the complexity of the relationship between actor and situation. Rather it merely acknowledges the role of situational factors in affording (or not as the case may be) an opportunity as perceived by the potential offender. However, he argues that a broader reading of the rational choice approach and input from psychology literature can enhance an appreciation of this complexity, particularly with regard to situational influences on criminal intent. Hence, Wortley believes that situations should be highlighted for their potential ability to 'ready' individuals for specific crimes.

These situations may be categorised into four types: situations that prompt; situations that pressure; situations that permit; and situations that provoke. With regard to situations that permit, for example, Wortley cites how deindividuation may occur in certain social circumstances. This phenomenon refers to a state where an individual's self-awareness is reduced through membership of a group (Diener, 1980; Prentice-Dunn and Rogers, 1989; Zimbardo, 1970). In addition two levels of self-awareness can be affected by deindividuating influences. First, an individual's public self-awareness may change. At this level an individual is conscious of their status as a social object. Through interactions with other group members, a sense of anonymity may emerge and concerns about possible censure from onlookers may abate as a consequence. Secondly, at another level, an individual's private self-awareness may be influenced by group membership. Private self-awareness affords the ability to focus on and monitor one's own thoughts, values and feelings. This ability is hindered as individual identities are submerged through group membership. In such circumstances one is susceptible to situational cues and may participate in behaviour which would not occur outside the group context. Hence, deindividuating effects on private self-awareness, resulting from group membership, can impair the ability to regulate one's behaviour.

Willison (2001) argues that with specific regard to IS security and organisations, readying can act as a 'sensitising' concept (Blumer, 1954) by drawing practitioners' attention to motivational factors. When discussing computer-assisted fraud, he argues, it is not unreasonable to assume that, in some cases, the inclination to commit fraud is a consequence of the organisational environment – i.e. the organisational environment may foster a situation which readies an individual. This argument is supported by a recent CBI / Ernst and Young (2000) publication which states:

> The motivation for fraud is often dissatisfaction based on being passed over for promotion and inadequate pay rewards, or a feeling of carrying more than a fair workload (CBI / Ernst and Young, 2000, p. 16).

Recognising these phenomena and their implications for IS security affords practitioners the ability to consider relevant safeguards and by doing so expand the preventive scope. Willison (2001) illustrates how the scope may be broadened, through the consideration of readying factors, by way of a simple time line (see Fig. 5).

T0 R CBA C T1

Fig. 5 Readying Time Line

T0 to T1 represents a period of time. The period may be a number of weeks, months or even years. T0 to R reflects a time of good working relationships in an organisation. R, however, indicates a readying situation e.g. a rumour of job cuts, or the announcements of staff losses. The now readied individual (or indeed individuals) proceeds to make a cost benefit analysis (CBA) – that is, a rational choice as to whether the organisational setting affords a specific opportunity. If it does, a commission (C) will take place. At that point on the time-line where the potential offender is weighing up possible opportunities and making rational choices (CBAs), motivational factors have already played their role and formed one of the antecedent stages in the commission of a fraud. That said, organisations could expand their preventive armoury by also addressing readying factors.

Willison (2001) argues that unfortunately traditional perceptions (held by fraud specialists and IS security practitioners generally) of the control environment have focussed on work processes. In terms of the time-line, however, the majority of these safeguards can be viewed as the last line of defence for companies in that their role is to stop the commission (C) of a crime, and so little attention is paid to those aforementioned stages, which the concept of readying helps to broach. Furthermore, any visibility afforded by the working processes is lost when considering controls that address motivational factors.

A central problem, Willison asserts, is that those charged with combating fraud - departmental staff, internal/external/fraud auditors, information security staff - may have some understanding of what motivates staff, but they do not have the knowledge or methods (underpinned by cogent theory) to tackle motivational factors. Hence appropriate knowledge and methods should be deployed for particular problems. In terms of such knowledge and methods, he advocates that IS academics and practitioners do not have to reinvent the wheel. Where better to gain insight into criminal motivations than from the field of criminology?

As mentioned, SCP, the rational choice perspective, routine activity theory and environmental criminology, focus on situations where criminal activity takes place. Traditionally, once consideration is given to motivational or background factors, therein is entered the world which dispositional theories examine. The organisational context, however, represents a unique hybrid of these two positions. If we subscribe to the concept of readying, we can see that not only can the organisational context provide the environment in which a crime occurs, but it also provides, in some instances, the situation in which motivational factors are created. This boundedness afforded by the organisational context allows us not only to consider the commission, but also the antecedent stages as represented by readying, and how they themselves are created. Hence it is also possible to consider motivational factors. There is reason to believe, therefore, that appropriate prevention strategies could be implemented to negate those conditions that ready individuals. Even if the organisational conditions were such that staff were readied, it is possible that additional measures could be introduced to deter the offender prior to criminal decision making.

The fact that the organisational environment may provide both the setting in which motivational factors may be created and the crimes themselves enacted, marks a departure from the crime specific opportunity structure which reflects the traditional distinction between disposition and criminal situations. However, there is no reason why the model could not be adapted in future research to permit an appreciation of the relationship between context and motivation. The bounded nature of an organisation allows a specific focus for prevention programmes both in terms of context and with regard to the relative contemporary nature of readying factors. This is unlike the dilemma faced by most dispositional theories of knowing where, and at what point in time, to introduce measures to overcome 'causes' of criminality (Clarke, 1980).

Bonus System

While the organisational environment may foster situations which ready individuals, the very nature of the relationship between trading, profits and bonuses, which also exists in a banking environment, may additionally impact on the number of potential offenders. Successful trading leads to good profits and consequently good bonuses. However, one inherent problem of this relationship revolves around the issue of incentives. Commentators have noted how large bonuses can act as such a compelling incentive that securities staff may be tempted to trade recklessly (and ultimately criminally) in an attempt to secure enough profits to afford large personal rewards. Such was the case of Joseph Jett, a trader with the firm Kidder Peabody, who fraudulently created millions of dollars of 'profits' through derivatives trading to substantially boost his annual bonus (*The Independent*, 27 February 1995).

Although the BoBS report extensively addresses those factors that led to the collapse of Barings, there is very little coverage as to why Leeson actually carried out the unauthorised trading. Nevertheless, the inherent risks associated with the bonus system have proved to be a matter of some concern for the Bank of England. Four months after the collapse of Barings, the Bank of England issued a stern warning to the City's leading investment banks, citing the dangers of linking remuneration exclusively to short-term profits. The alternative it advocated was to consider bonuses based on an organisation's long term performance and stable profits (*Financial Times*, 15 June 1995). A similar warning was issued two years later after the National Westminster Bank uncovered a £50 million black hole in its options trading business (*The Guardian*, 1 March 1997).

It might be assumed that one way to eradicate the risks associated with bonuses would be to scrap the system altogether. But, as noted, this form of remuneration is seen as sacrosanct by traders and senior executives. Indeed, when Salomon Brothers attempted to restructure their system, tying bonuses to more long-term performance of the company, senior staff simply resigned, taking up new positions with rival firms (*Financial Times*, 15 June 1995). To complicate the issue and compound the problem, many City firms now use bonuses as a form of 'golden-handcuffs' in an attempt to avoid staff defections to their competitors. Firms have realised that rather than taking over or merging with a competitor as a means to increasing market share, it is far more commercially viable to simply buy up a competitor's trading team. These teams in their own right can bring with them a considerable amount of business, and the promise of guaranteed bonuses can act as an effective incentive (*Financial Times*, 3 March 1997). Hence, on closer inspection the bonus system is far more ingrained in the business practices of investment banks than maybe first thought. While the Bank of England, and more recently the Financial Services Authority, have considered and advocated alternatives, they are yet to convince the organisations they regulate that a different form of remuneration would be more suitable.

The crime specific model is unable to explain how the risks associated with the bonus system may impact on the number of potential offenders. This divergence between theory and practice can be explained by recognising the nature of the banking environment. As noted, banks and organisations generally represent a departure from the contexts traditionally addressed by the theories incorporated in the model. For while the banking environment, like the more 'traditional' contexts represents a domain where a crime can be enacted, it may additionally foster readying situations, and incorporate working practices underpinned by a remuneration system that can possibly induce reckless trading.

6.1.2 Socio-Economic Influences

The original opportunity structure (Clarke, 1995) also depicts how socio-economic factors in the form of sub-cultural influences, alienation, neglect and a lack of love can impact on the numbers and motivations of 'potential offenders'. The revised model has perceived these influences in terms of addictions, marital breakdown, financial problems and the like. As noted previously, there is very little in the BoBS report that addresses what motivated Leeson to undertake the unauthorised trading. Nevertheless, the related literature does support the need to recognise and consider factors which exist predominantly outside the work environment (e.g. a gambling addiction), but which reach such magnitude that they motivate an individual to commit a fraud in the workplace. Essinger (1990) notes:

> There are also insiders who commit computer crimes in order to provide the means to satisfy some dependency or other ... Drugs, sex and gambling also

> feature here as vices and / or addictions which may tempt a hitherto honest person to exploit the possibilities which he sees his job as offering.
> (Essinger, 1990, p. 40)

This assertion is further supported by Comer (1998) who also points to the fact that there is considerable variation with regard to the age of the fraudster and the amount of time they have worked for a company. The evolving and eventually insurmountable problems that addictions may cause an individual help to explain how a staff member may work honestly for several years and then commit a fraud.

Is it, however, feasible to perceive factors such as marital breakdown, addictions in their various guises and financial problems as socio-economic influences, given that they represent an obvious departure from the ones cited by Clarke (1995) in the original opportunity structure? They are perhaps better described by what Clarke and Cornish (2000) have more recently termed as 'current life circumstances'. This category is one item of the 'initiation' model advanced by the rational choice perspective. The perspective incorporates three stages of criminal involvement - initiation, habituation and desistance. The opportunity structure most clearly mirrors the initiation model in that just as the former depicts those factors that constitute an opportunity up to the point of commission, the latter represents those factors that influence a person's choice regarding whether they are going to begin committing crime.

Furthermore, decisions at each stage of criminal involvement are influenced by three groups of variables, described by Clarke and Cornish (2000) as :

1. *Background factors*, including personality and upbringing.
2. *Current life circumstances*, routines and lifestyles.
3. *Situational variables*, that include current needs and motives, together with immediate opportunities and inducements (Clarke and Cornish, 2000, p. 27).

More specifically, the 'current life circumstances' incorporates factors such as marital status, leisure pursuits, employment, drinks, drugs and gambling. There is considerable overlap here between the aforementioned factors and those cited in the crime specific opportunity structure under the heading of 'socio-economic' influences. While Clarke and Cornish (2000) argue that background factors are most influential at the initiation stage, they further recognise that with some types of crime these factors may carry less weight. Indeed, in their article *Situational Prevention, Displacement of Crime and Rational Choice Theory* (Cornish and Clarke, 1986) they specifically cite computer fraud as a case in point.

In some respects addictions, financial problems and marital breakdowns can be seen as crime specific socio-economic influences. Their importance in terms of potential motivational factors, and their similarities with current life circumstances have been noted. One notable departure, however, from the traditional socio-economic influences, is the relative potential for addressing the crime specific socio-economic influences. Essinger notes:

> What is surprising is that the personnel file on the insider fraudster very often reveals personal problems which go some way towards explaining the reason for the person becoming involved in crime ... our research tended to suggest that if a counsellor could be established in a bank to monitor personnel personal problems many insider frauds would not happen (Essinger, 1990, p. 40).

So although personal problems may occur outside the organisational context, there is some potential for recognising and addressing them within such a domain.

Under the headings 'unhandled offender' and 'socio-economic' influences, it has been noted how certain factors may impact on the number and motivations of potential offenders. By addressing these factors, the crime specific model can be seen to mirror traditional risk analysis logic, which Ciechanowicz (1997) states as:

- If a set of assets of a high value to an organisation
- and if the likelihood of a threat occurring is high
- and if there is a vulnerability that can be very easily exploited by the threat
- then the level of risk is high

(Ciechanowicz, 1997, p. 225)

In this sense, an 'asset' can be viewed as the 'target' and the 'threat' takes the form of the potential offender. Additionally a 'vulnerability' can be translated into a lack of 'guardianship'. Like routine activity, when these three elements meet in time and space, then the risk is high. But as routine activity also states, it needs only one of these items to be absent for no crime to occur. Or, to use the risk analysis terminology, without a threat (in the form of a potential offender) there is no risk. The need therefore to address these factors that impact on the numbers and motivation of potential offenders should not be underestimated, for as Bologna (1993) argues:

> If corporate fraud is to be prevented we must focus our attention on two factors:
>
> 1. The social psychology of the fraud perpetrators, that is, their motivations.
> 2. The control environment of the firm that employs the potential fraudster, that is, the fraud opportunities provided by non-existent or unenforced accounting and security control.
>
> (Bologna, 1993, p. IX)

6.1.3 Targets

The notion of a 'target' with regard to the opportunity structure derives specifically from routine activity theory, and can be seen as one of the elements that must converge in time and space for a crime to occur. Hence a target may be a person or object that is attacked or taken by the offender. This might include, for instance, a man the offender wants to rob or a car he wishes to steal. The original opportunity structure (Clarke, 1995) denotes how targets, such as banks and convenience stores, are the result of the 'physical environment'. For the crime specific opportunity structure, the physical environment translates into departmental offices, and the targets are viewed in terms of computerised systems. The Barings case, however, highlights a possible variation on the targets concept inscribed in the model. Owing to the paucity of information explaining why Leeson actually carried out the unauthorised trading, it is therefore difficult to identify the actual target. Why this is so can be explained by a discussion of the benefits derived from offending. According to Clarke and Cornish (2000), the rational choice perspective takes the position:

> ... that criminal acts are never senseless. To the contrary, they are purposive acts intended to bring some benefit to the offender. These benefits are most obvious when they come in the form of money or material goods, but they can also include excitement, fun prestige, sexual gratification, and defiance or domination of

> others. A 'wanton' act of smashing a window might actually be committed because of the fun of breaking something or the excitement of running away afterwards. A man might brutally beat his wife, not simply because he is a violent thug, but because this is the easiest way of getting her to do what he wants. 'Senseless' acts of football hooliganism or gang violence might confer considerable prestige on the perpetrators among their peers. The term *joyriding* accurately conveys the main reason why cars are stolen – juveniles enjoy driving around in powerful machines (Clarke and Cornish, 2000, pp. 24-25).

Although there is no hard evidence to suggest it, the obvious assumption would be that Leeson carried out the unauthorised trading for personal financial gain. Hence the 'target' in this sense would have been the ability to undertake the unauthorised trading, while the benefits represented monies derived from the unsanctioned business. However, in his book *The Collapse of Barings*, Fay (1996) argues that behind Leeson's illegal activities was the desire to become one of the elite traders on the floor of SIMEX. Leeson got to know some of these traders owing to the fact that the companies they worked for (First Continental Trading and Spear, Leeds and Kellogg) used Baring Futures Singapore for clearing their trades with SIMEX. Admiring the status and prestige associated with the elite brokers, Fay argues that Leeson was keen to emulate their activities and establish himself as a name on the trading floor. To do this, however, rather than taking the conventional route, Leeson carried out the unauthorised trading, creating fantastic 'profits' through dumping losses in account 88888.

In this sense, the benefit derived from trading was not the obvious one of money, but rather the benefits of prestige and status that were afforded the top traders. What the two benefits have in common is the nature of the target, which was the ability to undertake unauthorised trading. This represents a departure from the crime specific opportunity structure, which depicts targets forming part of the physical environment. Although 'ability' has a comparatively intangible nature, it can still be viewed as consistent with routine activity theory, which views a target as one of the elements necessary for the commission of a crime. The data not only supports this proposition but, if we subscribe to Fay's (1996) argument, it also provides a good illustration of the different benefits that may be accrued from the commission of a crime. In Leeson's case, as noted, these benefits included prestige and status.

6.1.4 Guardianship Factors

According to routine activity theory, what also determines a target is whether or not the entity, which forms the basis for a target, either lacks or has present, a capable guardian. Thus, for example, a house where the owner is present is afforded a capable guardian. If, however, the owner is at work, the property lacks a capable guardian and consequently represents much more of a target to a potential offender. This example illustrates how the majority of guardianship is traditionally provided by people. As Felson (1994) states:

> The most significant guardians in society are ordinary citizens going about their daily routines. Usually you are the best guardian for your own property. Your friends and relatives also can serve as guardians for your person and property, as you can for theirs. Even strangers can serve as guardians by being nearby and thus discouraging offenders (Felson, 1994, p. 31).

The original opportunity structure proposed by Clarke (1995) depicts the degree of guardianship in terms of 'lack of guardianship', noting how this presents a viable target for the potential offender. The revised crime specific opportunity structure makes a slight departure from its predecessor by incorporating into the model 'guardianship factors'. The intention here was to illustrate how a number of safeguards (such as internal/external audit. compliance monitoring, risk management, segregation of duties) can provide guardianship over the target in a banking environment. This is perceived as still being in keeping with routine activity theory, given that the presence or absence of the guardianship factors would determine whether an entity represents a viable target.

However, it should be noted that the elements that are considered 'guardianship factors' in the Barings case are of a far more complex nature than those traditionally recognised by routine activity theory. More specifically, *a priori* conditions need to be met before they can exist. Take for instance Baring Securities Limited's internal audit group. A management committee would have decided on its establishment, the size of the group, and the positions that would need to be created. The employment vacancies would be advertised, people interviewed and selected. Obviously, only after its inception could arrangements have been made for the group to carry out audits in Baring Securities Limited's various subsidiaries.

It is not unreasonable to expect the number and complexity of guardianship factors, given the nature of business undertaken and the type of crime committed in Barings. When Cohen and Felson (1979) first introduced routine activity theory, it was solely used to explain direct-contact predatory crime, defined as 'someone definitely and intentionally takes or damages the person or property of another' (Cohen and Felson, 1979: 589). In keeping with this, the example cited at the start of this section of the home-owner residing in their property demonstrates the relative simplistic nature of guardianship, when compared with a banking environment.

Of course, even if guardianship factors like the internal audit group are introduced into the banking context, there is no guarantee that their mere existence will provide effective guardianship over the target they purport to safeguard. Rather they have to exist and be working effectively. This last assertion can be seen as a slight departure from routine activity theory, which asserts that the existence of a capable guardian would deter a crime. Obviously of importance here is what exactly constitutes a capable guardian, but routine activity does emphasise how the mere physical presence/existence (as also noted with the handled offender) is often sufficient to provide the necessary guardianship. Hence the presence of an individual in their home is a good illustration. Yet in the case of Barings, the existence of a guardianship factor is not sufficient. They must exist and be effective.

It should be noted that the prolonged commission period of the Barings fraud makes it difficult to view the issue of guardianship solely in terms of the relatively simple crime 'equation' espoused by the routine activity approach. Additionally the theory asserts that when the elements of a crime meet in time and space, a capable guardian will deter a crime, or the absence of a capable guardian will lead to one. And yet, while there was a lack of guardianship in the Barings case to stop the actual commission, other guardianship factors were at work, albeit ineffectively, during the two years and seven months in which the unauthorised trading took place. Therefore, guardianship in the Barings case was not of a 'one chance' nature, unlike the more traditional crimes addressed by routine activity theory. A central factor here is the commission time. The 'more traditional' crimes have a short commission time (burglary would probably represent the most time consuming), while Leeson's fraud lasted for over two and a half years. Hence, in terms of Barings, capable guardianship could have been used to intervene in the actual commission process. For the crime specific opportunity structure, the issue of guardianship factors intervening in the commission process, however, is a non-issue, because the model is only able to address opportunities up to the point of commission.

6.1.5 Facilitators

The concept of facilitators was first broached by Clarke (1992) who advocates their inclusion by routine activity theory as a means of enhancing the contribution of this approach to crime prevention. The understanding is that if we appreciate how facilitators are used to commit crimes, possible points for introducing safeguards may be uncovered. Examples of this concept include cars, guns and credit cards, which are perceived as tools used by the potential offender for the enactment of specific crimes. Also included in this category are disinhibitors such as alcohol and other drugs, which facilitate the perpetration of crimes. The original opportunity structure (Clarke, 1995) depicts facilitators as coming from the physical environment. While this is acknowledged in the crime specific model, the internal threat posed by staff, and the organisational environment in which they work, places a different spin on the notion of facilitators. As Willison (2000b) asserts:

> It is true that the physical environment can provide facilitators in the form of standardised systems. If everyone in the same department uses the same type of machine with the same operating system and programmes, then this facilitates the potential offender since knowledge of multiple systems is not required and, as a consequence the offender already has the working requisite knowledge of their co-workers computer systems. More interesting perhaps is the idea that potential offenders acquire facilitators in the course of their work. Unlike their physical counterparts, these facilitators are cognitive in nature, and ... are assimilated by staff the day they begin working for a particular company.
> (Willison, 2000b, pp. 104 -105)

Essentially these cognitive facilitators include those skills and knowledge that a person acquires to perform their jobs. A key point here is that, although on the whole these skills are used by employees for perfectly legal activities, they can also be used to help facilitate activities of an illegal nature. Perhaps not surprisingly, the BoBS report highlights numerous instances of Leeson using his skills in this manner. Indeed, all his criminal activities were underpinned by knowledge initially acquired to support legitimate work. This is clearly revealed by the very fact that the report makes the distinction between authorised and unauthorised trading.

For Leeson, the knowledge required to undertake the unauthorised trading was gleaned not just from his experience in Singapore, but also in London where he had previously worked in the late 1980s and early 1990s. Barings Securities Limited had commenced trading futures and options in 1989. In the same year Leeson joined the department which dealt with the settlements side of this business, and began to develop an in-depth knowledge of these products. It was his expertise in this area that landed him the position in Singapore. Furthermore, while Leeson was acquiring the necessary skills and knowledge to undertake his duties, he was also acquiring an in-depth understanding of the work processes of which his duties were an inherent part.

While it has been noted how there was considerable confusion over Leeson's reporting lines, the cognitive facilitator (in terms of a detailed knowledge of Japanese derivatives) that he acquired during his career, acted as a layer of protection against management enquiries. For while Leeson had a sound knowledge of these products, the evidence suggests that the managers who were supposed to oversee his activities did not. Hence Leeson's relative monopoly of knowledge further mitigated against effective supervision. The BoBS report cites the position of Ron Baker:

> Although Ron Baker had had some involvement in the derivatives markets, he had not previously been involved in exchange traded futures and options of the kind conducted by the Structured Products Group (later renamed Equity Financial Products Group) in Japan, including the 'switching' business booked in Japan and London, but managed in Singapore. In interview, Ron Baker told us: "There is no doubt in my mind, that my lack of experience in the area was a contributing factor to what has happened here [the collapse] (BoBS, 1995, p. 28).

Simon Jones' knowledge of Japanese derivatives appears equally wanting:

> Tony Gamby, the global settlements director in London, thought Jones did not fully understand the complexities of futures trading, and relied on Leeson to explain it to him. 'He could have understood it if he'd wanted to, but he had no desire to. If Nick had said black was white, Jones would have believed him,' Gamby said later (Fay, 1996, p.128).

6.1.6 Search Perception / Information Modelling

Under the headings 'Search / Perception' 'Information Modelling', the crime specific opportunity structure denotes the potential offender searching the environment for targets, assessing potential risks, efforts and rewards, and considering facilitators. This section of the model acknowledges the considerable insight provided by environmental criminology into the 'search' patterns of offenders. More specifically, this body of knowledge illustrates how the majority of crimes are committed within areas visited by offenders during their routine work and leisure pursuits. As Brantingham and Brantingham (1991) assert:

> One of the striking things about criminals often forgotten, is that most of them behave as ordinary people most of the time. Most offenders are not tied exclusively to some home base, but, like other people, are mobile. They move about the city. They develop information about other parts of an urban area through working (even sporadically), travelling to school, shopping, or seeking out entertainment and recreation. Criminals will develop an action space based on both their criminal *and* their innocent activities. Their actions help form an 'awareness space', the parts of the city they have some knowledge about. Information about the urban area will be distorted by movement patterns. Criminal can thus be said to posses a non-uniform information base defined by their awareness space (Brantingham and Brantingham, 1991, p. 35).

Hence those areas of the urban setting, which the criminal is well acquainted with, represent what Brantingham and Brantingham (1991) describe as 'potential' spaces for criminal activity. Like the offender portrayed by the rational choice perspective, the motivated individual engages in a 'multi-staged decision process' prior to the commission (or not as the case may be) of a crime. This process is informed by knowledge gleaned by the offender from their 'awareness space'. More precisely, Brantingham and Brantingham argue that a particular environment emits 'cues' relating to its cultural, legal, psychological and spatial characteristics. Furthermore, these cues are used by offenders to help ascertain suitable targets. An offender learns with experience to recognise configurations and sequences of cues associated with a 'good' target.

Data from the case study appears to support the crime specific opportunity structure in depicting the potential offender as an individual who collates information from their awareness space and uses it for criminal purposes. Leeson's 'awareness space' encompassed the offices he routinely worked in. These included not only Baring Futures Singapore and SIMEX, but also Baring Securities Limited (London) where he had worked prior to moving to the Far East. While performing his day-to-day duties, Leeson was able to note any weak links in the control environment. The following example illustrates how during his time at Baring Securities Limited, where he worked in the settlements section of a department dealing in Japanese futures and options, Leeson amassed a detailed knowledge of the existing security loopholes. Furthermore, when he moved to Singapore, he used this knowledge to support his criminal activities.

Prior to the commencement of the unauthorised trading, Leeson opened account 88888 to help conceal his aberrant activities. Leeson knew from his time in London, that as with other accounts, the trading details of account 88888 would be sent by Baring Futures Singapore to London in the form of four reports, which included a trade file, which gave details of the day's trading activity; a price file, which reported on closing settlements price; a margin file, listing the initial – and maintenance – margin details of each account; and the London gross file, which provided details of BFS's trading position. In order to stop details of account 88888 reaching London, Leeson instructed Dr. Edmund Wong, a computer consultant, to omit details of the account from three of the four daily trading reports. The exception was the margin file. Leeson was aware that the margin file represented a security vulnerability for Baring Securities Limited, simply because it was routinely ignored by staff in London. Conversely, for Leeson, the margin file represented no risk with regard to helping to uncover his unauthorised trading, given the oversight by staff in London. As a consequence, he was able to ignore it.

It should be noted the extent to which cognitive facilitators and knowledge of the awareness space can be seen to work in tandem. Leeson had assimilated the necessary skills and knowledge in order to execute his legitimate employment responsibilities. This assimilation additionally encompassed a sound knowledge of the respective department's working process in which his own duties were inherently intertwined. At the same time, Leeson was also able to review the control environment of the offices which formed his awareness space. Hence, he had a detailed knowledge of not only how to undertake the fraud, but also of the control environment. Knowledge derived from these two areas provided Leeson with considerable leverage both prior to and during the commission of the fraud.

This distinction between the 'two areas' is necessary to highlight the different theoretical propositions inscribed in cognitive facilitators and environmental criminology. In practice with regard to Barings it is very difficult, if not impossible, to delineate the two. As Leeson acquired the skills necessary to undertake his work, he also earned an appreciation of the working processes of which his duties were a part. Importantly, however, as Leeson gained an understanding of how to execute his responsibilities and the related work processes, he was able at the same time to assess the control environment configured around the processes.

Of key importance here is the fact that Leeson worked for Barings. This represents a slight departure from the offender's circumstance traditionally found in the studies of environmental criminology. For example, Brantingham and Brantingham (1991) cite the work of Dufala (1976) whose study addresses convenience store robberies in Tallahassee, Florida. Dufala reports how, for marketing purposes, the stores were situated near major roads. As a consequence, these stores also formed part of the awareness space of offenders who, like many other urban residents, lived nearby. Leeson's position, however, would be more comparable to that of a clerk in one of the shops. Hence, learning his trade and developing knowledge of his target took place in the same context.

A related point concerns the quality of information that the offender is able to garner. Although an offender's rationality is addressed in the next section of this chapter, the concept of bounded rationality ties in nicely with the offender's circumstance. This form of rationality, advocated by Clarke and Cornish (2000), assumes:

> ... that criminal decision making is inevitably less than perfect, because it reflects imperfect conditions under which it naturally occurs. Because offending involves risk and uncertainty, offenders are rarely in possession of all the necessary facts about costs and benefits (the risks, efforts, and rewards of crime). Although they try to act as effectively as they can, choices may have to be made quickly and revised hastily. And, because there are constraints on human information processing abilities, criminals may use rules of thumb to guide their actions (Clarke and Cornish, 2000, p. 25).

Unlike the convenience store robbers studied by Dufala (1976), however, Leeson had access to a relatively high quality of information, which enabled him to assess more accurately potential risks, efforts and rewards. Access to such information was primarily due to the fact that he worked for Barings. His employment first with Baring Securities Limited and then Baring Futures Signapore also provided Leeson with both the necessary time and locations to collate the relevant information.

Another departure from the offenders studied by environmental criminology (SCP, routine activity and the rational choice perspective) is the extent to which Leeson was able to manipulate his environment to afford what Brantingham and Brantingham (1991) describe as a 'good' target. Although examined at greater length in the next section, Leeson was able, for example, to engineer a source of funding from London, which by-passed a potential safeguard in the form of a reconciliation between a request for funding and the trading account for which the request was made.

Furthermore, Leeson was inadvertently aided by senior management in his attempts to create an environment more amenable to his unauthorised trading. As noted, when Leeson first moved to Singapore he was placed in charge of the front and back office of Baring Futures Singapore. One of the golden security rules in the banking industry is that there should be a segregation of duties between these two positions. In other words no one person should be solely in charge of these two business sections. Placing an individual in charge of both gives that individual managerial responsibility for the whole trading process, significantly increasing the risks of fraud. Such risks are increased because a manager can sanction a trade (bear in mind that this 'trade' could be fictitious, unhedged, unauthorised and the like) from its inception to the time when it is settled by the back office. If Leeson had only been in charge of the front office, then a back office manager would have been in a good position to question his activities. Leeson's managerial position, however, denied this option.

6.1.7 The Rationality of 'Potential Offenders'

This chapter has already addressed those factors which may impact on the number of potential offenders, through a discussion focusing on 'handled offenders', 'readying', the inherent risks associated with the bonus system and 'socio-economic' influences. When addressing the last item on this list, it was noted how there was considerable overlap between the socio-economic influences incorporated in the crime specific opportunity structure and the 'current life circumstances' which forms one section of the rational choice perspective's 'initiation' model. The latter represents the first in three stages of criminal involvement, the others being habituation and desistance. At each stage the offender makes a series of choices, so with regard to the 'initiation' stage, potential offenders must make choices about whether they are prepared to undertake criminal activities to fulfil their demands (Clarke and Cornish, 2000).

Apart from making involvement decisions, the rational choice perspective asserts that criminals additionally make 'event' decisions which, as the name suggests, refer to those decisions made during the commission of a crime. Early work in this area focused solely on choices made in terms of the potential target (Clarke and Cornish, 1985: Cornish and Clarke, 1986) but as a result of theoretical advancements, it was realised that as the criminal act unfolds the perpetrator makes a series of event decisions based on the stages of a criminal act. Clarke and Cornish (2000) illustrate this form of decisions by way of example:

> In the case of a suburban burglary, the event may be sparked by some random occurrence, such as two burglars meeting up, both of whom need money. Plans begin to be made and a car and van may be stolen for transport. The next step involves travelling to the neighborhood selected and identifying a house to enter. Ideally, this holds the promise of good pickings, without the chances of being disturbed by the owners. A point of entry that is not too difficult or risky must

> then be found. Getting into the house and rapidly choosing the goods to steal follows this stage. The goods must then be carried to the car without being seen by neighbors or passers-by. Afterwards, they may have to be stashed safely while a purchaser is found. Finally, they must be conveyed to the buyer and exchanged for cash (Clarke and Cornish, 2000, p. 31).

In keeping with the original opportunity structure, the crime specific model views the offender as a rational decision-maker. Critics have questioned first the degree to which offenders are rational, and secondly, whether some crimes can be perceived as rational. There is, however, considerable evidence in the Barings case to support the rational choice perspective and this will now be discussed. As noted, while the crime specific opportunity structure depicts an opportunity up to the point of commission, and while the majority of the data in the case study actually discusses events during the commission, this does not mean the data cannot be used to illustrate the rational actions of Leeson. Having said that, the limitations of the model should be acknowledged.

Prior to the commencement of the unauthorised trading, Leeson clearly planned and executed actions that afforded the necessary conditions to initiate the unsanctioned business. One example concerns the manipulation of funding from London. When Leeson first started work at Baring Futures Singapore, he informed Gordon Bowser (Head of Futures and Options Settlements in London) that owing to the manner in which SIMEX made margin calls, it would be difficult for Baring Futures Singapore to raise in time the appropriate monies to meet the requests. Leeson argued that it would be far easier if the funds could be advanced from London prior to the margin calls. What Bowser did not know was that the 'problem' of meeting SIMEX margin calls was pure fiction on Leeson's behalf. Unfortunately, Bowser believed him and agreed to the request. This meant that Leeson could call for funds from London without specifying the trading account to which the request related. Through his careful planning, Leeson had gained a 'safe' source of funding. The reconciliation between accounts and funding would have proved a useful safeguard, but by succeeding in gaining advanced funds prior to margin calls, Leeson knew this safeguard would be negated.

During the commission of the fraud, Leeson continued to demonstrate the actions of a rational offender. When losses began to accrue as a result of his unauthorised trading, these were placed in account 88888. In order to hide these losses, and in order to avoid detection, Leeson created false journal entries, generated fictitious transactions and sold a large number of options. From early 1993 he masked the month end balance of the account by making a journal adjustment, crediting 88888 with a sum which would leave the balance at zero. He would then make an additional journal adjustment by debiting the same amount to the SIMEX clearing bank account maintained by Baring Futures Singapore. After the month end reconciliation, the transaction was simply reversed. Although this technique was used on numerous occasions to hide the balance of account 88888, another method involved the selling of options. Leeson would simply take the premiums collected through the sale of options, and offset this amount against the losses residing in 88888.

Apart from the evidence derived from the case study, writers in the field of computer crime implicitly acknowledge the rational choice perspective. According to Warman (1993):

> Given the opportunity and appropriate circumstances, most people will want to improve their situation. In some cases, personal gain may only be achieved by carrying out actions that would not otherwise be contemplated. The decision on whether or not to carry out their actions will largely depend upon the perceived balance or 'pay-off' between the gains and the risks (Warman, 1993, p. 27).

In direct relation to fraud, Comer asserts that:

> The fraudster has the motivation, initiative, time and the interest to pay attention to detail. He chooses the battleground, the weapons and the timing and strikes only if the risk-reward ratio is overwhelmingly in his favour (Comer, 1998, p. 7).

6.2 Related Themes

Aside from the specifics of the model, several related areas are addressed in the following section.

6.2.1 Holistic Nature of the Model

One of the key advantages of the crime specific opportunity structure is the holistic approach it takes to IS Security. The model is not only able to view the control environment, but also allows for consideration of the factors that create potential offenders. As mentioned, if the prevention of corporate fraud is a serious goal for organisations, they must not only focus attention on the control environment where opportunities may exist through non existent or inadequate safeguards, but consideration must also be given to motivational factors that lead people to perpetrate a criminal act (Bologna, 1993).

With specific regard to the control environment, the model views IS security as an 'in progress' phenomenon, and hence is able to address all the elements that constitute the control environment. This is unlike most writings in the IS security field, which are unable to address how elements relate and work together, owing to the fact that they are unable to account for social aspects which form a key part of the interactive process. Instead, their focus tends to rest solely on one aspect of the subject area, such as intrusion detection systems or firewalls. As noted in the literature review, Dhillon and Backhouse (2001) argue that one explanation for this apparent inability is largely a consequence of how information systems have been conceptualised, and this has ramifications for what is considered IS security. To support their argument, they use the paradigmatic framework devised by Burrell and Morgan (1979) to traverse the information systems and security literature. With regard to the information systems literature they point to an increasing dissatisfaction with the 'formal, rational and overly mechanical conception in the analysis and design of information systems' associated with functionalist thinking. Furthermore, Dhillon and Backhouse argue that this technical perspective suited a past era where organisations were predominantly hierarchical, and when the computer service provision was used to undertake a single function. Given the devolution of computing power in the new networked organisations, there has been an increasing recognition of the need to address the associated social factors that impact on the analysis, design and workings of information systems.

The literature on IS security has, however, been slow to recognise this need, with the majority of writings characterised by a technocratic orientation. Early security evaluation approaches and risk analysis techniques, followed by more recent security evaluation methods, are founded on functionalist conceptions. With the early work on security undertaken by the US military, the safeguards that were subsequently developed suited such environments. Organisations which mimicked the military environment, i.e. a hierarchical structure where information processing in centralised, were best suited to adopting the safeguards. But, as Dhillon and Backhouse argue:

> Problems arise when organisational structures become flatter and more organism-like in their nature. When this happens a broader vision for addressing security concerns is needed which address social grouping and the behaviour of people (Dhillon and Backhouse, 2001, p. 145).

The holistic perspective offered by the crime specific model provides an important insight into 'social grouping' and the 'behaviour of people' with regard to the workings of IS Security in an organisational domain. This is discussed in more detail in the following section.

6.2.2 The Pedagogical and Strategic Capabilities of the Crime Specific Opportunity Structure

The crime specific opportunity structure could potentially be used as a pedagogical tool. As noted when discussing the literature concerning opportunity, several writers have argued that within organisations, IS security is often seen as a purely technical concern (Wood, 1995; Parker, 1997; Osborne, 1998; von Solms, 2001). The downside with this perspective is that it fails to view the problem domain holistically and as a consequence fails to appreciate all the elements that constitute such an environment. Given that the crime specific opportunity structure is able to view the whole of the problem domain including the interaction between the potential offenders and their environments, the model would appear to be an ideal candidate for educating managers, and in particular those responsible for the allocation of budgets. Indeed Parker (1997) argues that a key role of security practitioners is to understand the perceptions of security held by managers and correct any unfounded beliefs. The model could act as a useful tool for correcting the purely technical security perspectives held by managers.

The model could further be used in education and awareness programmes for staff by emphasising their role in supporting guardianship. One of the problems faced by organisations is gaining employee co-operation in maintaining effective security. This is often the result of staff failing to appreciate the vital role they play and perceiving security as solely the task of those people directly responsible for security (Wood, 1995). However, one of the facets of the model is its ability to emphasise the centrality of staff behaviour in providing effective guardianship over an information system. Education programmes could for example highlight the need for compliance to local security policies and describe such a relationship in terms of the simple offender, target and guardianship relationship. Indeed, examples could be imported from criminology (e.g. guardianship over property and personal belongings) to help highlight the 'informal' role people can play in prevention programmes.

Given the holistic nature of the model and its ability to view security as an in-progress phenomenon, it could further be used as a conceptual tool for developing inter-departmental prevention strategies. Any attempt at combating fraud, for example, requires the joint efforts of a number of functions, including departmental staff, internal and external audit, personnel and IS security. One of the problems associated with inter-departmental prevention strategies is in conceptualising how all the functions should be working together. The crime specific opportunity structure can be viewed as a conceptual tool enabling organisations to identify the elements that afford a control environment, while additionally highlighting the relationships between them.

6.2.3 The Potential for Developing Generic Crime Specific Opportunity Structures

The idea of developing generic crime specific opportunity structures which may have utility for a number of organisations, is undermined by the idiosyncratic nature of such organisations. More specifically, these idiosyncrasies relate to the type of business undertaken by organisations, and how this business is performed. These two factors dictate the possible types of crime and the manner in which they can be undertaken.

Having said that, banking and securities business practices are becoming increasingly standardised. Probably the most influential factor with regard to standardisation is the degree of regulation imposed by the relevant parties. With the case of Baring Futures Singapore, for example, their business processes were heavily standardised by SIMEX. Each exchange in effect acts as a business facilitator by bringing together buyers, sellers and products. To ensure harmonious trading, exchanges govern such business via a rule-book (Fay, 1996). The SIMEX book stipulates the rules which trading parties must abide by in order to conduct business on the Singaporean exchange. The rules dictate, for example, when and how trading can take place. With each broking house complying to the exchange rules, standardised practices ensue. Furthermore, through standardised practices harmonious trading takes place.

Regulation further imposes standardisation in the internal controls of organisations. All the internal controls discussed in the BoBS report are common to banks and securities houses which trade on exchanges. Indeed, a number of recent cases (at least the ones known) have illustrated common security failures in such organisations. Perhaps more alarmingly is the fact that these controls have illustrated the absence or failure of even the most fundamental controls. Some seven months after the collapse of Barings, investigators uncovered a $1.1 billion loss created by Toshihide Iguchi, who worked for Daiwa, a Japanese bank (The Guardian, 27 September 1995). The parallels with Leeson are clear. Like Leeson, Iguchi worked in a subsidiary office (New York) trading on the local exchange. Like Leeson, Iguchi was placed in charge of the front and back offices, allowing him to carry out unauthorised trading and manipulating the associated computer ledgers. Like Leeson, the fraud was perpetrated over a considerable period of time. Indeed, while the unauthorised trading at Barings lasted for two years and eight months, Iguchi perpetrated his trading over an eleven-year period.

In August 1996, Kikuo Watanabe, a trader for New Japan Securities was found to have created thousands of pounds worth of losses through unauthorised trading on foreign exchange markets. Like Leeson and Iguchi, Watanabe worked in a subsidiary office (London), and had control over front and back offices (The Guardian, 22 August 1996).

More recently the Allied Irish Bank fraud highlighted failings that were common to the Barings collapse. In this instance the perpetrator was John Rusnack, who worked for Allfirst (an AIB subsidiary) in the Treasury Funds Management department. Rusnack was responsible for foreign exchange trading. Over a period from sometime in 1997 to February 2002, he accrued losses amounting to $691m through trading in Far East currency forwards, a type of derivative.

The most striking similarity between the Allfirst and Barings cases concerns the issue of supervision. When Rusnack joined Allfirst in 1993, he originally reported to a trading manager, who further reported to the treasury funds manager Bob Ray. When the trading manager left in the Autumn of 1999, Ray decided against hiring a replacement, and asked Rusnack to report directly to him. While Ray had many years banking experience, his knowledge of foreign exchange forwards was limited. As a consequence, supervision over Rusnack proved difficult. This scenario clearly mirrors events that occurred in Barings. When Ron Baker became head of the Financial Products Group, he found himself in charge of Leeson with regard to the arbitrage business conducted on SIMEX and the Japanese exchanges. While Baker had experience of derivatives, these were of the 'over-the-counter' variety, which are not sold on exchanges. He had therefore, little knowledge or experience of the exchange-traded derivatives, which formed the switching business undertaken by Leeson.

There is therefore some evidence to suggest that the idea of generic crime specific opportunity structures may not lack feasibility as first thought. In order to throw more light on this area, the way ahead may be to undertake a comparative study, which assesses commonalities between cases of specific types of crime. So, for example, a comparative study could be undertaken to assess the commonalities between cases of unauthorised trading.

6.2.4 Further Theoretical Benefits

The theories inscribed in the model do point to additional areas in which further research progress could be made in the IS Security domain. In the second edition of *Situational Crime Prevention: Successful Case Studies*, Clarke (1997) lists sixteen opportunity reducing techniques. These techniques are further categorised according to those elements central to a criminal decision, as advocated by the rational choice perspective. Hence, the techniques are designed to increase perceived *effort*, increase perceived *risks*, reduce anticipated *rewards* and *remove excuses*. The last category, removing excuses, acknowledges how some offenders assess their own morality, and are often able to absolve themselves of the guilt and shame associated with criminal acts. Such absolution is achieved by the individual rationalising (hence the 'excuses' referred to above) their actions, which further reduces their own feelings of culpability. Common examples of these rationalisations include 'I was just borrowing it' and 'everybody else does it'.

Two bodies of theory that have influenced both the Rational Choice Perspective and Situational Crime Prevention with regard to the phenomenon of rationalisations are Sykes and Matza's (1957) 'techniques of neutralisation' and Bandura's (1976) social learning theory, which incorporates the concept of 'self-exoneration'. Focussing on the area of juvenile delinquency, Sykes and Matza's starting point is to question the idea of a delinquent sub-culture in which the prevailing values represent an inversion of those held by 'respectable society'. This is rejected by the authors who argue delinquents show signs of commitment to the dominant social order by exhibiting feelings of guilt and shame when laws are broken. Furthermore, they often respect and admire figures who conform to the social order (e.g. a law abiding mother). Finally, delinquents often discriminate between what are perceived to be 'appropriate' and 'inappropriate' targets. Sykes and Matza illustrate this last point with the maxims 'don't commit vandalism against a church of your own faith' and 'don't steal from friends', indicating how some elements of the social order are deemed sovereign by delinquents.

The paradoxical question, which subsequently emerges, is that which asks why delinquency occurs if there is a commitment to 'the usages of conformity'? Sykes and Matza respond by arguing that much deviance is underpinned by rationalisations applied to a criminal act by the delinquent. These rationalisations negate the influence of internalised norms and social controls designed to inhibit aberrant behaviour. More specifically Sykes and Matza term these rationalisations 'techniques of neutralisation' and list five types, which include 'denial of responsibility', 'denial of injury', 'denial of the victim', 'condemnation of the condemners' and 'the appeal to higher loyalties'.

So for example, with regard to the 'denial of the victim', Sykes and Matza assert:

> Even if the delinquent accepts the responsibility for his deviant actions and is willing to admit that his deviant actions involve an injury or hurt, the moral indignation of self and others may be neutralized by an insistence that the injury is not wrong in light of the circumstances. The injury, it may be claimed, is not really an injury; rather, it is a form of rightful retaliation or punishment. By a subtle alchemy the delinquent moves himself into the position of an avenger and the victim is transformed into a wrong-doer (Sykes and Matza, 1957, p. 668).

Another variation on this theme refers to how the circumstances of the deviant act may lead the delinquent to deny the existence of the victim. If the victim is unknown, absent, or a 'vague abstraction' (commonly the case with property crimes), their existence is marginalised, making it easier for the delinquent to perceive their actions as victimless.

Bandura (1976) attempts to explain aggression through the application of social learning theory. Dividing such an explanation into three areas, he examines how aggressive patterns are created, the factors that provoke aggressive behaviour from people, and how behaviour of this kind is maintained over a period of time. With regard to the maintenance of aggressive behaviour, he discusses how 'self-reinforcing' influences, which help to regulate an individual's conduct, can be divorced from aggressive actions. This, Bandura argues, is achieved through engaging in 'self-exoneration' practices, which include 'reconstructing aggression by palliative comparison', 'justification of aggression in terms of higher principles', 'displacement of responsibility', 'diffusion of responsibility', 'dehumanization of victims', 'attribution of blame to victims', and 'misrepresentation of consequences'.

In terms of the 'displacement of responsibility', for example, Bandura argues:

> People can be led to behave in an injurious way provided that a legitimate authority is willing to assume responsibility for their actions. Participants in studies who have been deterred from intensifying obedient aggression by distress over the suffering they have inflicted, continue to escalate shocks to hazardous levels despite their victims' agonizing cries, after the experimenter has assured them he will be fully accountable for the consequences of their behaviour (Bandura, 1976, pp. 225-226).

As can be seen, there is considerable overlap between the two bodies of theory. Although Sykes and Matza and Bandura address delinquency and aggression respectively, there is no reason why their work should not be applied to IS Security to help explain and analyse the actions of staff. There is some evidence to suggest that rationalisations were at work in Baring Futures Singapore. With regard to 88888 it has been noted how back office staff were aware of its existence, as their daily routines often led them to booking and making adjustments to trades in the account. Additionally, the BoBS report indicates that Baring Futures Singapore's floor traders were 'likely' to know of the account for during their daily routines the preparation of a 'daily blotter' involved summarising the trading activities. Despite the fact that the front and back office instructions from Leeson may have been perceived as unusual, particularly during the last few months prior to the collapse, none of the aforementioned staff raised any concerns with senior managers. Could it be that these actions represent what Bandura describes as the 'displacement of responsibility', where Leeson informed his staff that he would take full responsibility for any adverse consequences? For as noted, Bandura argues 'People can be led to behave in an injurious way provided that a legitimate authority is willing to assume responsibility for their actions'.

In this sense, techniques of neutralization and self-exoneration could possibly make a contribution to the theoretical underpinning of prevention programmes. The above example points to the need to make staff aware of their responsibilities and accountabilities. In other words, employees should not be allowed to 'pass the buck'. This is confirmed in the literature on fraud (Comer, 1998), but whether such literature is informed by theories proposed by the likes of Sykes, Matza and Bandura is debatable. Further research into this area could prove highly enlightening for IS security practitioners.

6.3 Conclusion

The first section of the chapter addresses the theoretical coherence of the model, using the Barings case as a 'test bed'. Hence the theoretical propositions, concepts and the relationships between them are examined. It is noted how some of the concepts, notably the 'intimate handler', the 'handled offender' and 'guardianship' lack the necessary sophistication to appreciate the complexity of the organisational context. That said the majority of concepts and their related propositions are easily transferred into the IS domain. The Barings case and related writings further illustrate how the organisational context can motivate individuals into perpetrating some form of computer abuse. Although this represents a departure from the crime specific opportunity structure, there is no reason why the model could not be adapted to consider the influence of the organisational environment on criminal motivations.

The second section of the chapter addresses related themes. It is noted how one advantage of the model is the holistic approach it takes to IS security, viewing the aforementioned as an 'in-progress' phenomenon and, by so doing, affording consideration of all the elements that constitute the control environment. The model, therefore, could be used to underpin education programmes, or as a conceptual tool for developing interdepartmental prevention strategies. The potential for developing generic crime specific opportunity structures is also discussed, with the final theme highlighting how theories inscribed in the model point to possible future research in the IS security domain.

Chapter Seven: Conclusion

This final and concluding chapter is divided into four main areas. It opens with an overview of the dissertation, and then moves on to address the contributions of this research in terms of their theoretical, methodological or practical nature. The third section of the chapter examines the implications of the research approach in terms of design limitations and the adequacy of the theoretical framework. The fourth and final part examines the potential and scope of future research in this area of study.

7.1 Overview of the Dissertation

In the opening chapter the motivations for and scope of the research are discussed. This is followed by a definition of what is understood in this research to be an IS and hence what constitutes IS security. The current status of IS security research is then discussed with the penultimate section of the chapter examining the objectives of the study. The final section provides a description of the thesis structure.

Chapter Two reviews the literature on opportunity. Those texts which directly address opportunity can be seen to divide into two distinct groups. First there are those which address how opportunities may act as a motivational factor with regard to individuals. The second group focuses on how opportunities are created through deficient security. More precisely, this literature examines how opportunities are created through the absence, poor implementation and maintenance of safeguards. Although the existing literature highlights the problem areas associated with opportunity, there are a number of deficiencies. First, there is little written on opportunity. This is probably due to the fact that the meaning of the term opportunity is regarded as obvious and hence there seems little reason to examine the subject. Secondly, there has been a failure to define what is meant by the term 'opportunity'. The final deficiency is the existing literature's prescriptive value. A flawed understanding of the term offers little scope for developing effective prevention programmes.

The theoretical framework assessed in the thesis is introduced in Chapter Three. The chapter begins by discussing a criminological school of thought known as situational crime prevention (SCP). A central aim of this approach is to reduce the opportunities for crime. The chapter then moves on to describe a number of similar theories which have proved influential in the development of SCP. These include the rational choice perspective, environmental criminology, routine activity theory and lifestyle theory. The rational choice perspective focuses on the decision-making processes of offenders with regard to their criminal careers and the actual perpetration of crimes. Considerable insight into the search patterns of offenders has been provided by environmental criminology, highlighting how much criminal activity occurs in areas visited by offenders during their everyday work and leisure pursuits. Routine activity theory addresses the 'chemistry' of crime by looking at the minimal elements required for perpetration. The final theory examined in this section, lifestyle theory, looks at the relationship between the risks of victimisation and people's exposure to potential offenders. In essence, a person's lifestyle activities may increase their exposure to offenders and possibly victimisation. An attempt to synthesise these theories in the form of the 'Opportunity Structure for Crime' is then described. The chapter then moves on to describe a number of changes made to this model, culminating in a description of the 'Crime Specific Opportunity Structure', which represents the theoretical framework assessed in the current research.

The Fourth Chapter describes the research methodology. The first section examines the philosophical assumptions of the research, drawing on the interpretive and, more precisely, the hermeneutic tradition. The reasoning behind these choices is discussed. The chapter then describes the research strategy used in the study, namely an ethnographic approach. Several central, defining characteristics common to ethnographic research are examined followed by a review of the IS ethnographic literature. Contributions and limitations of this approach are highlighted, leading to an examination of why an ethnographic, and, more specifically, a document-based ethnographic approach was chosen. This section of the chapter ends with a debate centring on the utility of this approach in terms of scholarly contribution. The last part of the research methods chapter describes the data collection and analysis techniques. With regard to data collection three sources were used to construct an account of the collapse of Baring Bank. These include the Board of Banking Supervision report, books and newspaper articles. A discussion then focuses on the relationship between the researcher and the texts that constituted the data sources. Drawing on hermeneutic philosophy, the chapter examines how the use of written sources does not mean that the subsequent work based on them is limited by definitive and static meanings that reside in an author's text. Rather, meaning is disclosed in the process of reading by whoever chooses to read the text. The data analysis section examines how information from the sources was assimilated by the researcher in terms of reading and note taking with the aim of eliciting the appropriate information on which to base an account of the collapse of Barings.

The account of the fall of the bank forms the Fifth Chapter. The chapter opens with a brief history and background to the development of Barings bank, including the purchase of a fifteen man trading team which formed the nucleus of Baring Securities Limited. The expansion of this company and its relationship with its banking counterpart, Baring Brothers & Co., is discussed, followed by an examination of the merger of these two companies to form Baring Investment Bank. During the expansion of Baring Securities Limited one of the subsidiaries opened was Baring Futures Singapore. The creation and management of this subsidiary is discussed. Leeson was a key figure in Baring Futures Singapore and the confusion over job responsibilities and the associated lines of management are addressed at length. The chapter moves on to address the authorised trading activities on the Singapore and Japanese exchanges followed by a description of the unauthorised trading conducted by Leeson on SIMEX. The methods he used to conceal the latter are then discussed with the next section examining the failings in the control environment which afforded Leeson the ability to draw on the capital of Baring Securities Limited. The failings in the internal controls of a number of Barings' companies are subsequently examined with the next two sections of the chapter discussing the internal and external audits of BFS. The penultimate section highlights the regulation of the relevant Barings companies by the SFA and the Bank of England. The chapter ends with a summary of the main points.

The discussion and analysis section forms Chapter Six of the thesis. This chapter assesses the feasibility of a crime specific opportunity structure. The opening section addresses the theoretical coherence of the model. Using the Barings case as a test bed, the chapter examines whether the propositions and concepts inscribed in the model hold theoretical water when applied to the case study. Using data from the case study each element of the model is duly assessed. Where relevant, the relationships among the elements of the model are also examined. The chapter then examines related themes. The main areas for discussion in this section include the holistic nature of the model, the potential pedagogical and strategic capabilities of the model, the feasibility of developing generic crime specific opportunity structures, and the potential for future IS security research based on theories inscribed in the model.

7.2 Contributions

This section of the chapter discusses the contributions of the research. Grouped into three areas, which are now described, these contributions are theoretical, methodological or practical in nature.

7.2.1 Theoretical Contributions

One of the deficiencies with regard to the literature on opportunity is the lack of material that focuses on the subject. This is probably due the fact that the meaning of the term 'opportunity' is regarded as obvious and hence there is little reason to examine the subject. However, the importation of criminological theory, in the form of the crime specific opportunity structure for crime provides a new perspective and hence insight to the problem of opportunity. In consequence, another deficiency of the existing literature is that it fails to define what constitutes an opportunity. The crime specific model is not only able to provide a definition, it is also able to help conceptualise the constituent elements. More specifically, the various theories inscribed in the model each contribute to an understanding of the concept, and these contributions are now discussed.

The rational choice perspective provides insight into the decision-making processes of rogue employees. One of the deficiencies with regard to the common-sense approach to opportunity is that it cannot explain why some opportunities are acted on in some instances and not in others. This points to the interplay of other factors, most notably the role of the agent, which the common-sense view is at a loss to explain. The rational choice perspective is able to explain the variance in terms of criminal decision making. Hence a situation offers an opportunity in terms of the risks, efforts and rewards perceived by the offender. In this sense an opportunity is a subjective relationship between the criminal and their environment. Furthermore, even though a situation may offer the makings of an opportunity e.g. a house with a window left open, if there is no offender present, there is no opportunity because it is ultimately the offender who decides whether the situation offers an opportunity.

Data from the case study supports the idea of a rational offender. Leeson clearly planned and executed actions that allowed him to initiate his unauthorised trading. During the period in which his aberrant trading took place, he continued to demonstrate the actions of a rational offender. When losses accrued as a result of the trading, not only did Leeson place them in a specially designated account (88888), he also instigated actions to hide the losses and avoid detection.

The Routine Activity approach contributes significantly to the theoretical underpinning of the crime specific model. In respect of the issue of supervision, this school of thought depicts such a relationship in terms of the 'intimate handler' and the 'handled offender'. The application of this concept offers some insight into the management problems experienced by Baring Futures Singapore. Routine activity theory asserts that an offender must be lacking an intimate handler for a crime to take place. To some extent this mirrors the problems experienced by the Singaporean subsidiary. Leeson was afforded little supervision and hence was provided with a relatively free hand to undertake the unauthorised trading. However, as we shall see later, the aforementioned theoretical constructs lack the necessary sophistication to appreciate the complexity of the supervisory relationship both at Barings and in organisations generally. As a consequence, 'insights' into the failings of supervision afforded by the 'intimate handler' and the 'handled offender' are found wanting.

The concept of targets is likewise drawn from routine activity theory. Traditionally, examples of this concept take a physical form, including cars to steal, banks to rob and houses to burgle. Although the target in the Barings case proved to be the ability to undertake trading, and hence represents a departure from its physical counterparts, this is still consistent with routine activity's theoretical proposition, which views a target as one of the elements necessary for the commission of a crime. Hence, if appropriate controls were in place, then the ability to undertake unauthorised trading would not have been a suitable target, owing to the presence of appropriate levels of guardianship.

As noted above, the degree of guardianship determines what constitutes a target. The crime specific model depicts this concept in terms of 'guardianship factors'. The intention here was to illustrate the plethora of safeguards found in an organisational environment. While the Barings case supports the proposition that their absence would provide a lack of guardianship, as will be discussed later, this concept is viewed to be inadequate when applied to the organisational context.

The final major input from routine activity with regard to the crime specific opportunity structure relates to facilitators. Traditional examples of this concept have taken a physical form, including for example, cars for get-aways, guns for the commission of armed robberies, and stolen credit cards for the perpetration of retail fraud. While acknowledging the tangible nature of some facilitators, the crime specific model further incorporates the intangible cognitive facilitators. Data from the case study provides ample evidence of these mental facilitators at work. Given the nature of the crime perpetrated at Barings, it is reasonable to suggest that the skills and knowledge Leeson acquired to perform his work acted as a 'tool' for the perpetration of the unauthorised trading. Indeed, any understanding of computer crime must be able to account for and consider how cognitive facilitators are used for the commission of such crimes. In this sense, the facilitators concept is easily translated into the field of IS security.

Environmental criminology provides additional insight into how knowledge acquired by the offender is used for illegal purposes. This area of criminology helps to focus attention on the search patterns of offenders in their everyday 'action' and subsequently 'awareness spaces'. Furthermore, environmental criminology highlights how offenders glean the necessary knowledge from their awareness space with regard to the security provisions of potential targets. Like facilitators, the theoretical concepts of environmental criminology, depicted in the model as 'search-perception / information modelling', are easily translated into the IS security field. The Barings case provides supporting evidence, illustrating how knowledge of security provisions was used by Leeson to his advantage. The search patterns of offenders, married with cognitive facilitators, provide a useful theoretical grounding in understanding how a rogue employee combines knowledge of the environment with the skills acquired through work to perpetrate a fraud.

The rational choice perspective in conjunction with environmental criminology can further help to explain how the quality of information to which employees have access can lead to the perpetration of frauds over considerable periods of time. The concept of bounded rationality asserts that criminal decision making is impaired by the quality of information to which the offender has access. The Barings case, however, illustrates how employees have access to a relatively high quality of information given their circumstances. Another recent example was provided by the Allied Irish Bank fraud. John Rusnack's knowledge of back office vulnerabilities acted as one of the factors which enabled him to undertake unauthorised foreign exchange trading leading to losses of $691 million over a four year period.

The theories inscribed in the crime specific opportunity structure point to additional areas in which research progress could be made in the IS security domain. As noted, the opportunity reducing measures advocated by SCP are categorised according to those elements central to a criminal decision making espoused by the rational choice perspective. Hence the measures are designed to increase perceived *effort*, increase perceived *risk*, reduce anticipated rewards and remove *excuses*. The last category, removing excuses, acknowledges how some offenders assess their own morality, and are often able to absolve themselves of the guilt associated with criminal acts. This is achieved through rationalisations such as 'everybody else does it', which reduces feelings of culpability. This rationalising process has been explained by Sykes and Matza (1957) and Bandura (1976) who discuss 'techniques of neutralization' and methods of 'self exoneration' respectively. There is some evidence to suggest that these type of rationalisations were at work in Baring Futures Singapore. Future research which examines this phenomenon in the organisational domain could prove fruitful for academics and security practitioners. A clearer understanding of the rationalisation process could reinforce IS security efforts by highlighting related points for prevention. Hence, the importation of this body of theory from criminology could assist both academic, and ultimately, practitioner progress in the IS security field.

Such importation of theory would prove timely for as discussed earlier, one of the general deficiencies of IS security is the lack of theory both used and advocated by academics in the field. The position taken in this research is that in order to understand computer crime and computer criminals, the academic discipline which can provide substantial insight into this area is criminology. Given the multi-disciplined nature of criminology, drawing from psychology, sociology, law, social policy and economics, it can be seen to provide a voluminous body of knowledge which IS academics can utilise. The current research indicates how common-sense perceptions of concepts can fail on closer scrutiny. Furthermore, this study illustrates how the fertilisation generated by criminological theories applied to IS can provide new perspectives and insights, leading to potential advancements in addressing existing and emerging security issues. Until now the application of criminological theory to the IS security field has been minimal. Indeed, the author is unaware of any texts from the field that draw on the discipline. One of the contributions of the current research, therefore, is the importation and advocation of criminological theory for IS security research.

From another perspective, the importation of criminological theory into IS security can be seen as a contribution to criminology itself. The subject field of computer abuse is a relatively unexplored area for criminology and in this sense the current research acts as a contribution to the existing and under-developed knowledge base. The use of such theory in new contexts further enables the possibility of expanding and enhancing existing themes and concepts. The concept of cognitive facilitators is a case in point. The world of banking highlighted by the Barings study represents a marked departure from the environments traditionally addressed by approaches such as routine activity theory. Hence the banking context afforded consideration of the facilitators used in this environment. After further reflection it was deemed reasonable to consider the skills and knowledge acquired by an employee as a type facilitator, albeit of the intangible variety.

7.2.2 Methodological Contributions

This research is founded on the belief that if we are to understand the true nature of security problems that IS face, we must be able to examine the whole of the problem and view IS from a socio-technical perspective.

Furthermore, an interpretive position was adopted. If we subscribe to the socio-technical perspective, then insight into the social reality that prevails within the workings of information systems can be garnered by understanding the existing social reality, which is constructed through shared and negotiated meanings, and as a consequence, the countervailing social reality. Those interpretive researchers who take the view that to understand IS you must also address the social context have increasingly turned to ethnography as a suitable qualitative approach, and this is the approach used in the current research.

The ethnographic approach was adopted primarily for its ability to afford an holistic perspective of an organisation. For the majority of organisations, security practices are an inherent part of their everyday working life. An appreciation of these practices (and the associated safeguards) and the interrelationships between them is vital for understanding the IS security domain. Consequently, given their ramifications and impact on other areas particular aspects of security cannot be studied in isolation. The ethnographic approach was deemed a suitable research method given the insight it affords into the human, social and organisational aspects of an IS. Such an approach further allowed for an appreciation of working practices in a real world setting and is in keeping with the assertion that security practices cannot be studied in isolation given their interrelated nature. Finally, the ethnographic approach was chosen for its ability to encompass multiple perspectives which underpin the principle of 'thick-description'. These multiple perspectives enable a consideration of potential areas of conflict, ambiguity and misunderstandings. This was certainly the case with regard to Barings where conflicts, ambiguity and misunderstandings exerted considerable impact on the efficacy of the control environment.

The reasons for adopting a document-based ethnography were influenced by pragmatic criteria, but also by developments in the field of anthropology and ethnography. Given the difficulties with access that researchers experience in the IS domain, and particularly those who focus on security, the use of the document-based approach in the current research can be seen as a pro-active solution to the challenge of access. As noted in the methodology chapter, there is an existing body of literature which supports, and by so doing legitimates, the methods used in the study. The document-based ethnography can therefore be seen as a positive scholarly contribution.

7.2.3 Practical Contributions

The practical contributions of this research stem primarily from the theoretical importation of criminological theory into the IS security domain. One consequence of this fertilisation of knowledge is that the crime specific opportunity structure is able to take an holistic approach to IS security. Not only is the model able to view the control environment, it also affords consideration of those factors that create potential offenders.

Most writings in the IS security field are unable to account for the interaction between those elements that constitute a control environment. This is due largely to their failure to account for the social aspects which form a key element of the interactive process. Hence the emphasis of these writings tends to be on one single area, such as firewalls, intrusion detection systems and the like. The crime specific model, however, is able to view security as an 'in-progress' phenomenon and can therefore account for those elements that provide guardianship, and the interaction between them.

Given that the model is able to view those elements that constitute security and how they interact, it could potentially be used for developing inter-departmental prevention strategies. More specifically, the model could address the increasingly topical issue of operational risk. This form of risk encompasses the threat from rogue employees. Efforts to combat such a threat require input from a number of departments/functions, including external/internal audit, compliance, information security and personnel.

However, one of the major problems organisations face is being able to conceptualise how all the aforementioned parties work together, while accounting for the potential threat from potential offenders. The crime specific model can therefore be seen as a strategic tool, which allows for an inter-departmental/functional conceptualisation of the control environment, and one which encompasses and hence considers the insider threat.

Apart from offering an in-progress and holistic view of the security domain, the crime specific model also offers practitioners a theoretical grounding with which to enhance prevention programmes. The rational choice perspective, for example, provides a useful insight into the criminal decision making process. The theories inscribed in the model are relatively 'user-friendly' and could be translated into a series of principles for those responsible for security.

Another possible contribution offered by the model relates to its pedagogical capabilities. One problem that exists in many organisations concerns the perceptions of security held by managers. More specifically, security is often perceived as a purely technical matter. This myopic perspective is unable to view the whole of the problem domain and thus fails to appreciate all the elements that constitute the security environment. The associated risk is that safeguards implemented from a technical perspective will fail to address all the elements that need securing. As one of the advantages of the crime specific opportunity structure is its holistic perspective, it could feasibly be used as an educational tool in helping to correct limited perceptions of security held by managers. Furthermore, the model could help to illustrate the insider threat from dishonest staff. Another common misconception held by managers is that risks to IS come solely from external threats, and principally in the form of hackers. However, the threat from inside an organisation should not be underestimated. Certainly the largest frauds have been committed by staff, who as noted, are in a 'privileged' position in terms of assessing the control environment and utilising their skills and knowledge for criminal purposes.

The model could additionally be used as a means for raising the awareness of staff with regard to their central role in maintaining security. Organisations often find it difficult to establish and maintain end-user co-operation with regard to IS security initiatives. This is partly due to staff undervaluing their importance in such initiatives and perceiving security as a marginal function, carried out by specialists. However, one advantage of the model is its ability to explain the importance of staff compliance in providing effective guardianship and further highlighting the consequences of its absence. Indeed, practitioners could use examples drawn from criminology, such as a homeowner, providing capable guardianship over their property, to illustrate the 'informal' and necessary preventive role enacted by individuals.

7.3 Implications of the Research Approach

7.3.1 Research Design Limitations

The reasons for adopting and developing the document-based ethnographic approach were led primarily by pragmatic criteria. Achieving access is difficult enough for researchers, but when a proposed study aims to address IS security issues, it becomes even harder. Organisations are particularly sensitive about their reputation, which can be easily damaged through adverse publicity. In consequence many companies view research into organisational security as a potential risk in its own right.

This desire for organisations to protect their reputations could prove problematic for the development of document-based ethnographies into an established research approach. Obviously for ethnographic accounts to be developed using this approach, the researcher requires access to a considerable amount of secondary data. With regard to the Barings case, this proved to be unproblematic. It should be noted that this was an extremely high profile case, particularly given the collapse of the bank. As a consequence the amount of material open to the researcher was voluminous. Unfortunately, this may not be true for other cases of computer fraud or computer abuse generally. Because companies are so concerned about their reputation, if some forms of computer crime do occur, they more often than not prefer to deal with the matter in-house, avoiding law enforcement involvement and the potential publicity that may ensue. Hence it is debatable whether cases which provide the necessary material for research will come to light in the future.

Having said that the document-based ethnographic approach could be adopted by other IS researchers whose interests lie outside the field of security. One area that comes to mind is that of IS implementation. An example of implementation that could be studied by using this approach is that of the London Ambulance Service, which experienced a failure of its Computerised Despatch System in 1992.

7.3.2 Adequacy of the Research Framework

Despite the theoretical contributions of the crime specific model, discussed in the previous section, there are three areas of the theoretical framework which are open to criticism. First, some of the concepts inscribed in the model lack the necessary sophistication for application to the organisational domain. Secondly, the model is unable to consider how the workplace environment can engender criminal motivational factors. Thirdly, the model cannot address collusion.

One of the primary deficiencies of the crime specific opportunity structure concerns the sophistication of some of the concepts inscribed in the model. It was noted how the concept of 'handling' allowed some insight into the supervision afforded Leeson by highlighting how the lack of management overview (i.e. the absence of a handler) provided him with a relatively free hand to undertake the unauthorised trading. Hence, the concept of handling emphasises the primacy of physical presence in deterring offending. However, the Barings case illustrates how it was not only the lack of a supervisory presence that benefited Leeson, but also the fact that when he was supervised, the managers responsible had a limited knowledge of the products he traded in and the business processes which underpinned such trade. The form of 'supervision' espoused by routine activity is left wanting when applied to the supervision typically found in organisations.

This lack of conceptual sophistication is further evident when discussing the issue of guardianship. Traditional examples of this concept emphasise how the physical presence of an individual can provide 'capable guardianship' over a potential target. When applied to the Barings case, the relative 'crudeness' of the concept becomes evident. First, the case demonstrates the plethora of safeguards required in a banking environment, and in consequence more than one factor determines guardianship.

Secondly, *a priori* conditions need to be met before guardianship factors can exist. The discussion and analysis chapter cites the example of internal audit. A management committee would decide on its establishment, advertise the positions and select the necessary staff. Thirdly, even if such functions exist, there is no guarantee that they will provide effective guardianship.

A determining factor in the utility of the handling and guardianship factors is the complexity of the crime to which they are applied. Routine activity when first advocated restricted its application to 'direct contact predatory crimes' i.e. where one or more persons directly take or damage the person or property of another. This is a far cry from unauthorised trading on SIMEX. However, when discussing the usefulness of the aforementioned concepts, the issue of granularity should be introduced into the debate. The Barings case is extremely detailed, encompassing many individuals and organisations, and as noted certain elements of the model find it difficult to accommodate such complexity. That said, the model might prove more fruitful when applied to less complex cases of computer abuse.

The second deficiency of the research framework concerns the inability of the model to explain how the organisational context might promote criminal motivations. The discussion and analysis chapter cites how these motivations may be the result of poor working relations, or through the nature of business enacted in organisations which may tempt criminal behaviour. In terms of the former, theories such as routine activity theory and environmental criminology focus on the setting in which criminal activity takes place. Traditionally, motivational or background factors are examined by dispositional theories. As mentioned the organisational context represents a unique hybrid of the two positions, for not only can the organisational environment provide the necessary setting in which crimes can be enacted, it can also provide the environment in which criminal motivations may be fostered. Hence, certain situations in organisations, such as a rumour of job cuts, being passed over for promotion or carrying an unfair workload, may 'ready' an individual for some kind of computer abuse. In terms of the organisational context, there is evidence that the bonus system of remuneration, common in the banking world, can promote reckless trading. Owing to the fact that successful trading leads to good profits and subsequently good bonuses, there is a flaw in this relationship. Trading staff may be tempted to trade recklessly in an attempt to boost their profits which then translate into larger bonuses.

Given the generic origins of the model, it may be overly harsh to cite the above two areas as deficiencies, for it is expected that if any future crime specific opportunity structures were to be developed, such structures would have to be adapted to represent the idiosyncratic nature of the very thing it was to model, that is a specific crime. Additionally, any crime specific model created, which incorporates the organisational domain could, if necessary, be adapted to represent the appropriate context.

The third major deficiency is that the model is unable to address collusion between rogue staff. Central to the crime specific opportunity structure is the sole potential offender who searches the environment, collating information and making criminal decisions based on such information. Cases of fraud and other forms of computer abuse, do, however, provide evidence of collusive practices, where two or more employees work together to perpetrate a crime. These types of criminal relationships cannot be addressed by the model. That said, the research framework, if adapted could possibly account for the reasons behind such actions. As noted in the discussion and analysis chapter, the readying concept could be incorporated into the crime specific model to aid understanding of how organisational environments can actually evoke motivational feelings. For example, the threat of job cuts may engender, not only in an individual, but also individuals, feelings of misplaced trust, resentment and betrayal. A greater understanding of when and under what circumstances readying situations occur may lead to a more informed understanding of prevention points. The hope would be that readying situations are negated or handled to stop feelings of resentment being translated into criminal actions.

7.4 Areas of Further Research

The potential for developing crime specific opportunity structures was considered in the discussion and analysis chapter. Although the idiosyncratic nature of organisations appears to mitigate against such structures, it was noted how practices in the banking world are to some extent standardised through the stock exchanges on which they trade and the associated regulators which oversee this form of business. Furthermore, it was noted that future research to address the feasibility of generic crime specific opportunity structures could take the form of a comparative study. Hence, for example, such a study could be undertaken to review the common denominators in cases of unauthorised trading. Research in this area would help to assess the generic or idiosyncratic nature of those factors that led to unauthorised trading in the specific cases. The examples of unauthorised trading cited in the discussion and analysis chapter indicate common failings in the most fundamental controls. Whether other cases would share common failings, and therefore point to the benefits of generic crime specific structures, would be the focus of further research in this area.

Another area for future research would be to address the theoretical shortcomings of the model. As noted when discussing the adequacy of the research framework, some of the shortcomings arose as a result of the detailed nature of the Barings fraud. Given this, one option may be to apply the model to instances of computer abuse, which are less complex in nature with regard for example to the commission time, and the number of individuals and companies involved.

A further option would be to take the relevant theoretical concepts and propositions and attempt to develop them with regard to the organisational domain. To some extent this process is evident in the current research in terms of the concept of facilitators. Traditional theoretical accounts describe facilitators in terms of physical entities, such as getaway cars, which act as tools for the perpetration of a crime. The Barings case, however, also provides evidence of how cognitive facilitators i.e. skills and knowledge that a person acquires to perform their work, were also used by Leeson to perpetrate the unauthorised trading. This type of theoretical development would not only reinforce the utility of the model, but would also help to establish criminology as a valuable body of knowledge for the IS security field.

One further area for future research could focus on developing evaluation criteria for the crime specific opportunity structure. Such research would probably examine the potential for a weighting system in which elements of the model are given 'scores' depending on their contribution (or lack thereof) to the control environment. The total score would indicate how effective a certain control environment would be in addressing specific crimes. If a weighting system could be developed, it might be used as a complementary analytical tool in conjunction with traditional risk analysis techniques.

Appendix One

Derivatives

Derivatives are financial products. These products get their name from the fact that their value is derived from other underlying variables that include commodities, e.g., copper, pork bellies, wheat etc., and financial entities such as stocks, and stock indices e.g., the FTSE 100, currencies, etc.

There are two types of derivatives central to the account of the fall of Barings. The first is futures; the second, options. Both are traded on exchanges like SIMEX.

Futures

A futures contract is an agreement between two parties to buy or sell an asset at a certain price at a certain time in the future. One of the parties takes a long position. By doing so, this party is agreeing to buy the underlying asset. The other party takes a short position, and hence agrees to sell the underlying asset at the set price and time in the future. The trading of these contracts are facilitated by the broking companies (e.g., BFS) who trade either for clients (agency trading) or for themselves (proprietary trading) on the various stock exchanges throughout the world. Stock exchanges further facilitate trade by specifying standardised features of futures contracts and providing an infrastructure through which trading can take place. A range of commodities and financial assets underpin the futures contracts traded on these and other exchanges situated around the globe. In terms of the former, these include, for example, wool, copper aluminium, sugar, cattle, and gold; while the latter incorporates stock, stock indices, currencies, treasury bills, bonds, and the like.

To ensure a degree of financial protection for the parties involved in the trading process, those investors who buy or sell futures must deposit a portion of the value of the contracts with their brokers. This portion is known as 'margin' and is designed to reduce the number of contract defaults. A client margin account is therefore maintained by the broking company. When a futures contract is initiated, 'initial margin' is required to be paid by the investor into the margin account. Aside from this initial margin, daily 'variation margin' calls are also required to be paid by investors, depending on what is known as the 'marking to market' position of their contracts.

The depositing of margin does not stop at the investor-broker relationship. This relationship is mirrored between a clearing-house member (a stock broking company such as BFS) and the stock exchange's clearing house (an adjunct to the exchange). Hence, just as a client's margin account is maintained by a broker, so too is a brokers's margin account maintained by the clearing house of the exchange. It should be noted that not all broking companies are clearing house members. If not, then their business must be channelled through a clearing member. Margin is called by an exchange via the clearing-house, to afford some degree of protection if one of its members folds.

The main role of the clearing-house is to keep track of all the trading on the exchange. At the end of each day, the clearing house works out the gains and losses for each member's accounts. Each member may find themselves having to either add or (be in the fortunate position to) remove funds, depending on the price movements of the investments.

Options

It has been almost thirty years since the first options were traded on an exchange. Since then, options markets have grown dramatically, and are now traded on many exchanges throughout the world. Like futures, the assets that underpin their value include, for example, wool, copper, aluminium sugar and gold.

But there are noticeable differences between these two types of derivatives. Moreover, there are two types of options, called 'call' and 'put'. A call option gives the holder the right to buy the underlying asset, at a certain time, for a certain price. A put option gives the holder the right to sell the underlying asset, at a certain time at a certain price. The date specified in the contract is known as the 'exercise'/ 'expiration' date or the date of maturity. The price specified in the contract is known as the 'strike' or 'exercise price'.

Another notable difference between futures and options is the trading obligations that arise as a result of entering into a contract for either of these derivatives. The holder of an option has the right (dependent on whether holding a call or put option) to exercise the option, but is not obligated to do so; hence the name 'options', as holders have the option to exercise or not. This is unlike futures, where holders are obliged to buy or sell the underlying asset.

An example can perhaps best illustrate what influences the decision on whether or not to exercise the option. This further illustrates how profits can be accrued from the trading in options. For ease of explanation, the role of the securities organisations who trade on behalf of clients (e.g., BFS) is omitted, but it is worth pointing out that monies are made by such organisations through client commissions (agency work), or through trading on their own account (proprietary trading). For example: An investor purchases 100 call options (recalling that a call option gives the holder the right to buy) on Microsoft stock with a strike price of $100. Assume that the current stock price is $98, the options expire in two months, and the actual price of the option is $5. If, on the date of maturity, the option price is less than $100, then the holder will not exercise the right to buy, since there is little point in purchasing stock for $100, if the stock value is less than that amount. By declining to purchase the options, the investor loses $500 (i.e., the number of options: 100 multiplied by the cost per option [$5]). However, if the stock price is above $100, then the investor will exercise the option. Suppose the stock price is $115: As a consequence of exercising the option, the investor is able to purchase 100 shares at $100 each. If the investor decides to immediately sell the shares, a gain of $15 would be the result. The sum total of $1500 would therefore equate to $1000 profit given that the cost of the options were $5 each. The above example illustrates the position of someone who purchases call options.

But what about the investor who buys 'put' options? In this instance, the individual is hoping that the share price will decrease. Suppose an investor buys 100 put options on Microsoft stock, with a strike price of $100. Again, assume that the current stock price $98, the date of maturity is in three months' time, and the price per option is $5. At the expiration date, imagine that the share price is $90. The investor can then buy 100 shares for $90 and with regard to the terms of the contract, sell them for $100, producing a gain of $1000 (ignoring transaction costs). When the price of the options is taken into account ($5 each), the total profit made amounts to $500. The down-side to this is if the stock price is over $100 on the expiration date, in which case the options is worthless, and the investor loses $500.

The other major difference is that while futures contracts are 'paid' for at their expiry date, (when call or put options are purchased), the price of the option must be paid in full. This is because options contain a substantial amount of what is known as 'leverage', which refers to the relationship between profit and cost . Given that the options are paid in full, investors are never in a position where they have to pay margin for such trades.

Another point worth mentioning regarding options refers to the price of these financial instruments. The more likely these financial instruments are to be exercised, the more expensive they are. Additionally, the price of options reflects the volatility of a market. When markets are relatively stable and prices of the assets (which underpin options) are changing slowly, it is less likely that the options will be exercised, and hence their price will become cheaper. However, in volatile markets, it is more likely that options will end up 'in the money', i.e., producing financial rewards through their purchase or sale, and will therefore cost more to buy.

One final point involves the intent of trading in these financial instruments. There are essentially three reasons for this. First, there are investors who wish to 'hedge' against foreign currency fluctuations, e.g., an American company who knows that in three months time it will be paying a British supplier £500,000. To guard against unfavourable movements in the sterling exchange-rate markets, the American company may purchase a future or call option. This type of business is known as 'hedging'. Secondly, there are those investors who wish to speculate on the derivatives markets. Their sole intention is to 'take a position' (in the markets) and make profits in this manner. Finally, there are those who make profits through arbitrage trading. This involves spotting price differences of a single product, sold on different exchanges. The arbitrage trader makes a risk-free profit by entering simultaneously into transactions on two or more markets. Consider a stock that is traded both in New York and London: Suppose the stock price is $172 in New York and £100 in London, with an exchange rate of $1.7500 per pound. An arbitrageur can make a profit by purchasing 100 shares in New York and simultaneously selling them in London for $300 (100 x ($1.75 x 100 - $172)).

Glossary of Banking Terms

N.B. All glossary definitions are taken from the BoBS (1995) report.

Arbitrage:

Purchase of a security in one market and the simultaneous sale of the same or an equivalent security in the same or another market for the purpose of profiting from the price differential between the two markets as a result of prevailing conditions in those markets.

Back Office:

Those departments of a financial institution responsible for the trade processing, settlement and other administration.

Broker Dealer:

An intermediary between market and investor which buys and sells securities on behalf of clients and takes proprietary positions in securities.

Clearing House:

An institution which registers, monitors, matches and guarantees trades on a derivatives exchange and which carries out the financial settlement of those transactions.

Clearing Member:

A member of a futures clearing house. Each clearing member must also be a member of the relevant exchange. Clearing members may provide registration and settlement services on behalf of other exchange members who are not themselves clearing members.

Cross Trade:
A transaction whereby a dealer buys and sells the same securities or futures contracts either on behalf of two clients or between clients' accounts and the house account. In most exchanges, the trading rules require that this cross must be offered to the market in order to maintain transparency.

Derivative:
A contract of instrument that changes in value depending on the price movements in another instrument or index, e.g. future, option.

Euroyen:
Yen denominated instrument traded outside the formal control of the Japanese monetary authorities.

Floor Trader:
A trader on the exchange floor who executes the orders of the firm's customers, who are not themselves exchange members.

Hedgers:
A generic term for users of derivatives instruments whose primary purpose is to reduce their risk exposure.

Initial Margin:
The amount of cash and securities to be deposited at a clearing house to establish a futures or options position. Initial margin is established at a level estimated as sufficient to enable a clearing member to meet its obligations should it fail to pay variation margin at the end of the day.

JGB:
Japanese Government Bond.

JGB Future 10 Years:
A futures contract traded on SIMEX, TSE and LIFFE based on JGB.

Margin:

Cash or securities deposited with an exchange both as a form of collateral and a way of setting realised and unrealised profit and loss on positions. Margin also attempts to ensure that clearing members have sufficient resources to support open positions.

Margin Call:

A demand from an exchange, or from a broker or dealer carrying a customer's position, for additional cash or collateral in respect of a position.

Mark-to-Market:

The valuation of a securities portfolio to current market prices.

Nikkei 225:

An index based on 225 Japanese stocks traded on the Tokyo Stock Exchange. The most widely followed index in Japan and the basis for the major Japanese equity derivatives contracts.

Nikkei 225 future:

A futures contract based on a multiple of times the Nikkei Stock Index traded on OSE and SIMEX. The contract specification is different between the two exchanges.

Nikkei 225 option:

An option contract based on the Nikkei 225 future traded on OSE and SIMEX.

Open Outcry:

A trading method where trading places in a designated physical area of the exchange within an agreed time period. Prices are agreed by traders on the floor of the exchange, after which both traders complete a deal ticket to record transactions. These tickets are matched by exchange officials, after which the deal is recorded.

OSE:

Osaka Securities Exchange, a derivatives exchange offering contracts on the Nikkei Stock Indices.

Over-the-Counter (OTC):

A security or other instrument that is not traded on an organised exchnage. OTC instruments can be created with any provisions allowed by law and acceptable to counterparties.

Position:

A holding of an instrument.

Proprietary Trading:

Generally used to describe risk positions for an institution's own account as principal and distinct from client business.

Speculators:

Generic term for traders whose primary purpose is to achieve profits from anticipated price movements.

Switching (See also Arbitrage).

In the case of Barings, this activity typically involved the simultaneous purchase and sale of the same futures contract on the different futures exchnages.

Three Month Euroyen Contract:

A futures contract traded on SIMEX and TIFFE based on three month interest rate for Euroyen.

Bibliography

Adams, A. and Sasse, M. (1999) Users Are Not The Enemy. *Communications of the ACM* 42 (12): 41-46.

Adler, P. and Adler, P. (1988) Intense Loyalty in Organizations: A Case Study of College Athlectics. *Administrative Science Quarterly* 33: 401-417.

Anderson, R. (1994) Why Cryptosystems Fail. *Communications of the ACM* 37 (11): 32-40.

Audit Commission. (1994) *Opportunity Makes a Thief: An Analysis of Computer Abuse*. London. Audit Commission Publications.

Audit Commission. (1997) *Ghost in the Machine: An Analysis of IT Fraud and Abuse*. London. Audit Commission Publications.

Audit Commission. (2001) *Your Business@Risk: An Update on IT Abuse 2001.* London. Audit Commission Publications.

Avison, D. and Myers, M. (1995) Information Systems and Anthropology: An Anthropological Perspective on IT and Organisational Culture. *Information Technology and People* 8 (3): 43-56.

Backhouse, J. (1997) Information at Risk. *Information Strategy*. January: 33-35.

Backhouse, J., Liebenau, J. and Land, F. (1991) On the Discipline of Information Systems. *Journal of Information Systems*. 1: 19-27.

Bandura, A. (1976) Social Learning Analysis of Aggression. In E. Ribes-Inesta and A. Bandura (eds.), *Analysis of Delinquency and Aggression*. Hillsdale, NJ. Lawrence Erlbaum Associates, Publishers.

Banville, C. and Landry, M. (1989) Can the Field of MIS be Disciplined? *Communications of the ACM* 32 (1): 48-60.

Barber, R. (2000) Implementing Public Key Infrastructures in a Dynamic Business Environment. *Computers and Security* 19 (3): 230-233.

Barber, R. (2001) The Evolution of Intrusion Detection Systems - The Next Step. *Computers and Security* 20 (2): 132-145.

Bateson, G. (1978) *Steps to an Ecology of Mind*. New York. Ballantine Books.

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

Bennett, T. and Wright, R. (1984) *Burglars and Burglary*. Farnborough. Gower.

BloomBecker, J. (1984) Introduction to Computer Crime. In J. Finch and E. Dougall (eds.), *Computer Security: A Global Challenge*. North-Holland. Elsevier Science Publishers.

Blumer, H. (1954) What is Wrong With Social Theory? *American Sociological Review* 19: 3-10.

Board of Banking Supervision (1995) *Report of the Board of Banking Supervision Inquiry into the Circumstances of the Collapse of Barings*. London. HMSO.

Bogdan, R and Biklen, S. (1992) *Qualitative Research for Education: An Introduction to Theory and Methods*. Boston. Allyn & Bacon.

Boland, R. (1991) Information System Use as a Hermeneutic Process. In H.-E. Nissen, H.Klien and R. Hirscheim (eds.) *Information Systems Research: Contemporary Approaches and Emergent Traditions.* North-Holland. Elsevier Science Publishers.

Bologna, J. (1993) *Handbook on Corporate Fraud.* Boston. Butterworth-Heinemann.

Brantingham, P. and Brantingham, P. (1975) The Spatial Patterning of Burglary. *Howard Journal of Criminal Justice* 14: 11-23.

Brantingham, P. and Brantingham, P. (1991) Environmental Criminology. (2nd ed.). Prospect Heights, IL. Waveland Press.

BS7799. (1999) *Code of Practice for Information Security Management.* British Standards Institute.

Burrell, G. and Morgan, G. (1979) *Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life.* London. Heinemann.

Burt, C. (1925) *The Young Delinquent.* London. University of London Press (reprinted 1969).

Carroll, J. and Weaver, F. (1986) Shoplifter's Perceptions of Crime Opportunities: A Process-Tracing Study. In D. Cornish and R. Clarke (eds.), *The Reasoning Criminal.* New York. Springer-Verlag.

CBI/Ernst and Young. (2000) *Fraud: Risk and Prevention.* London. Caspian Publishing Limited.

Ceruzzi, P. (1999) *A History of Modern Computing.* Cambridge, MS. MIT Press.

Chapman, S. (1984) *The Rise of Merchant Banking.* London. George Allen and Unwin.

Ciechanowicz, Z. (1997) Risk Analysis: Requirements, Conflicts and Problems. Computers & Security 16 (3): 223-232.

Clarke, R. (1980) Situational Crime Prevention : Theory and Practice. *British Journal of Criminology* 20: 136-137.

Clarke, R. (ed.) (1992) *Situational Crime Prevention : Successful Case Studies.* Albany, NY. Harrow and Heston..

Clarke, R. (1995) Situational Crime Prevention. In M. Tonry and D. Farrington (eds.), *Building a Safer Society. Strategic Approaches to Crime Prevention. Crime and Justice: A Review of Research.* Vol. 19. Chicago. University of Chicago Press.

Clarke, R. (ed.) (1997) *Situational Crime Prevention : Successful Case Studies.* 2nd ed. Albany, NY. Harrow and Heston.

Clarke, R. and Cornish, D. (1985) Modelling Offender's Decisions : A Framework for Policy and Research. In M. Tonry and N. Morris (eds.), *Crime and Justice : An Annual Review of Research.* Vol. 6. Chicago. University of Chicago Press.

Clarke, R. and Cornish, D. (2000) Rational Choice. In R. Paternoster and R. Bachman (eds.), *Explaining Crime and Criminals: Essays in Contemporary Criminological Theory.* Los Angeles, CA. Roxbury Publishing Company.

Clarke, R. and Felson, M. (eds.) (1993) *Routine Activity and Rational Choice. Advances in Criminological Theory.* Vol. 5. New Brunswick, NJ. Transaction Publishers.

Clarke, R. and Martin, D. (1971) *Absconding from Approved Schools.* Home Office Research Study. No.12. London. H.M.S.O.

Cohen, A. (1955) *Delinquent Boys.* Glencoe, ILL. The Free Press.

Cohen, L. and Felson, M. (1979) Social Change and Crime Rate Trends : A Routine Activity Approach. *American Sociological Review* 44: 588-608.

Comer, M. (1998) *Corporate Fraud* (3rd ed.). Vermont. Gower.

Computer Fraud & Security, July 2001, *Firms Fear Current and Past Employees.*

Cornish, D. and Clarke, R. (1986) Situational Prevention, Displacement of Crime and Rational Choice Theory. In K. Heal, and G. Laycock (eds.), *Situational Crime Prevention: From Theory into Practice*. London. H.M.S.O.

Corsaro, W. (1981) Entering the Child's World – Research Strategies for Field Entry and Data Collection in a Pre-School Setting. In J. Green and C. Wallat (eds.), *Ethnography and Language in Educational Settings*. Norwood, NJ. Ablex.

Creswell, J. (1998) *Qualitative Inquiry and Research Design: Choosing Among Five Traditions*. London. SAGE Publications.

CSI/FBI (2002) *Computer Security Issues and Trends*. San Francisco. CSI.

Cusson, M. (1986) L'analyse Strategique et Quelques Developpements Recente en Criminologie. *Criminologie* 19: 51-72.

Dale, R. (1992) *International Banking Deregulation: the Great Banking Experiment.* Oxford. Blackwell.

Davies, D. (1996) Personal Computers - More Power; More risks. *The Computer Law and Security Report* 12 (2): 110-111.

Davies, R. and Atkinson, P. (1991) Students of Midwifery: 'Doing the Obs' and Other Coping Strategies. *Midwifery* 7: 113-21.

Davis, L. (1991) Researching the Organisational Culture Contexts of Information Systems. In Nissen, H., Klein, H and Hirscheim, R. (eds.) *Information Systems Research in the 1990s*. Amsterdam. Elsevier.

Davis, L and Nielsen, S. (1992) An Ethnographic Study of Configuration Management and Documentation Practices in an Information Technology Center. In K. Kendall, K. Lyytinen and J. DeGross (eds.), *The Impact of Computer Supported Technology on Information Systems Development*. Amsterdam. North Holland.

Dening, G. (1980) *Islands and Beaches: Discourse on a Silent Land – Marquesas, 1774-1880*. Chicago. Dorsey Press.

Dexter, L. (1970) *Elite and Specialized Interviewing*. Evanston, Ill. Northwestern University Press.

Dhillon G. (1997) *Managing Information Systems Security*. London. Macmillan.

Dhillon, G. and Backhouse, J. (1996) Risks in the use of Information Technology Within Organisations. *International Journal of Information Management* 16 (1): 65-74.

Dhillon, G. and Backhouse, J. (2001) Current Directions in IS Security Research: Toward Socio-Organisational Perspectives. *Information Systems Journal* 11 (2): 127-153.

Diener, E. (1980) Deindividuation: The Absence of Self-Awareness and Self-Regulation in Group Members. In P. Paulus (ed.), *The Psychology of Group Influence*. Hillsdale, NJ. Lawrence Erlbaum.

Dorey, P. (1994) Security Management and Policy. In W. Caelli, D. Longley and M. Shain, (eds.), *Information Security Handbook*. Macmillan Press Ltd. London.

DTI (2000) *Information Security Breaches Survey*. London. DTI.

Dufala, D. (1976) Convenience Stores: Armed Robbery and Physical Environmental Features. *American Behavioral Scientist* 20: 227-246.

Ekblom, P. (1994) Proximal Circumstances: A Mechanism-Based Classification of Crime Prevention. In R. Clarke (ed.), *Crime Prevention Studies.* Vol. 2. Monsey, NY. Criminal Justice Press.

Ernst and Young. (2002) *Global Information Security Survey.* Presentation Services. London.

Essinger, J. (1990) Computer Security in Financial Organizations. Oxford. Elsevier Science Publishers Ltd.

Farrell, G. (1992) Multiple Victimisation: Its Extent and Significance. *International Review of Victimology* 2 (2): 85-102.

Farrell, G. (1994) Predicting and Preventing Revictimisation. In M. Tonry and D. Farrington (eds.), *Preventing Crime, Crime and Justice.* Vol. 19. University of Chicago Press. Chicago.

Farrell, G., Phillips, C. and Pease, K. (1995) Like Taking Candy: Why Does Repeat Victimisation Occur? *British Journal of Criminology* 35 (3): 384-399.

Fay, S. (1996) *The Collapse of Barings.* London. Richard Cohen Books.

Felson, M. (1986) Linking Criminal Choices, Routine Activities, Informal Control, and Criminal Outcomes. In D. Cornish and R. Cornish (eds.), *The Reasoning Criminal : Rational Choice Perspectives on Offending.* New York. Springer-Verlag.

Felson, M. (1992) Routine Activities and Crime Prevention: Armchair Concepts and Practical Action. *Studies on Crime and Crime Prevention.* 1: 31-34.

Felson, M. (1994) *Crime and Everyday Life: Insight and Implications for Society.* Thousand Oaks, CA. Pine Forge Press.

Felson, M. (2000) The Routine Activity Approach. In R. Paternoster and R. Bachman (eds.), *Explaining Crime and Criminals: Essays in Contemporary Criminological Theory*. Los Angeles, CA. Roxbury Publishing Company.

Felson, M. and Clarke, R. (1995) Routine Precautions, Criminology, and Crime Prevention. In D.Barlow (ed.), *Crime and Public Policy*. Boulder, CO. Westview Press.

Fetterman, D. (1998) *Ethnography: Step by Step*. London. SAGE Publications.

Financial Times, 15 June 1995, *Investment banks vow to reduce bonus-led risks.*

Financial Times, 3 March 1997, *Bonus Fever.*

Forester, T. and Morrison, P. (1994) *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. MIT Press. Cambridge, MA.

Frake, C. (1964) A Structural Description of Subanun 'Religious Behaviour'. In W. Goodenough (ed.), *Explorations in Cultural Anthropology*. New York. McGraw-Hill.

Frake, C. (1983) Ethnography. In R. Emerson (ed.), *Contemporary Field Research*. Boston. Little Brown.

Gabor, T. (1996) *Everybody Does It! Crime by the Public*. New York. Macmillan.

Galliers, R. (1991) Choosing Appropriate Information Systems Research Methodologies: A Revised Taxonomy. In H-E. Nissen, H. Klein, and R. Hirscheim (eds.), *Information Systems Research: Contemporary Approaches and Emergent Traditions*. Amsterdam: North Holland.

Galliers, R. and Land, F. (1987) Choosing Appropriate Information Systems Research Methodologies. *Communications of the ACM* 30 (11): 900-902.

Gamst, F. (1980) *The Hoghead: An Industrial Ethnology of the Locomotive Engineer.* New York. Holt, Rinehart & Winston.

Geertz, C. (1973) Thick Description: Toward an Interpretive Theory of Culture. In C. Geertz (ed.), *The Interpretation of Cultures.* New York. Basic Books.

Gladstone, F. (1978) Vandalism Amongst Adolescent Schoolboys. In R. Clarke (ed.), *Tackling Vandalism.* Home Office Research Study. No 47. London. HMSO.

Gold, R. (1958) Roles in Sociological Fieldwork. *Social Forces* 36: 217-23.

Golden-Biddle, K. and Locke, K. (1993) Appealing Work: An Investigation of How Ethnographic Texts Convince. *Organization Science* 4 (4): 595-616.

Goodenough, W. (1976) Muliculturalism as the Normal Human Experience. *Anthropology and Education Quarterly* 7 (4): 4-7.

Gottfredson, M.R. and Hirschi, T. (1990) *A General Theory of Crime.* Stanford, CA. Stanford University Press.

Guardian, 27 September 1995, *Controls Tightened After Daiwa Loss.*

Guardian, 22 August 1996, *Four Expelled From City as SFA Cracks the Whip.*

Guardian, 1 March 1997, *Fresh City Scandal as NatWest Loses Pounds 50m.*

Gulliver, P. (1958) *Land Tenure and Social Change Among the Nyakusa.* Kampala. East African Institute of Social Research.

Hammersley, M. and Atkinson, P. (1995) *Ethnography Principles and Practice (2nd ed.).* London. Routledge.

Harris, A. and Yen, D. (2002) Biometric Authentication: Assuring Access to Information. *Information Management & Computer Security* 10 (1): 12-19.

Hartshorne, M. and May, M. (1928) *Studies in the Nature of Character (vol.1): Studies in Deceit.* New York. Macmillan.

Harvey, L. and Myers, M. (1995) Scholarship and Practice: the Contribution of Ethnographic Research Methods to Bridging the Gap. *Information Technology and People* 8 (3): 13-27.

Hawley, A. (1950) *Human Ecology: A Theory of Community Structure.* New York. Ronald.

Hechter, M. and Kanazawa, S. (1997) Sociological Rational Choice Theory. *Annual Review of Sociology* 23: 191-214.

Heffernan, S. (1996) *Modern Banking in Theory and Practice.* Chichester. Wiley.

Hinde, S. (2001) The Weakest Link. *Computers & Security* 20 (4): 295-301.

Hindelang, M., Gottfredson, M. and Garofalo, J. (1978) *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimisation.* Cambridge, MA. Ballinger.

Hirscheim, R. and Klein, H. (1989) Four Paradigms of Information Systems Development. *Communications of the ACM* 32 (10): 1199-1216.

Hirscheim, R. and Newman, M. (1991) Symbolism and information systems development: myth, metaphor and magic. *Information Systems Research* 2 (1): 29-62.

Hirschi, T. (1969) *Causes of Delinquency.* Berkeley and Los Angeles. University of California Press.

Hitchings, J. (1995) Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology. *Computers & Security* 14 (5): 377-383.

Homan, R. (1980) The Ethics of Covert Methods. *British Journal of Sociology* 31 (1): 46-59.

Hughes, J., Randall, D. and Shapiro, D. (1992) Faltering from Ethnography to Design. *Proceedings of the Conference on Computer-Supported Co-operative Work: Sharing Perspectives (CSCW 92).* New York, NY. ACM Press.

Hull, J. (1997) *Options, Futures and Other Derivatives.* 3rd ed. New Dehli. Prentice-Hall India.

Hunt, L. and Heinrich, K. (1996) *Barings lost: Nick Leeson and the Collapse of Barings plc.* St. Leonards, NSW. Allen and Unwin.

Independent, 27 February 1995, *An accident waiting to happen?: A single deal may have ruined Barings bank.*

Introna, L. (1997) *Management, Information and Power: A Narrative for the Involved Manager.* London. Macmillan Press Ltd.

Junker, B. (1960) *Field Work.* Chicago. University of Chicago.

Karp, D. (1980) Observing Behavior in Public Places: Problems and Strategies. In Shaffir, W., Stebbins, R. and Turowetz, A. (eds.), *Experiencing Fieldwork: An Inside View of Qualitiative Approaches to Social Research.* Newbury Park, CA. Sage.

Kennedy, D. (1990) Facility Site Selection and Analysis Through Environmental Criminology. *Journal of Criminal Justice* 18: 239-252.

KPMG. (2000) *Information Security Survey.* KPMG. London.

Kube, E. (1988) Preventing Bank Robbery: Lessons from Interviewing Robbers. *Journal of Security Administration* 11: 78-83.

Land, F. (1992) The Information Systems Domain. In R. Galliers (ed.) *Information Systems Research. Issues Methods and Practical Guidelines.* London. Blackwell Scientific.

Laslett, P. (1965) *The World We Have Lost.* London. Methuen.

Lee, A. (1991) Integrating Positivist and Interpretive Approaches to Organizational Research. *Organization Science* 2: 342-365.

Lee, A. (1994) The Hermeneutic Circle as a Source of Emergent Richness in the Managerial Use of Electronic Mail. In J. DeGross, J.Huff and Munro, M (eds.) *The Proceedings of the Fifth International Conference on Information Systems.* Vancouver.

Lee, A. (1994a) Electronic Mail as a Medium for Rich Communication: An Empirical Investigation Using Hermeneutic Interpretation. *MIS Quarterly.* June.

Lee, A., Baskerville, R. and Davies, L. (1992) A Workshop on Two Techniques for Qualitative Data Analysis: Action Research and Ethnography. In J. DeGross, J. Becker and J. Elam (eds.), *Proceedings of the Thirteenth International Conference on Information Systems,* December 13-16, Dallas, Texas.

Lee, A., Liebenau, J. and DeGross, J. (eds.) (1997) *Information Systems and Qualitative Research.* London. Chapman and Hall.

Leeson, N. and Whitley, E. (1996) *Rogue Trader.* London. Little Brown.

Lichtenstein, S. (1996) Factors in the Selection of a Risk Assessment Method. *Computers & Security* 4 (4): 20-25.

Light, R., Nee, C. and Ingham, H. (1993) *Car Theft: The Offender's Perspective.* Home Office Research Study. No.130. London. H.M.S.O.

Lindup, K. (1996) The Role of Information Security in Governance. *Computers & Security* 15 (6): 477-485.

Lofland, J. and Lejeune, R. (1960) Initial Encounters of Newcomers in Alcoholics Anonymous. *Social Problems* 8: 102-11.

Luzwick, P. (2001) Security? Who's Got Time For Security? I'm Trying to Get my Job Done. *Computer Fraud & Security*. January 2001.

Maguire, M. (1980) Burglary as Opportunity. *Research Bulletin* No 10. Home Office Research Unit. London. Home Office.

Maguire, M. (1982) *Burglary in a Dwelling*. London. Heinemann.

Malinowski, B. (1922) *Argonauts of the Western Pacific*. London. Routledge & Kegan Paul.

Markus, L. and Lee, A. (1999) Special Issue on Intensive Research in Information Systems: Using Qualitative, Interpretive, and Case Methods to Study Information Technology. *MIS Quarterly* 23 (1): 35-38.

Matza, D. (1964) *Delinquency and Drift*. New York. Wiley.

Mayhew, P., Clarke, R., Sturman, A. and Hough, J. (1976) Crime as Opportunity. Home Office Research Study. No.34. London. H.M.S.O.

McCullough, D., Schmidt, T. and Lockhart, B. (1990) *Car Theft in Northern Ireland*. Cirac Paper No.2. Belfast, U.K. The EXTERN Organisation

Mischel, W. (1968) *Personality and Assessment*. New York. Wiley.

Myers, M. (1997) *Crtical Ethnography in Information Systems*. In A.Lee, J. Liebenau and J. DeGross (eds.), *Information Systems and Qualitative Research*. London. Chapman and Hall.

Nash, J. (1979) *We Eat the Mines and the Mines Eat Us.* New York. Columbia University Press.

Newman, M. and Robey, D. (1992) A social process model of user-analyst relationships. *MIS Quarterly* 16: 249-266.

Normandeau, A. and Gabor, T. (1987) *Armed Robbery: Cops, Robbers and Victims.* Springfield, IL. Charles C. Thomas.

Nosworthy, J. (2000) Implementing Information Security in the 21st Century – Do You Have the Balancing Factors? *Computers & Security* 19 (4): 337-347.

Nugent, S., Burnes, D., Wilson, P. and Chapell, D. (1989) *Risks and Rewards in Robbery: Prevention and the Offender's Perspective.* Melbourne. The Australian Bankers' Association.

Olnes, J. (1994) Development of Security Policies. *Computers & Security* 14 (8): 628-636.

Opp, K.-D. (1997) Limited Rationality and Crime. In G.Newman, R.Clarke and S.Shoham (eds.), *Rational Choice and Situational Crime Prevention: Theoretical Foundations.* Aldershot. Dartmouth Publishing Company.

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

Orun, A., Feagin, J. and Sjoberg, G. (1991) Introduction : The Nature of the Case Study. In J. Feagin, A. Orun and G. Sjoberg (eds.), *A Case for the Case Study.* Chapel Hill. The University of North Carolina Press.

Osborne, K. (1998) Auditing the IT Security Function. *Computers & Security* 17 (1): 34-41.

Parker, D. (1976) *Crime by Computer*. Charles Scribner & Sons. New York.

Parker, D. (1997) The Strategic Values of Information Security in Business. *Computers & Security* 16 (7): 572-582.

Pease, K. (1993) Individual and Community Influences on Victimisation and their Implications for Crime Prevention. In D. Farrington., R. Sampson and P-O. Wikstrom (eds.), *Integrating Individual and Ecological Aspects of Crime*. Stockholm. National Council for Crime Prevention.

Pease, K. (1994) Crime Prevention. In M. Maguire, R. Morgan and R. Reiner (eds.), *The Oxford Handbook of Criminology*. Oxford. Clarendon Press.

Peyravian, M. and Nevenko, Z. (2000) Methods for Protecting Password Transmission. *Computers and Security* 19 (5): 466-469.

Pettigrew, A. (1985) Contextualist Research and the Study of Organizational Change Processes. In E. Mumford, R. Hirscheim, G. Fitzgerald and A. Wood-Harper (eds.), *Research Methods in Information Systems*. Amsterdam. North-Holland.

Poyner, B. and Webb, B. (1991) *Crime Free Housing*. Oxford. Butterworth Architect.

Prasad, P. (1997) Systems of Meaning: Ethnography as a Methodology for the Study of Information Technologies. In A.Lee, J. Liebenau and J. DeGross (eds.), *Information Systems and Qualitative Research*. London. Chapman and Hall.

Prentice-Dunn, S. and Rogers, R. (1989) Deindividuation and the Self-Regulation of Behavior. In P.B. Paulus (ed.) *Psychology of Group Influence* (2nd ed.). Hillsdale, NJ. Lawerence Earlbaum.

Reppetto, T.A. (1974) *Residential Crime*. Cambridge, M.A. Ballinger.

Ricoeur, P. (1976) *Interpretation Theory: Discourse and the Surplus of Meaning.* Fort Worth, TX. The Texas Christian University Press.

Ricoeur, P. (1981) *Hermeneutics and the Human Sciences.* Cambridge. Cambridge University Press.

Riem, A. (2001) Cybercrimes of the 21st Century. *Computer Fraud & Security.* April 2001.

Rosenhahn, D. (1973) On Being Sane in Insane Places. *Science* 179: 250-258.

Scarr, H.A. (1973) *Patterns of Burglary.* 2nd ed. Washington, D.C. U.S. Department of Justice, National Institute of Law Enforcement and Criminal Justice.

Schneier, B. (1998) Security Pitfalls in Cryptographic Design. *Information Management & Computer Security* 6 (3): 133-137.

Schryer, F. (1980) *The Rancheros of Pisaflores: The History of a Peasant Bourgeoisie in Twentieth Century Mexico.* Toronto. University of Toronto.

Scott, S. (2000) A Situated Discussion of 'Truth and Method' in Interpretive Information Systems Research. *LSE Working Paper Series.* No. 91.

Short, J., Jr. and Strodtbeck, F. (1965) *Group Processes and Gang Delinquency.* Chicago. University of Chicago Press.

Silverman, M. (1980) *Rich People and Rice: Factional Politics in Rural Guyana, 1902-1970.* Leiden. E.J. Brill.

Silverman, M. and Gulliver, P. (eds.) (1992) *Approaching the Past: Historical Anthropology Through Irish Case Studies.* New York. Columbia University Press.

Sinclair, I. (1971) *Hostels for Probationers.* Home Office Research Study. No.6. London. H.M.S.O.

Sinclair, I. (1975) The Influence of Wardens and Matrons on Probation Hostels : A Study of a Quasi-Family Institution. In J.Tizard, I. Sinclair, and R,Clarke, (eds.), *Varieties of Residential Experience.* London. Routledge and Kegan Paul

Smith, C. (1989) The Case Study: A Vital Yet Misunderstood Research Method for Management. In R. Mansfield (ed.), *Frontiers of Management.* London. Routledge.

Smith, D. (1995) Youth Crime and Conduct Disorders: Trends, Patterns, and Causal Explanations. In M. Rutter and D. Smith (eds.), *Psychological Disorders in Youth Populations. Time Trends and Their Causes.* Chichester. John Wiley and Sons.

Southall, A. (1962) *Social Change in Modern Africa.* London. Oxford University Press.

Spencer, E. (1992) *Car Crime and Young People on a Sunderland Housing Estate.* Crime Prevention Unit Paper 40. Home Office. London.

Spurling, P. (1995) Promoting Security Awareness and Commitment. *Information Management & Computer Security* 3 (2): 20-26.

Star, S. and Ruhleder, K. (1996) Steps Towards an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information Systems Research* 7 (1): 111-134.

Stevenson, G. (2000) Computer Fraud: Detection and Prevention. *Computer Fraud & Security.* November 2000.

Stoller, L-A. (1985) *Capitalism and Confrontation in Sumatra's Plantation Belt, 1870-1979.* New Haven. Yale University Press.

Sturman, A. (1976) *Crime As Opportunity.* Home Office Research Study. No. 34. London. H.M.S.O.

Suchman, L. (1987) *Plans and Situated Actions: The Problems of Human-Machine Communication*. Cambridge. Cambridge University Press.

Sullivan, M., Queen, S. and Patrick, R. (1958) Participant Observation as Employed in the Study of a Military Training Program. *American Sociological Review* 23 (6): 660-667.

Sykes, G. and Matza, D. (1957) Techniques of Neutralisation: A Theory of Delinquency. *American Sociological Review* 22: 664-670.

Taylor, P. (1999) *Hackers: Crime and the Digital Sublime*. New York. Routledge.

Tedeschi, J. and Felson, R. (1994) *Violence, Aggression and Coercive Actions*. Washington, DC. American Psychological Association.

Thomas, D. (2002) *Hacker Culture*. Minneapolis. University of Minnesota Press.

Thomas, W. and Znaniecki, F. (1927) *The Polish Peasant in Europe and America*. New York. Knopf.

Thomson, M. and von Solms, R. (1998) Information Security Awareness: Educating Your Users Effectively. *Information Management & Computer Security* 6 (4): 167-173.

Tinker, T. (1998) Hamlet Without the Prince: The Ethnographic Turn in Information Systems Research. *Accounting Auditing & Accountability Journal* 11 (1): 13-33.

Tonks, I. and Webb, D. (1989) *The Reorganisation of the London Stock Market : The Causes and Consequences of 'Big-Bang'*. London. LSE Financial Markets Group.

Trasler, G. (1986) Situational Crime Control and Rational Choice: A Critique. In K. Heal, and G. Laycock (eds.), *Situational Crime Prevention: From Theory into Practice*. London. H.M.S.O.

U.S. National Commission on the Causes and Prevention of Violence. (1969) *Crimes of Violence*. Washington. U.S. Government Printing Office.

Vincent, T. (1982) *Teso in Transformation: The Political Economy of Peasant and Class in Eastern Africa*. Berkeley. University of California Press.

Vincent, T. (1984) Marriage, Religion, and Class in South Fermanagh, Ireland, 1840-1920. In O. Lynch (ed.), *Culture and Community in Europe: Essays in Honour of Conrad M. Arsenberg*. Delhi. Hindustan Publishing.

Von Solms, B. (2001) Corporate Governance and Information Security. *Computers & Security* 20 (3): 215-218.

Wagner, I. (1993) A Web of Fuzzy Problems: Confronting the Ethical Issues. *Communicaitons of the ACM* 36 (4): 94-101.

Waller, I. and Okihiro, N. (1979) *Burglary: The Victim and the Public.* Toronto. University of Toronto Press.

Walsh, D. (1980) *Break-Ins: Burglary from Private Houses*. London. Constable

Walsham, G. (1993) *Interpreting Information Systems in Organisations*. Chichester. John Wiley & Sons.

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

Walsham, G. (1995b) The Emergence of Interpretivism in IS Research. *Information Systems Research* 6 (4): 376-394.

Warman, A. (1993) *Computer Security Within Organisations*. London. Macmillan.

Weibschuh, T. (2000) IT Security – An Historical Perspective. *Computer Fraud & Security*. September 2000.

Weick, K. (1983) Contradictions in a Community of Scholars: The Cohesion-Accuracy Trade-off. *The Review of Higher Education* 4: 253-267.

Wolcott, H. (1987) On Ethnographic Intent. In G. Spindler and L.Spindler (eds.), *Interpretive Ethnography of Education.* London. Lawrence Erlbaum Associates, Publishers.

Wolcott, H. (1995) Making a Study More Ethnographic. In J. Van Maanen (ed.), *Representation in Ethnography.* Thousand Oaks, CA. Sage Publications.

Wood, C. (1995) Writing InfoSec Policies. *Computers & Security* 14 (8): 667-674.

Wood, C. (1997) Policies Alone Do Not Constitute a Sufficient Awareness Effort. *Computer Fraud and Security.* December 1997.

Woods, P. (1981) Understanding Through Talk. In C. Adelman (ed.), *Uttering, Muttering: Collecting, Using and Reporting Talk for Social and Educational Research.* London. Grant McIntyre.

Wolfgang, M. and Ferracuti, F. (1967) *The Subculture of Violence: Toward an Integrated Theory in Criminology.* London. Tavistock Pulbications.

Wilkins, L. (1990) Retrospect and Prospect: Fashions in Criminal Justice Theory and Practice. In D. Gottfredson and R. Clarke (eds.), *Policy and Theory in Criminal Justice.* Aldershot. Avebury.

Willison, R. (2000a) Understanding and Addressing Criminal Opportunity: The Application of Situational Crime Prevention to IS Security. *Journal of Financial Crime* 7 (3): 201-10.

Willison, R. (2000b) Reducing Computer Fraud Through Situational Crime Prevention. In S. Qing and J. H.P. Eloff (eds.), *Information Security for Global Information Infrastructures.* Boston. Kluwer Academic Press.

Willison, R. (2001) The Unaddressed Problem of Criminal Motivation in IS Security: Expanding the Preventive Scope Through the Concept of Readying. *LSE Working Paper Series.* No. 101.

Wilson, J. Q. (1975) *Thinking About Crime.* New York. Basic Books.

Witte, A., Tauchen, H. and Long, S. (1984) *Violence in the Family: A Non-Random Affair.* Working Paper No. 89. Department of Economics, Wellesley College.

Wortley, R. (1997) Reconsidering the Role of Opportunity in Situational Crime Prevention. In G. Newman, R. Clarke and S. Shohan (eds.), *Rational Choice and Situational Crime Prevention.* Aldershot. Ashgate Publishing.

Wright, M. (2001) Keeping Top Management Focussed. *Computer Fraud & Security.* May 2001.

Wynn, E. (1979) Office Conversation as an Information Medium. Unpublished Ph.D. Dissertation. University of California, Berkley.

Wynn, E. (1991) Taking Practice Seriously. In J. Greenbaum and M. Kyng (eds.), *Design at Work.* Hillsdale, NJ. Lawrence Erlbaum.

Yablonsky, L. (1962) *The Violent Gang.* New York. Macmillan.

Yapp, P. (2001) Passwords: Use and Abuse. *Computer Fraud & Security.* September 2001.

Yin, R. (1989) *Case Study Research: Design and Methods.* Newbury Park, CA. Sage Publications.

Zenkin, D. (2001) Fighting Against the Invisible Enemy: Methods for Detecting an Unknown Virus. *Computers and Security* 20 (4): 316-321.

Ziegler, P. (1988) *The Sixth Great Power: Barings 1762-1929.* London. Collins.

Zimbardo, P. (1970) The Human Choice: Indivuation, Reason, and Order, vs Deindividuation, Impulse, and Chaos. In W.J. Arnold and D. Levine (eds.) *Nebraska Symposium on Motivation 1969*. Lincoln, NE. University of Nebraska Press.

Zuboff, S. (1988) *In the Age of the Smart Machine*. New York. Basic Books.