# *Bank clerks, computers and crime :*

An assessment of the different types of risk that banks face with regard to computers and crime.

Simon Cunliffe Rogerson

Submitted for the Degree of Doctor of Philosophy

Canterbury Business School
University of Kent at Canterbury
1997

# *Abstract*

**Author:** Simon Cunliffe ROGERSON

**Short Title:** Banks clerks, computers and crime

**Full Title:** An assessment of the different types of risk that banks face with regard to computers and crime.

**Keywords:** Banks, Banking, Change, Clerks, Clerical, Computers, Crime, Management, Strategy

The purpose of this thesis is to examine the changes that have occurred in the banking industry during the period at the end of the 1980s and the beginning of the 1990s to assess the impact that they had on the attitudes and opinions of bank clerks. The main concern of the research was the banks'employees'attitudes to crimes such as computer crime.

To achieve this, two major pieces of research were conducted by the author - one in the banking industry, and another conducted via Internet to reach a cross section of computer users. The results of these surveys were used to evaluate the risks that the banking industry currently faces both from external and internal forces.

These two pieces of work may be analysed to assess the potential for computer crime in the banking industry. The bank employee survey aims to develop a motivation model which draws on the work of Fishbein. This model maps the possible factors involved in the attitude of employees to crime and unacceptable behaviour in the banking industry. The computer survey gathers information regarding computer users'opinions towards the act of cracking and other acts of computer misuse. The banking survey develops a profile of the average bank employee whilst the computer user survey develops a profile of a cracker. These two profiles tend to indicate that the risk of more sophisticated computer crimes being committed by bank employees against their employers is slim.

During the evaluation of the risks that the banks face, consideration has been given to the phenomenon of white collar crime and the associated topic of fraud - both of which represent a threat to the financial world.

# contents

# Preface

*"Trust men and they will be true to you; treat them greatly and they will show themselves great." Emerson "Prudence" Essays (1841).*

*"In this business you can't sleep for trying to figure out all the tricks they could pull on you, you're like the guy behind the roulette wheel watching the customers to make sure they don't crook the house.*

*"Then one night you get to thinking how you could crook the house yourself, and do it smart, because you've got the wheel right under your hand; you know every notch in it by heart." Walter Neff in the film "Double Indemnity" (Chandler and Wilder, 1944).*

The ideas behind this thesis first arose when I left Barclays Bank in 1990. I had joined the bank in 1985 straight from school and had anticipated a long career with them ending in retirement with a healthy pension. I was not alone in my ambitions. It was possible with diligence and hard work to have very realistic ambitions of branch management if you were willing to wait.

A bank job did not pay well but it was secure and offered good fringe benefits. When I joined I was given a day a week study leave and was entitled to take time off for sport, Territorial Army commitments, local government duties and was encouraged to undertake positions of authority in clubs and associations. The remuneration was complemented by preferential rate loans and mortgages. During my time with the bank nearly all such entitlements were withdrawn.

As this was happening the bank's branch network was rationalised leading to fewer but larger branches. Within these branches there was also a reduction in the number of middle management grades - a process well documented by the likes of Scase and Goffee (1989). This change occurred at a time of increasing competition from the other banks and the building societies and at a time when the effects of the bad debts in less developed countries were starting to wreak havoc with the banks' balance sheets. Public opinion of banks was apparently declining and morale was very noticeably low in 1990 when I left.

This morale problem was exasperated with the announcements of layoffs in an industry that had seen dramatic growth over the 1980s. The initial reductions were

hardly noticed by the majority of employees as they were achieved through natural wastage and a decline in the number of new staff employed. The banks then offered voluntary redundancy packages but eventually, whilst I was working on this thesis, they resorted to compulsory redundancies. Such action was an option when I conducted my research but most hoped that it was not to be necessary. The belief that it was possible indubitably affected the results received.

When I left I had spent five years working with some very honest people and was somewhat shocked by the difference in attitude between them and many of my colleagues at university. This lead me to wonder whether there was possible research to be conducted into their attitudes and why they do not commit crimes - was it possible that the package that the banks offered and the promise of job security was attractive to highly moral individuals? When they clearly have so many opportunities why do they not commit more crime? In my time with the bank there were always rumours of managers who had escaped to Spain with millions of the bank's money but such stories were never substantiated, the only crime that came to my attention was that of a loans officer who had been issuing loans in the name of doubtful customers and pocketing the money himself. When the loans defaulted he would write them off as bad debts. When the story came out it was revealed that he had been having an affair with a female clerk and had consequently been suffering financial pressures. Most other bank employees have opportunities to commit crimes everyday but do not, why not?

This fascination with crime represented the seed of the idea to conduct a number of pieces of research to assess the risks facing the banking industry with the changing employee profile, the decline in the number of supervisory and middle management grades, the increasing use of computers, the changing face of the market they compete in, and the change in the psychological contract between employee and bank and its consequential impact on the "contract of trust". These changes all represent pressures that have consequences for the employees of the retail banks. Many of these changes so far were poorly communicated to the staff and loyalty has been tested.

The banks face then a number of sources of risks when fraud is considered. The bank staff in the retail branches have been a low risk source but a large potential source all the same. The risk of fraud by bank employees on third parties was a type of crime considered in passing in chapter 3 which considered the problem of City Crimes.

The greater use of computers prompted the survey to consider the factors that must be considered when assessing the risk of computer crime. Was it realistic to expect bank employees to resort to computer crimes when they felt that the banks no longer cared?

The ultimate aim of this thesis was to highlight the fact that the banking industry is changing and that consideration must be given to the impact that this change has had on the loyal individuals who joined the bank when lifetime employment was still a given and a job in a bank was seen as a position of respectability in the community.

Simon Rogerson,
September 1995,
Brussels.

# Acknowledgements

There are many people who have offered me assistance with the research and work that has gone to the preparation of this thesis. My supervisor, Professor John Sharp, deserves a great deal of sympathy for what he has suffered from me over the time it has taken to reach any form of conclusion. He deserves most of the credit for any good points that this thesis makes and none of the blame for the crass errors that I claim as my own. Thank you John for your patience - you will never realise how much you actually taught me from the reading of this.

Professor John Glynn deserves some of the blame for my enrolment as a PhD student. He has since proved to be a good friend and I hope that he will not be too displeased with his decision.

Mary Hughes is thanked profusely for her patience and I hope that other students are aware of the sterling work that she does in attempting to help lazy students finish thesis on time.

My family deserve some credit for embarrassing me into at least submitting a work of some description. They have always been supportive and I could not wish for more. I love them all.

My former colleagues proved to be a willing sample set and offered introduction to further sample members. They talked frankly about the changes and their attitudes to their work.

The strangers whom I pestered with my computer misuse survey are acknowledged with gratitude. Many wrote essays in response to some of their questions and their labours may be found in full in appendix a.

The staff at CBS deserve a special thank you for being so accommodating to me during my stay with them. It is possibly their fault that it took so long to finish as I wasn't in a hurry to leave the comforts of such a "home".

Chris Clarke and the staff of Ecole Superieure de Vente Industrielle Internationale are thanked for offering me a home when my grant ran out. I enjoyed teaching there and would have loved to have stayed if it wasn't for the lure of well paid employment in Brussels.

Special thanks also goes to a young lady in Belgium who twisted my arm to try to finish. Thank you.

*"Do not try to find out - we're forbidden to know - what end the gods have in store for me, or for you." Odes, I, Horace.*

# Chapter 1

## General Introduction

*"The FBI estimate that white-collar crime cost US employers $40 billion last year [1988]. And nearly 25 per cent of all white-collar crime is linked to the banking and financial services industries...*

*"Employees who steal from banks do not fit into a nice identifiable profile. Sure, some are habitual offenders, and some have expensive addictions. Other recent inside bank robbers include a grandmother with a spotless 20 year employment record, a top senior manager on his way to retirement, and others who were respected pillars of their community...*

*"Nearly 90 per cent of computer fraud is committed by insiders. As banking becomes more and more electronic, the chances of major losses and illegal funds transfers can happen with a few quick strokes at a keyboard." (Bankers Monthly page 42, April 1989)*

### introduction

The purpose of this thesis is to examine the relationship between crime by employees and changes in the banking industry. It will focus on non-violent financial crimes and the motivation process involved in *preventing* such actions. Emphasis will be placed on the possible impact that the computer might have on this process, both in the way that it may be used in the execution of a deviant act and also on the way that it is altering job expectations and the psychological contract of many employees.

### thesis structure

The main body of this thesis is divided into three broad sections. The first section proposes a motivational model for *business deviance*, especially those deviant acts committed by employees against or on behalf of their employers. This first section of this thesis will consider the relationship between *skill, opportunity* and *motivation* and their importance in the commission of *business deviance*. Does opportunity really create a thief as the proverb maintains? What are the dimensions of opportunity and how important is the *division of responsibility* or the *random rotation of duties* for the prevention of white collar crime. It must be remembered that it is not just the opportunity to perpetrate the crime that is important but, perhaps more importantly, the opportunity to *get away with it*.

The key aspects of motivation will be considered and appropriate theories considered; particular attention will be given to *Fishbein's Theory of Motivation* and how it might be used to understand the *criminal motivation process*. From these theories a map of motivation has been devised. The aim of this exercise is to offer an overview of the situation and to forward a possible relationship between the various factors involved. It is not intended that this map should be used as a definitive article, merely that it should operate as an aid for discussion; to try to create a more exact model of such a complex process is bedevilled with many drawbacks. The aim of this process is to create a highly exploratory model that identifies many of the key dimensions involved in the motivation process.

There are many different types of *business deviance* that may be committed and these may be categorised in a number of ways. They may be classified by motive:

- Need for money (Breed 1979)
- Need to balance the books (Ditton 1977)
- Need to improve poor figures
- Revenge against an employer (Greenburg 1990)
- Vandalism
- Showing off

They may also be categorised by the position of the individual committing them (West 1983):

- Senior managers
- Junior managers
- Supervisors
- Junior employees
- Outsiders

The level of the individual will affect the type of crime that they may commit in the other categories. For instance, a senior manager will have more opportunity, and possibly motivation, to balance the books. The crime may

be categorised by the amount of money involved. Here again the level of the individual in the firm will affect the category that it will potentially fall into. There is then a categorisation that divides the crimes by the method used to perpetrate the fraud. The major category with this method is believed to be the old fashioned *input fraud*[1], although *advance fee fraud*[2] also represent a growth area, certainly with regard to serious fraud.

For the purpose of this thesis a categorisation method is proposed which divides the crimes by way of the parties involved and how they are related (see chapter 2). The reason that this is done is so as to examine the process involved in the execution of a crime by an employee and to assess how this process differs when the company is the victim as compared to when it is the beneficiary. Also many of the other methods are inappropriate for the clerical and junior managerial grade bank employees at a branch level. Most importantly, though, it offers a categorisation that highlights the major areas of risk from internal factors. Some of these internal risk factors are as a result of the motivational impact of the banks' increasing reliance on computers, a reliance that has also increased the external risks from *computer-related crimes.*

The second section of this thesis will be divided into three parts which will examine the three types of *business deviance* proposed in more detail. This will be achieved by way of three studies - one on the changes in the banking industry and their impact on employee motivation; one examining the problem of computer misuse; and one about fraud and other financial crimes. Each of these studies will focus on a particular risk that the banking industry as a whole faces.

---

[1]An input fraud involves the manipulation of input documentation for fraudulent purposes. For instance a clerk might alter the payee's name on a payment instruction to that of an alias or accomplice after authorisation has been received.

[2]An advance fee fraud is a fraud that involves the creation of a bogus project that the fraudster will offer to firms to bid for. As part of the bidding process the company will have to show their commitment by pay set-up costs in advance. The fraudster leaves and the project never materialises. Sometime referred to as *Nigerian Frauds*.

The study of the changes in the banking industry will highlight the situation with regard to the level of staff employed in the major banks and the possible effects that declining employment levels and compulsory redundancies may have had on the attitudes of current employees. The banks have become reliant upon computers over the last forty years and they now perform many of the tasks that were fulfilled by humans. This has led to a possible rise in the number of opportunities to commit input frauds. The reason that this assumption is made is that computers are easier to deceive because they do not work on intuition or hunches, or because humans do not feel the same guilt deceiving a machine. A second possible reason for making the above assumption is due to the effect that the computer, and in particular *management information systems*, have had on the structure of organisations. The banking industry has seen a reduction in the number of levels within its structures that has led to a reduced number of middle managers and supervisors capable of checking work.

This study goes on to present the results of a survey conducted by the author which addresses the issue of crime in the banking industry. More particularly it tries to measure the attitudes of the current employees in the banking sector towards the issue of crime and also the computer. With regard to the computer the intention is to show that the majority of branch staff in the main clearing banks have limited computer ability, that they would, on the whole, be incapable of committing a sophisticated computer crime. That said, the survey will show that many employees believed that the number of opportunities has increased with the decrease in the number of supervisory positions.

The survey considers the respondents' attitudes to crime, both within the banking industry and in general. It aims to highlight motivational problems that have arisen as a result of the changes in structure and perceived employment terms. The relationship is hard to confirm on a factual basis other than by the remarks of some of the respondents. The reason that it is of

concern is because some research has indicated that there may be a link between job dissatisfaction and crime against the employer (Greenburg 1990). If it can be shown that the staff of the clearing banks at branch level are dissatisfied with the way that their employers have handled certain changes in their employing bank's working environment then it is possible to conclude that there is a risk of crime as a result. Of course it is impossible to say definitively that this risk exists and that the cause of this risk is the dissatisfaction felt by the bank employees as a result of the changes in their working environment.

The second study in this section will address the issue of *computer misuse*. This study will attempt to highlight the key factors with regard to computer crime and the law regarding such activities. This study will produce a three tier categorisation of computer crime which may be used in the assessment of risk. It will consider the issue of *security* and the methods used; and the relationship between *cracking* and security. The developments in computer communication will be outlined and the importance of the *Internet* metanetwork in this will be considered. The issue of *netiquette* and what the *Internet* should be used for will be examined. There have been many changes in the environments in which computers operate as well as changes in the computer systems themselves. The types of software used have become more complex and the processing power and memory storing capabilities of the hardware on which they run has improved exponentially; a growth so stunning in size that it is hard to conceive of it occurring in any other industry. These changes seem to have made many systems accessible to the public at large that never were before. It is not many years since user accounts on university mainframes were limited to computer science students and faculty members. Now it is possible to access the World from home with the aid of relatively cheap equipment; although the cost of telephone time in the UK may make this prohibitive, it is still a possibility. This increased use of networks has brought together an interesting mix of the purist and entrepreneur. As *Philip Elmer-Dewitt* put it :

*The world's largest computer network, once the playground of scientists, hackers and gearheads, is being overrun by lawyers, merchants and millions of new users. Is there room for everyone? (Time July 25, 1994 page 34)*

The system also faces the possibility of regulation because of the abuses of some of these new users. Many governments fear the threat of hackers and pornographers who seek to use the network for illegal purposes. As part of this second study the results of a survey which considers the problem of *computer misuse*, in particular the problem of *cracking* and other types of computer misuse, will be presented. A questionnaire was devised which asked for responses from computer professionals around the world, and was then *e-mailed* to every address on the list of contributors in *The Hacker's Dictionary*. The responses were very encouraging on the whole but included a number of negative comments alluding to misuse of the Internet. Such comments make interesting reading when considering the question of a *Lost Eden*.

The main purpose of this second piece of original research was to identify dimensions associated with the committing of computer crimes, or more appropriately the committal of acts of computer deviance, as crime *per se* is measured by law whilst deviance need not necessarily be illegal. The purpose of trying to uncover the dimensions involved was to show that on the whole they were inconsistent with the dimensions that the average bank employee works with. This allows us to make the assumption that the average bank employee is not very likely to commit a pure computer crime or *computer exclusive crime*[3]. That is not to say that they will not commit a computer-related crime just that it is unlikely to be of the category of crimes that require a high level of computer knowledge. They are more likely to commit a computer-related crime that falls into the category of frauds known as *input frauds*.

[3]The terms Computer Exclusive Crime and Computer Related Crime will be discussed in more detail in Chapter 8.

The final study in the middle section will consider the risks to the banking industry of fraud, embezzlement and mismanagement resulting in financial loss. This section will also consider the impact that fraud by the *elite* within an organisation might have on junior employees, in particular it will consider the *signal* process phenomenon that such crimes represent to these employees. It will be argued that these crimes represent a greater threat to the banking industry due to their potential size and *"Baringesque"* impact.

In the final section of this thesis it is intended that the map of motivation will be amended to outline the possible motivation process for a bank employee. This *knowledge map* will draw upon the theories of *Fishbein, Herzberg, et al*, as well as the responses from the bank employee survey to develop an approximation of the process involved in the commission and moral prevention of deviant behaviour by bank employees. This part of the thesis will also include any inferences that may be made about trends and likely scenarios. It will attempt to highlight those factors that must be considered by rational decision makers and any other threats that could potentially arise as the banks change. This section will also highlight the conclusions that may be made as with regard to the risks that the banking industry face and what lessons may be learned from the findings of this thesis.

## rationale behind such an approach.

The personal element of computer related crime has been inadequately addressed in the rush to implement Utopian "*foolproof*" security measures. Just as the alchemists search for the formula for gold was fruitless so shall be the search for the completely secure computer system. The main weakness with any computer system is the point at which it must interact with humans, who by there nature are not *secure*. Whilst technicians strive for this elusive goal many managers overlook a very practical approach to this problem and that is to consider the motivation of the employees. The *Trinity of Fraud* will be introduced later and from this it is apparent that the motivation of the culprit is an important aspect of any fraud. It is therefore possible to envisage

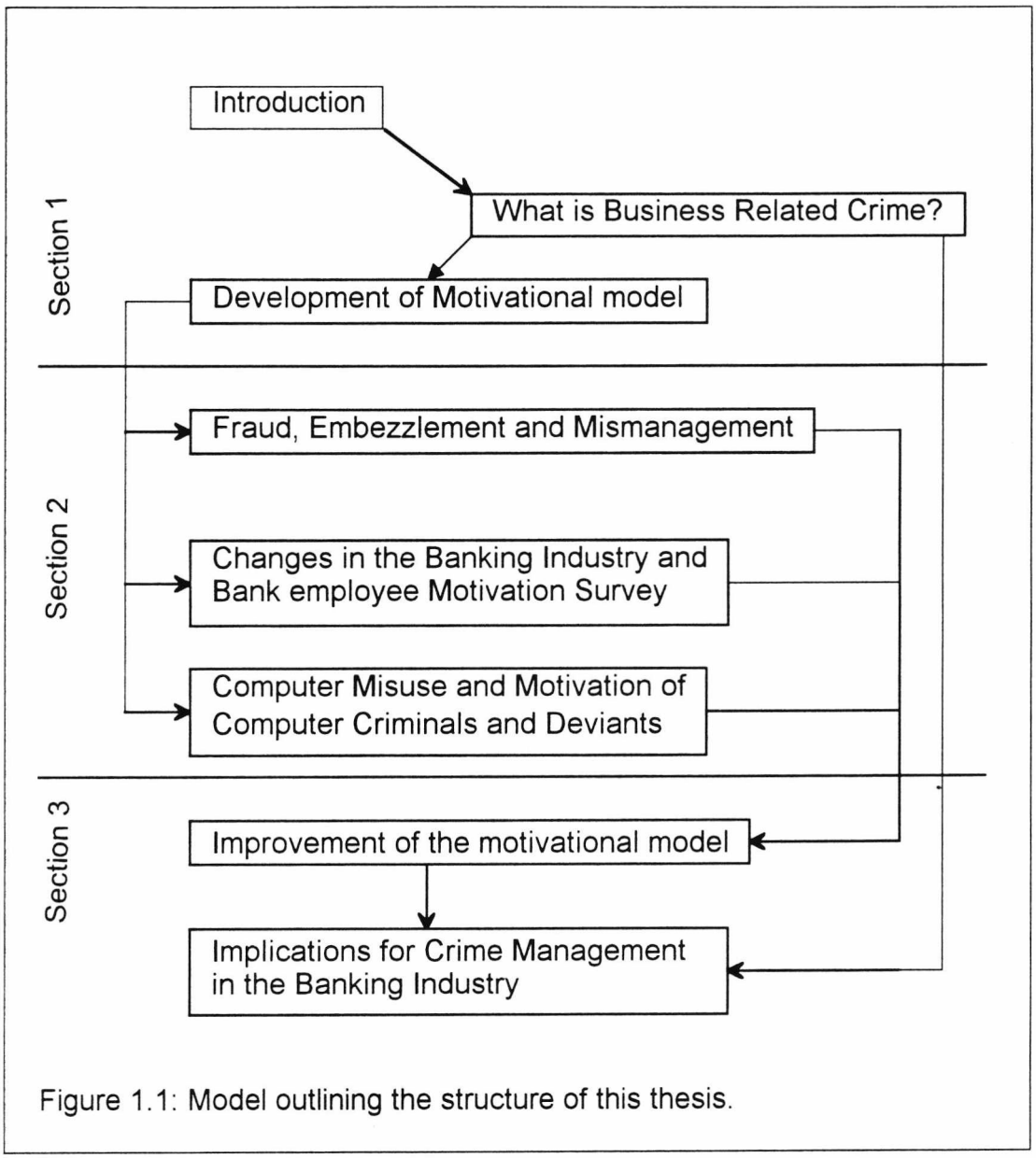



Figure 1.1: Model outlining the structure of this thesis.

an environment in which secure systems are achieved based on the honesty of the employees that operate them. Of course there are many instances where this is not possible if the system is also open to non-employees.

Another important area related to the increase in computerisation is the attitude of employees. Many computers are undertaking jobs that were formerly completed by humans. This loss of work can be highly demotivating if it is not substituted with alternative forms of employment. What happens then to employee attitudes if the general economy is suffering from high levels of unemployment and there is a threat of future redundancies in their industry, especially if this coincides with a rise in the use of computers. It is

just such a scenario that faced the Financial Sector at the beginning of the 1990's.

Improving the attitude of employees and increasing morals as well as morale would seem to be an effective alternative. Increasing the trustworthiness and encouraging honesty and openness through the culture of the company or unit could have very positive results.

Figure 1.1 offers an overview of how the issues raised above will be tackled. The thesis has been organised into three broad sections. Section 1 (Chapters 1 and 2) offers an overview of the issue of crime at work before presenting the Model of Motivation that will be developed from the findings of the research.

Section 2 of this thesis consists of Chapters 3 to 8 and tackles three broad areas. Chapter 3 considers Fraud, Embezzlement and Mismanagement by looking at two high profile cases and the general crime of Insider Dealing. The case studies offer lessons on what can happen when the management do not understand the organisation that they lead or the environment that it operates in.

Chapters 4 and 5 then go on to consider the issue of fraud from the bankers' perspective. This offers an interesting view of the issue of crime by employees by asking the question: *Why do employees not commit crimes more often*? This section looks at the changes that the banks have experienced and consider the impacts that these changes may have from a motivational perspective. These chapters present the findings of a survey conducted by the author to ascertain the views of bank employees to the changes that they are currently experiencing and their attitudes towards crimes and deviant behaviour in the workplace.

The final three chapters of this section look at the issue of computer crime and includes an Internet survey conducted by the author to gather information about computer misuse and *Crackers*.

These three sub-sections broadly consider the three types of crime proposed in Chapter 2 and consider the issue of managing people in environments with changing or different cultures. In particular it gathers information about the risks that banks face as their reliance on computers increases and their culture changes from a service to a sales oriented one.

Section 3 draws the various findings together and proposes a Model of Motivation for how a moral employee might act deviantly. The purpose of this model is to highlight the areas that managers need to focus on when considering crime management from a motivational perspective. It does not negate the need for good supervisory systems or internal audits.

## white collar and computer crime in general.

Estimates of the effect that White Collar Crime has on business and the community at large can be startling in size[4]. Research in America suggests that the cost to business in the USA is measured in billions of dollars every year. The FBI estimated that this cost was $40 billion in 1988, and that nearly $10 billion of this loss was linked to banking and financial services (Bankers' Monthly, April 1989). Lipman and McGraw (1988) suggested that bank employees stole nine times the total stolen by bank robbers in the years 1984, '85 and '86. Their figure for 1986 is not as staggering as that of the FBI for 1988, but at $1.1 billion is still significant, so significant that they suggest

[4]It is safe to say that white collar crime has risen with the increase in the number of people employed in white collar jobs. It is not possible to assume that this rise is *pro rata* though. In the next chapter a categorisation will be proposed that sorts crimes and deviant behaviour by the parties involved. By considering *business deviance* rather than merely white collar crime allows an examination of the motivational process without being *hamstrung* by preconceived ideas of what the crime entails - white collar crime now being a media reality involving crime by the priveledged.

that "*insider fraud and theft is a factor in about one-third of all bank failures.*" (Lipman and McGraw 1988 page 52).[5]

These figures are related purely to white collar crime in the USA, but estimates for similar *business deviance* in the UK are just as staggering. The Confederation of British Industry estimated the total lost by British business to criminals is between £5 and £10 billion a year, more, they point out, than was spent on non-military research and development (CBI 1990). These figures are only estimates, but can be assumed to be reasonable if we consider that the fraud squads of the City of London Police and the Metropolitan Police investigated frauds with a combined total of over £1.3 billion in the London area alone in 1985 (Levi 1987, page 23). If we also assume that much fraud goes unreported, for various reasons, and of course undetected, then we may assume that the CBI's estimate is reasonable for the country as a whole.

The research on which this thesis is based considers the impact that crime might have on banks and their staff. It is also interested in the impact that computers will have in this regard. It has been suggested that "*nearly 90 per cent of computer fraud is committed by insiders.*" (Bankers' Monthly, April 1989, page 42). Insiders have perpetrated frauds with the use of computers at many well-known firms and multi-nationals. Volkswagen lost $260 million as a result of phoney currency transactions, whilst First National Bank of Chicago nearly lost $70 million as a result of a series of bogus computer transfers. A bank clerk in the Netherlands made two fraudulent computer transfers using his and another's passwords. $15 million was involved and he was caught only due to a *technical malfunction.*

The first of these three cases is perhaps the most sophisticated fraud of the three, involving the manipulation of exchange rate transactions and was perpetrated by four "insiders". It still involved, what may be termed, *input frauds.* An input fraud involves the manipulation of system input

[5]By comparison the four biggest clearing banks in England made a combined profit of £3.1 billion in 1986 (British Banking Association 1984, Table 2.01, page 26)

documentation. It requires a knowledge of the administrative procedures, but very little of the system that executes the processing of the documentation. In the pre-computer era the processing was handled manually, but is now handled in many cases by computer. This change, it can be argued, has converted these frauds into *computer-related frauds*, albeit the least sophisticated of such frauds (the categories of *computer-related fraud* will be discussed in chapters 6, 7 and 8).

The Audit Commission stated that "*... the value [of input frauds reported] was significantly higher, and of the 57 cases, the five relating to creditor payments represented 70 per cent of the total fraud losses*" (Audit Commission 1987, page 3). The Audit Commission recorded a total of 118 cases of computer fraud and abuse. This is a small total but it must be remembered that much computer fraud goes unreported. The responses presented in the Audit Commission's 1993 report indicated a wider range of misuses. Of 285 incidents listed, 97 involved fraud, of which 88 *per cent* involved *input fraud*. Of the other incidents, 61 involved use of illicit software or use of computer equipment for personal use, 75 cases of virus attacks and 10 of hacking. In total, losses of £3,822,213 were incurred by the respondents of which nearly 80 *per cent* related to fraud, all of which were perpetrated by *insiders* or employees of the company.

Some estimates suggest that as much as 85 *per cent* of *computer-related crime* goes undetected or unreported (Webber 1984). Computer fraud and abuse may go unreported for a number of reasons:

- No financial loss was involved
- The victim was too embarrassed to report the fraud
- The fraud was concealed and was not discovered
- The system manager put it down to system error or software failure
- Or, in the case of the Audit Commission's survey, the victim was not sent a questionnaire

This list is far from comprehensive, but shows many possible reasons why the Audit Commission's 1987, 1990 and 1993 totals are far less than the true total.

One other problem is in the definition of what constitutes a *computer-related crime*. The term, like white collar crime, is a far from exact one. It has been used to describe acts ranging from battery with a computer keyboard[6], to some sophisticated computer cracking involving military computers in the USA (Stoll 1991, Haffner & Markoff 1992, Sterling 1992), academic and medical facilities in the UK[7], and the world-wide exploits of *the Condor*, Kevin Mitnick. This problem will be considered further later, in the meantime it is necessary to consider the factors that influence the general fraud process.

Unfortunately, "*There is no general offence of fraud as such in English Law*" (Law Commission, 1987, page 1), although the Law Commission does offer a possible definition as being when, "*[a]ny person who dishonestly causes another to suffer [financial] prejudice, or who dishonestly makes a gain for himself or another commits an offence*" (Law Commission, 1987, page 133). It is possible to conclude that a fraud is any action, or sequence of actions, that deprives another of money or rights by illegal methods. It must also be remembered that fraud should not be confused with other forms of theft. Fraud usually occurs in relationships of a financial or commercial nature, and normally involves an element of trust by the eventual victim. Just such a relationship has existed for many years within the banking industry. Trust was rewarded with job security and good, but long-term, job prospects. But *the times they are a changing* (Cressey & Scott 1992, Taylor 1993). It is necessary now that bankers understand the motivation of crime so that they may assess the risks associated with these changes and the effects that they may have on the attitudes and norms of employees.

---

[6]A rather tongue in cheek hypothetical example offered by **Wasik** (1991) to emphasise the extent that the term might be used. A more recent example to test the term is the theft of automatic teller machines (ATMs) using a JCB digger, to term such as computer-related is, whilst technically correct, somewhat preposterous

[7]Nicholas Whiteley was prosecuted in 1990 for just such activities. He is believed to have caused more than £25,000 worth of damage. (**The Times**, May 2, 1990 & June 8, 1990)

## criminal motivation

It has been suggested (Comer 1985) that for a fraud to occur three main factors must be present: *knowledge/skill*, *motivation/intention*, and *opportunity*. It is necessary to consider what interdependencies there are between these three factors. For instance, will someone who, for what ever reason, feels motivated to commit a fraud, have more confidence in his skill to perpetrate the fraud. It is clear that a criminally motivated individual must be aware of the opportunity, and must believe that they have the skill required, before they will attempt to commit a fraud.

There is no link between *opportunity* and *knowledge/skill* as it is assumed that every opportunity is an opportunity regardless of the skill level required to perpetrate the fraud. Therefore, the theory implies that a fraud can only be committed if the level of skill is equal to, or greater than, the level required to take the opportunity. There is another aspect to opportunity that must be considered by the criminal: the opportunity to *get away with it*. The fear of punishment probably deters many who would otherwise feel inclined to deviate.

Most people experience one or more of the factors at some time or other, but will not commit a crime/deviant act unless all three are experienced simultaneously. Some crimes are harder to commit than others, either opportunities to commit are rare, or the skill required to complete the crime successfully is high.

Computer crime is a good example of a high *knowledge/skill* crime and for that reason it is viewed with an element of awe by the general public, but is this a fair assessment? Possibly, but the current evidence seems to suggest that the majority of computer crimes are quite simple in nature. The Audit Commission found that: "*By far the largest number of frauds was perpetrated as a result of unauthorised submission and alteration of data*" (1985 page 14).

In other words the vast majority of computer crimes were *input frauds*, a fraud determined more by *opportunity* than by *knowledge/skill*. Wasik supports this finding:

> *"While it is true that some hacking techniques are much more ingenious than [basic computer security methods], the evidence is that the vast bulk of cases of unauthorised access to a computer occur in circumstances where quite inadequate security precautions have been taken. It is relatively cheap and simple to install these defences, which will effectively deter the majority of attempts to gain unauthorised access." (Wasik 1991 page 43)*

But such a finding is based on a relatively small number of crimes reported to the Audit Commission[8]. So do these figures portray the picture fairly? or are many cases of computer misuse going unreported? There are a number of possible reasons, listed above, why such frauds may not be reported. There is one that is listed above, which must be considered as very important in the case of banks and their ilk, *embarrassment*. One reason why the banks might feel embarrassed to admit that their security system had been breached is to do with their *Duty of Confidentiality*[9] and because they have certain duties under the *Data Protection Act 1984*.

In one case, prior to the introduction of the Computer Misuse Act 1990, two hackers hacked into British Telecom's Prestel service[10]. In 1984 they broke into the mailbox of Prince Philip leaving a message saying: "*I do so enjoy puzzles and games. Ta. Ta. Pip! Pip! HRH Royal Hacker.*" (Clough & Mungo 1992, page 39). They also altered messages and information pages including, on November 2, 1984, the rate of exchange quoted by the Financial Times for £/$ to £1 to $50. Gold and Schifreen were eventually arrested in 1985, were charged with forgery of passwords, and were fined £600 and £750 respectively, plus £1000 costs each. They appealed to the Court of Appeal who held that their offences were not covered by the Forgery Act and overturned the verdict. The House of Lords upheld this decision on the subsequent appeal thus acquitting the pair (Clough & Mungo 1992, page 41-42). Whilst this case does not involve a bank as a victim it still highlights a

[8] 77 cases in 1985, 118 cases in 1987.
[9] Tournier v National Provincial and Union Bank of England [1924] 1 K.B. 461.
[10] Gold & Schriffren v. R [1988] AC 1063.

possible threat, and raises the question of just how secure computer based files are. It must also be emphasised that it is often the human element that undermines the system's security[11]. Banking folklore has that, in the early 1980s, journalists were able to gain access to bank details of the Prime Minister's husband and son using only a phone and stealth. Such *attacks* cause embarrassment to the enterprises responsible for running the systems.

In a survey by the *Computer Fraud and Security Bulletin*[12], it was found that 80% of respondents said that they would have been alarmed if they heard that their bank had been defrauded, but 90% said that they would also be shocked to hear that their bank had failed to prosecute for fear of bad publicity. If the embarrassment factor is a significant one for the banks, then careful consideration is required before action is taken. This survey may support the argument that fraudsters should always be prosecuted, but banks might still be reluctant unless they can ensure success in court.

[11]In the case above the passwords they encountered were laughably simple and easy to guess.
[12]Reported by Comer (1985 page 281).

# Chapter 2

## Background

*"It's all done by lawyers," he said helplessly, "and I suppose they embezzle a lot." Sebastian Flyte in Brideshead Revisited (Evelyn Waugh) page 61.*

*"Computer frauds are not unique in character; rather, computers are used to facilitate frauds which might well have been committed by traditional means. Whether the quantitative change posed by the advent of computers has resulted in a quantitative change to new forms of fraud is a barren question. There can be no doubt that they have changed the magnitude of the risks." (Leigh, 1982 page 61).*

*"In the end, Conrad's death was not a great problem. Although he was sullen to the end, I had the impression he went willingly enough. Maybe he was ready to sacrifice his life to save my career... He was smiling when I pulled the trigger." (Walker 1985 pages 237 and 240).*

### the trinity: skill, opportunity & motivation.

To assess the risk effectively it is necessary to understand that for a crime to occur (or any action for that matter) three factors must be present: skill, opportunity, and motivation. Skill is the ability to commit an act which is effective at realising the opportunity and may also refer to the ability to avoid detection, or *get away with it*. Opportunity may also refer to the opportunity of detection avoidance. An English proverb claims that *opportunity creates a thief*, but this is far from true in the majority of cases. It takes more than mere skill and temptation. There is the third factor, the motivation of the potential perpetrator, that must be present before the act will be executed.

The level of crime in an environment where the opportunity is high and the skill required low will be dependent on the motivation of those that experience the opportunity. If we consider the case of bank clerks (who experience a similar environment to many office workers but with the exception that their role involves dealing with large sums of money) we can assume that the vast majority of clerks have very little computer expertise[13]. They may be able to operate a word-processor or input *waste* (a collective banking term for the cheques and credits when input) at speed, but these skills are insufficient to

[13]An assumption that is supported by the responses to the survey presented in chapters 4 and 5.

navigate the intricacies of a network, or for the writing of a programme to capture passwords for instance. This would seem to indicate that the threat of computer exclusive crime being committed by employees is slim.

The most obvious area of exception is that of the computer department of banks. These employees are recruited for their skills with computers so that the chance that they are able to write malicious programmes, or have the knowledge of how to cover-up transfer payments[14] will be high. The control of such a threat requires special skills, although some simple measures may be taken like ensuring that such employees have a recognisable career path to pursue. It is not the intention of this thesis to consider these problems in detail, the author is more concerned with the process by which computer-related crimes are committed by non-computer staff and possible ways in which they may be prevented.

The majority of recorded computer crimes are low tech (*computer dependent* [15] and *computer related*) rather than high tech (*computer exclusive*), so it may be assumed that for a fraud to succeed, and that includes avoiding detection, the perpetrator need not be a computer expert. It is not a knowledge of computing that will ensure obscurity, although it may help, but a knowledge of the organisation's procedures, as ignoring the internal and external auditing process will lead to a fraudsters's downfall. A company employs individuals to further its aims and will in many cases take measures to avoid fraudulent activity by its employees. This may be achieved in one of three ways. Firstly employ idiots who are incapable of *fiddling the books*. Secondly, create a procrustean and bureaucratic organisation that double-checks its double-checks. Thirdly, ensure that their employees are not motivated to act fraudulently.[16]

---

[14]The opportunity to "get away" with the crime is an important consideration when planning a fraud or any crime. Ensuring that employees feel that the chances to "*cover-up*" a fraud are minimal will reduce the chances that the fraud will be committed. Conducting regular internal audits and communicating the fact is one way to do this.

[15]Terms discussed in Chapter 8.

[16]The three alternatives offered here relate to the way that the management of a firm views its people. Ideally a company should also set-up good procedures and conduct regular internal audits of such. Many companies also have departments dedicated to the audit

Obviously these three alternatives are grossly simplified, but it is clear that, with few exceptions, the third approach is by far the sanest. The second has many good points which should not be ignored, but in the most cases good computer "*common sense*" can ensure that embarrassment caused by computer fraud is kept to a minimum; a major consideration for system managers in all organisations, especially banks. For years the security of a system has been dependent on the limitation of opportunity[17]. This focus has been at the expense of other approaches. This thesis considers the problem from a motivational perspective; an approach that is of value when you remember that the vast majority of recorded computer crime is low tech. Ensuring that your staff are motivated positively rather than negatively is a must for all good managers. As computers become more prominent in the operations of book-keeping, payroll management, logistic management, etc. it is important that the risks associated with a poorly motivated workforce, or indeed a motivated one suffering from other pressures, are understood.

So what pressures do individuals experience that might make them act in an unacceptable manner? There are of course various drugs and mood altering substances that affect the way individuals think and behave. They represent serious problems for many people. Of more interest are "*social*" pressures, that is the influence that groups exert on their members, and corporate pressures. If a manager feels pressurised and will only make their target by dumping toxic waste in an illegal manner they may do so. They do not act in this way because they think it is the best decision, but because they feel it is the only decision; a new manager will do it if they do not. Kramer (1992) tells the story behind the Challenger space shuttle disaster and how during a

---

process and conduct random reviews of the ways that the procedures are executed to ensure that their are no anomalies and computer systems can be used to alert management to the warning signs which might herald problems. The primary purpose of this thesis is not to review the internal audit process but to consider ways that it might be strengthened by better understanding and management of the motivation of employees. These processes are not mutually exclusive but should represent integral parts of any crime management system.

[17]This approach is logical when the defence is designed to withstand "attack" from unknown individuals. In such instances opportunity is the only element known. With the case of internal security for banks this is not the case; skill and motivation are also assessable.

recess from a meeting with NASA officials, senior managers from MTI, the company responsible for the fatal O-rings, told an engineer to "*take off his engineering hat and put on his management hat...*" (page 232). The advice about the O-rings was reversed and the rest, as they say, is history. There are a number of studies by Milgram (1963), Asch (1955) and Bonini (1964) that show the part that obedience, group pressure and "profit" pressure might play in the process. Whilst Janis (1972) coined the term *Group-Think* to describe the process by which a group of apparently clever people might make stupid decisions. It seems that human beings prefer to be wrong with the crowd than right on their own.

Sutherland (1940, 1949) proposed the theory of *differential association* to explain the behaviour of white collar criminals. He argues

> *that criminal behavior is learned in association with those who define such behavior favourably and in isolation from those who define it unfavourably, and that a person in an appropriate situation engages in such criminal behavior if, and only if, the weight of the favorable definitions exceeds the weight of the unfavorable definitions. (Sutherland 1949 page 234).*

Whether an individual becomes a criminal or not is determined, he argued, by the "*comparative frequency and intimacy*" of that individual with the two types of behaviour - deviant and law-abiding (Sutherland 1940).

The second process that Sutherland (1940,1949) proposed as part of his theory of white collar crime was that of "*social disorganisation*". He argues that:

> *differential association culminates in crime because the community is not organized solidly against that behavior. The law is pressing in one direction, and other forces are pressing in the opposite direction. In business, the "rules of the game" conflict with the legal rules. (Sutherland 1940, page 11)*

The idea of *forces* is developed further by Lottier (1942) who proposes a "*A tension theory of criminal behavior*". He argued that his theory supplemented the theory of differential association "*by attempting to explain the criminal*

*behavior of these offenders in terms of tension arising from biological and interpersonal as well as cultural conditions.*" (Lottier 1942, page 840). Lottier's theory was based on contact with embezzlers in a court's psychopathic clinic and from these discussions he concluded that there were two general categories of embezzler - the individual embezzler and the group embezzler. The individual embezzler occupied a position of trust and appropriated "*privately and by deceit and trickery the property entrusted to him by a reputable employer.*" (Lottier 1942, page 841). Lottier argued that

> *the individual embezzler is a member of a competitive society who commits embezzlement as a consequence of tension producing conflicts in the organismic, psychic, interpersonal, and cultural conditions of his adjustment. These four conditions are not separate and the theory emphasizes their unity. (Lottier 1942, page 842)*

He argued that the tension was critical in all the cases that he had contact with, that "*a critical tension situation*" had "*invariably precede preceded the embezzlement behavior*" (Lottier 1942, page 844). The group embezzler is also affected by the tensions apparent in the group and it is here that the theory of differential association must be considered Lottier argues (Lottier 1942).

The norms of the organisation, of perhaps more importantly, the group of people that an individual most closely works with, affect the way that that individual behaves. This internal environment may be affected in turn by the external environment in which an organisation works. Clinard and Yeager (1982) argue that this cultural environment "*may actually encourage or discourage criminal or deviant behavior*" by corporations (Clinard & Yeager 1982, page 74). Within the organisation, they argue, the norms of the sub-groups may be affected by the "*ethical tone*" set by the senior management, in particular the chief executive officer, they go on to argue that:

> *The atmosphere thus becomes one in which participants... learn the necessary values, motives, rationalizations, and techniques favorable to particular kinds of crimes. A corpo-*

*ration may socialize its members to normative systems conducive to criminality. (Clinard & Yeager 1982, page 77).*

Normalisation is a very important process in organisations as it represents an important part in the induction process. An individual is encouraged to accept the values and beliefs of the organisational culture - "*the glue binding together the disparate parts*" (Hunt 1986, page116) - and thus become a more effective member of the organisation. If the individual rejects the norms of the organisation the consequences for both the individual and the organisation might be difficult. Schein (1988) argues that the consequences of the rejection of norms is dependant on whether the norms are *pivotal* or *peripheral.* To accept both norms is considered *conformity*, and to reject both *open revolution.* It is possible for the individual to accept one type of norm but not the other. If the individual considers that the basic organisational goals are right but that there are other goals that they find unacceptable, then they are considered to be *creative individualists* as they accept the *pivotal norms* but not the *peripheral norms* (Schein 1988, page 100).

Clinard and Yeager (1982) noted that conformity is often achieved by the employing organisation through its training programmes. This is especially true of those individuals with potential to hold positions of responsibility they argue. It was a process supplemented by other aspects of the induction process:

*outside connections were reduced, and a club mentality is bred through overwork, frequent transfers, which inhibit attachment to loacal communities, and provisions for recreational and educational needs during leisure time. Co-workers and higher-ups become "significant others" in the individual's work and social life. (Clinard & Yeager 1982, page 80).*

Such a system helps to foster conformity and acceptance of both the pivotal or peripheral norms. If either group of norms is deviant then crime may occur. The goals of an organisation are of interest then to anyone concerned with the etiology of white-collar crime or business deviancy. Sherman (1982) suggests that many organisations have two sets of goals - *real* and *formal.* The *real* goals of an organization are determined by its interaction with its

environment. The real goals may be the same as the formal goals but are likely to be in some way different because of the effect of the forces - both internal and external - which impact upon it.

Sherman (1982) goes on to suggest two ways in which an organisation might become deviant. Firstly, it may adopt goals which deviate from the norms of society or which may only be achieved through law-breaking. Or secondly, the organisation encourages its members to act in a deviant or illegal manner in order to achieve socially acceptable and legal organisational goals. (Sherman 1982, page 66).

That legitimate organisational goals might lead to deviant behaviour is supported by Coleman (1992) who cites the case of the *Ford Pinto* as an example of where organisational goals or their sub-goals led to an illegal act. Ford had stipulated to their engineers that they wanted a car that cost less than $2,000 and weighed less than 2,000 lbs. When a fault became apparent in the design of the petrol tank the engineers chose to ignore it even though the cost of redesigning and improving the safety of the tank was $1 and an extra 1 lb - they were more concerned with meeting their targets. (Kramer 1982). Kramer (1992) in a later study of *The Space Shuttle Challenger Explosion* remarks that:

> *Given the strong performance emphasis at NASA, it is easy to see how the organizational strains that arose from the design flaw of MTI's solid rocket booster field joint pushed the space agency toward an illegitimate solution to the problem. (Kramer 1992, page 234).*

Organisational deviancy is important in the consideration of individual deviancy because of the relationship between the two. Organisations are merely collections of individuals, for an organisation to be deviant there must be an element of individual deviancy against the norms of society.

> *We assume that white-collar crimes are determined by social norms, accepted and enforced by groups and individuals with whom the individual identifies, groups which tend to give social support to the illegal activity. On the other hand, the legal rules and their enforcement are also determined by social norms, accepted and enforeced by other kinds of social*

*groups with which the legislators and enforcement agencies identify themselves and with which even the violators often have some measure of identification. The problems of the etiology of crime and of punishment seem then to relate to the same set of basic theoretical concepts. (Aubert 1952, page 267).*

A lot of fraud within companies is committed by individuals who are often termed *first time offenders*[18], who are surely less likely to be affected by personality traits and more likely to be affected by circumstances? Have the morals of society or parts of society changed that the opportunity is now more likely to be taken? Has the increase in Information Technology played a part in this process? If people's attitude to crime has changed such that they find it easier to justify *petty crime*, the incidence of fraud is likely to rise. Whether information technology has aided this process is debatable.

There is of course a variation on the theory that fraud has increased with the rise in use and dependence on information technology and that is that Information Technology has caused the rise in reported crime through the improvement in internal auditing systems, reporting systems themselves (the Police's Crime Reporting System etc.) and such like. Thus if one were to study the evidence there would seem to be a link between the use of computers etc. and the rise in reported crime, and that this link would seem to be a positive one. For instances, computers can be used to assess vast amounts of data to identify inconsistencies, an activity that is often not humanly feasible. On this matter Krauss and MacGahan (1979) state that:

*Government auditors and internal auditors should be alert to how the computer can be used to trace things and to locate inconsistencies. All too often, auditors fail to make the computer part of their routine audit procedures because of under-staffing and lack of data processing qualifications. (Krauss and MacGahan, 1979 page 7)*

In terms of the development of computer technology and their uses, 1979 is a long time ago. Nevertheless this quote highlights a problem which has taken

[18] That is not to say that they have not previously offended or committed frauds, just that they have not previously been caught.

a long time to be resolved, if indeed it has been. The fact is that advances in Information Technology are considerably ahead of the actual use of computers in business.

Krauss and MacGahan (1979) go on to offer examples of successes; of how an insurance company was able to identify a doctor who had made six claims in one year for the removal of the same patient's tonsils; or another doctor who claimed for an abortion for a patient in whose name he had previously claimed for a hysterectomy! Of course not all the successes are quite so bizarre. Such practices offer the auditors a very useful weapon in their fight against fraud.

## computers in banking.

The growth in the number of computers in the finance industry in general has been great and the effects have been acute. There are few areas of this industry that have remained unscathed by the impact of computerisation. The impact of this process on the banking sector institutions and their employees has been great and they have changed the way this sector operates. Computer systems have improved communication and funds transfer between branches within the constituent institutions and between the institutions themselves. ATMs and systems such as CHAPS, SWIFT, IMTs, BACS, Truncation of cheques, Switch and EFTPOS have changed the way money moves and funds are transmitted and received, but have also ensured that the number of opportunities for *computer-related crime* have increased

.

There have been a number of advantages and disadvantages inherent in this process. The most obvious potential problems relate to computer abuse - both by employees and outsiders - and theft of funds and information by employees. As well as these two there is the related problem of a loss of confidence and the importance of confidentiality. Banks must also adhere to the regulations and laws governing the use of computers - the most

applicable being the Data Protection Act - thus they must educate their employees about their changing duties and responsibilities.

The banking sector is a sector going through great change which involves the increasing use of computers and a decrease in the number of employees. Those employees who remain are facing great changes in their jobs and working lives as a consequence of these changes. These changes have led to a great change in the attitude of those employees still in the industry. It is an attitudinal shift that may have undermined the honesty inherent in the *trust culture* that has prevailed in the banking industry and computerisation has introduced three new areas of risk into the financial sector. The first is directly related to computers and that is the misuse of the systems that computers support. Misuse of computers themselves represent very low level crime and may or may not fall into the category of computer-related crime. Examples of this type of deviancy include the theft of a computer itself and should not be included in any serious analysis of the problem.

The second area is that of demotivation. Computerisation effects people in different ways. Firstly it improves performance appraisal, but only in a quantitative way, therefore focusing attention on those variables that affect the financial performance of units and individuals; and secondly it has reduced the level of employees need to fulfil many tasks. Levin (1992) suggests that were computers to become completely inoperative that the number of specialists required in every professional field from accounting to medicine would exceed 100 million in Western Europe alone. Whilst this can only be an estimate of the importance of computers it is still a startling one.

This loss of jobs has been felt quite markedly in the banking sector but its full impact was delayed by the increased requirement for manpower as a consequence of the *Lawson Boom* (Smith 1992, page 8) of the late 1980s. The number of people employed in the banking sector declined in the early 1990s. It was a decline that was evident in the late 1980s but was disguised

by changes in the profile of the type of individual employed by the banks. Between 1980 and 1990 the number of people employed in the British banking and bill discounting industry rose by over 40 per cent and rose every year with the exception of 1983 when the total fell slightly. In 1991 there was a decline of nearly 50,000 in the number of individuals employed to a total of 443,100 (these figures exclude those for the Abbey National PLC).

The consistent rise in the number employed from 1980 to 1990 hides one or two changes in the structure of the underlying figures. Analysis of the total number of males shows that this figure has been falling since its peak of 200,800 in 1988, whilst the number of females employed part-time rose again in 1991 so that over 12 per cent of the workforce were female part-timers compared with less than 9 per cent in 1980. This suggests a shift in emphasis from career oriented, salary earning employees towards a workforce of more part-time and possibly commission earning individuals.[19]

The future suggests further cuts in the number of employees in the banking sector. The major clearing banks have all announced cuts in the number of employees to be effective over the period to 1997. This obviously has effects on the motivation of those individuals currently employed by the banks.

## effects on motivation.

*All change in the banking sector.* But is this change at the cost of an increase in crime? It is impossible to measure the decrease in morality or a deterioration in norms as there is no adequate base with which to compare any findings of the current situation. That said, it is possible to make some assumptions about the moral code of bankers in previous years from literature and other commentary. It will be argued in this thesis that it is these strong norms that prevent most individuals in banks from committing crimes against their employing organisation except those *crimes* that have been normalised, such as the use of telephones to make personal family calls.

---

[19]This phenomena is discussed in greater detail in chapters 4 and 5.

As banks change their staffing levels in response to the challenge of new information technology, the move towards *flatter* organisational structures, and the need to cut costs in an attempt to retain their competitiveness and to mollify the City Institutions that demand larger profits, they will face growing problems with the staff that remain. In the past people joined banks with the view that they provided secure jobs, although a shade low paid. Now that has changed so that job security is no longer a part of the package.

Scase and Goffee (1989) conducted a survey into the effects that a flatter organisational structure had on the middle management of a number of large organisations who were flattening their structures. Such flattening usually involves the removal of layers of the hierarchy, if an individual is lucky they will be promoted or moved to a similar level in an unaffected part of the organisation; if they are unlucky they will be made redundant.

One of the sectors that their study covered was the financial and insurance sector. They found that, in general, motivation was low and that individuals sought more and more clarification as to what was expected of them, thus reducing any possible *intrepreneurial*[20] benefit to be gained from having more autonomous front line staff.

Whilst the Scase and Goffee survey considered the motivation of middle management it is possible to conclude that similar feelings will be felt by more junior members of staff within these organisations. These individuals may have aspirations of attaining middle managerial positions and as the number of such posts changes, so will their chances of promotion. Or they may be affected by the *trickle-down* effect as frustrated and demotivated middle managers take it out on their subordinates in such a way that they too feel demotivated and frustrated etc..

---

[20]Kanter 1983, 1989.

## fraud and motivation

One of the ways that the low morale levels might manifest themselves is in the level of *petty crime* that might occur (Greenburg 1990). It would seem clear that either the perpetrators of *computer frauds* are very effective at concealment, a definite possibility if managers lack the sufficient skills to *police* the new systems, or fraud is not as big a problem as feared. What is certain is that whilst the frequency of such frauds is apparently low; the magnitude of potential loss is correspondingly high.

What are the motives of the fraudster? In view of the low tech nature of most reported frauds[21], is it not possible that they are merely motivated by financial need or pure greed? How therefore does the high-tech fraudster differ from his or her unskilled cousin? There seems to be a greater acceptance of such crimes by the general public due to their intellectual nature. This acceptability is heightened when the victim is a very large corporation or government body [22]. A good example of this is the film "War Games":

> *"What War Games insinuates is that being able to handle a computer with virtuosity puts one above the common morality" John Sutherland (The Guardian 12 April 1984)*

This is an attitude that they themselves believe:

> *"There is a temptation to allow their technical wizardry to sanctify what is clearly antisocial behaviour. This should be taken into account when organising our response to hacking and other types of illicit computer linked behaviour." (Doswell and Simons 1986 page 58).*

Can controls be improved? In view of the fact that systems will be entered however secure, is it not time to consider strategies other than "*barricading the door*"? For instance, creating false trails for the intruder to follower; the "*minator*" approach to system security. See Stoll (1991) for an example of just such an approach in successful operation. What effect does the Computer Misuse Act 1990 have in this area? Does it go too far or not far enough? What

---

[21]The 1985 report by the Audit Commission found that the vast majority of computer related fraud was committed by way of "input" manipulation, rather than to do with the programmes of the computers themselves.

[22]Although this is not the case when the victim is "weak and helpless".

implications does this have for those who work with such systems? What approaches must the auditors of companies and their internal accountants adopt to counter these changes? The answers to these questions are technically oriented and are therefore largely outside the scope of this thesis.

This rest of this chapter will attempt to identify some of the motivations that lead people to commit *Business Deviance*. It will be argued that it is often the organisations that these "*criminals*" work for that cause them to commit crime. But it is not just this crimogenic nature of organisations that leads to a high incidence of such crimes, the ambiguity of the law that governs business and its general reliance on the doctrine of the "*reasonable man*" make the illegality of some actions far from certain.

Crime occurs in all walks of life, although the extent to which it occurs within business is difficult to assess as much goes unreported or unrecorded. John Banham, Director General of the Confederation of British Industry, and Steven Norris, Chairman of Crime Concern (UK) , have stated that:

> *Crime against business costs well over £5 billion a year and some estimates put it at over £10 billion...[m]ore money is stolen from British business every year than is spent on non-military research and development. (C.B.I. 1990, page 5).*

And that is only in Britain; estimates for other countries are just as startling. Lipman and MacGraw (1988) have stated that:

> *"America's national pastime is not baseball; it is theft. This is as true today as it was 15 years ago. If anything, the situation has grown worse. That might sound alarmist, but the facts cannot be ignored. In 1984, bank employees stole $382 million, nine times more than bank robbers stole. The total lost by bankers to insider fraud and embezzlement rose to $850 million in 1985 and to $1.1 billion in 1986, and insider theft is a factor in about one-third of all bank failures. Estimates of the cost of internal theft of all kinds range up to $40 billion a year, and it is thought that from 5 to 30 percent of all business failures each year result from internal theft." (Lipman and McGraw 1988 page 52).*

But by no means all of this is committed by *white collar criminals*; the vast majority is attributable to pilfering and other petty thefts perpetrated by employees of all categories as well as outsiders. The *white collar criminal* receives the press

as his[23] actions usually involve the abuse of trust or power and are usually for larger sums than usually attainable through other methods of crime. But what is a *white collar crime*?

> *White collar crime may be defined approximately as a crime committed by a person of respectability and high social status in the course of his occupation. (Sutherland 149, page 9)*

Friedrichs (1992) points out that whilst Sutherland gets the credit for the introduction of the term white collar crime some credit is due to the work of Marx and Engels, and Bonger (Friedrichs, 1992 page 6). Whilst Sutherland himself conceeds that the term white collar was borrowed from the title of a General Motors manager's autobiography. Nevertheles, it is Sutherland's definition which has represented a focus for discussion, sometimes heated, sometimes not, between the various sides of this on-running criminological and sociological debate.

> *We seek a definition of the white-collar criminal and find an amazing diversity, even among those flowing from the same pen, and observe that characteristically they are loose, doctrinaire, and invective. (Tappan 1947, page 275)*

Tappan was a critic of Sutherland and it is arguably his "pen" that he refers to in principal. Sutherland's primary aim was not that of a form of etymology but that of highlighting a weakness in the administration of the law. His purposes when introducing the term white collar crime was "*rooted in a moralistic and polemical tradition, and clearly intended to promote a broader consciousness of crime in high places.*" (Friedrichs 1992, page 6). It may be just as well that he did not insist on crystalising any definition as it is arguable that over half a century after the terms introduction there still is little consensus on what a white collar criminal is or what constitutes a white collar crime. Friedrichs refers to it as a multi-sided "*Chinese puzzle*" (Friedrichs 1992, page 16). Tappan (1947) sees the problem in black and white arguing that there can only be crime if the perpetrator's actions are prosecuted by courts under a

[23]If the prison population is any guide, the incidence of white collar crimes involving women is very low. At the end of June 1990 only 5.9% of inmates convicted of fraud, etc. were women (Home Office, 1992b)

penal code. Until prosecution is possible the crime is not a crime. Such debate caused Geis and Meier (1977) to state that:

> *The definition of white-collar crime, for instance, has always represented something of an intellectual nightmare. (Geis & Meier 1977, page 25)*

And following on from this they emphasised the difficulty that those who try to cost white collar crime face when they commented that:

> *The truth of the matter is that there is no reasonable manner in which to determine the monetary cost of white-collar crime. Other kinds of alleged consequences of white-collar crime, such as lowered social, moral, and inter-personal trust, may be measured, but it is an exceedingly intricate (and perhaps an impossible) task to demonstrate causal relationships between such phenomena and white-collar crime, even presuming agreement might be achieved on an operational meaning of white-collar crime. Thus, statements about the heinousness of white-collar crime most fundamentally represent tactics to call dramatic attention to forms of behavior that the writers believe (but cannot really demonstrate) have serious consequences for important aspects of social life, as, indeed, they may. (Geis & Meier 1977, page 26).*

Perhaps one of the most practical categorisations made was between *occupational* and *corporate crime*.

> *Occupational deviation includes all occupational behavior that violates the institutionalized expectations of an occupation, that is, deviant behavior that occurs in the course of occupational activity. It should be made explicit at all times, however, whether or not the behavior in question is criminal as well as a deviation from occupational norms. (Quinney 1977, page 287)*

Conklin (1977, page 13) uses the term *business crime* to refer to criminal acts in the business world. Whilst Ermann & Lundman (1982) identify 4 types of corporate deviance, clearly avoiding the use of crime and therefore being able to address a wider range of activities that may be harmful to society:

1. Deviance against owners
2. Deviance against employers
3. Deviance against customers
4. Deviance against the public-at-large

Indeed it may be argued that the distrust that such acts can cause is greater than any financial loss. On this point Sutherland wrote:

> *The financial loss from white-collar crime, great as it is, is less important than the damage to social relations. White-collar crimes violate trust and therefore create distrust, which lowers social morale and produces social disorganization on a large scale. (Sutherland 1940, page 5)*

The question of harm is an interesting one. Friedrichs (1992) poses the following conundrum:

> *A critical or realivistic conception of white collar crime stresses consequences over abuse of trust. A museum which exhibits a fake Van Gogh and misrepresents it as authentic is committing a deception with no real identifiable harmful consequences. A tobacco company which sells cigarettes labeled as harmful to one's health is not engaging in deception, but very real harmful consequences are involved. Which of these cases is more convincingly categorized as white collar crime? (Friedrichs 1992, page 12).*

It is clear then from the vagueness of the term *white collar crime* that it is necessary for a thesis dealing with this topic to offer its own definition to clarify the sub-section that its focus is intended to cover; Sutherland's being largely an omnibus definition. As has been partially seen from above, many have sort to analyse only those deviants in power, or at the top of their organisations, referring to such as "*elite deviants*"[24]. Others have sort to include all crimes and indiscretions in the economic environment as White Collar Crime; a broader category than even Sutherland's far from comprehensive original.

For the purposes of this chapter therefore it is necessary to offer a number of definitions. *White collar crime* is taken as including all actions taken by officers of organisations that can be construed as criminal. From a psychological standpoint it is also useful to include deviant behaviour which is prejudicial to the company, or its associates, whilst not being necessarily illegal[25]. It is not the purpose of this chapter to discuss the difference between purely illegal and purely immoral action or indeed to discuss the reasons why

[24] Simon and Eitzen (1990)

[25] Some cases lead to civil proceedings. There have been calls in Britain for such to be used in the future for the handling of cases involving the breach of Securities regulations etc.. On this point Fildes commented: "*The case would be decided on the balance of probabilities, not, as in the criminal courts, by imposing the burden of proof* " (The Daily Telegraph, July 20, 1992). Another point that must be made here is that what may be illegal in one country may be legal in another similar country.

immorality and illegality are not always inextricably linked. In view of the fact that *business deviance* is such a broad category of criminal behaviour, committed by a variety of people, it is worth splitting this large group into a number of sub-groups.

> *On the matter of defining white collar crime one might say there are definitional theists, atheists, and agnostics. In this situation of 'conceptual anarchy' it has been said that white collar crime is whatever its students want it to be. (Friedrichs 1992, page 7).*

## three sub-groups.

Table 2.1 proposes that *business deviants*[26] may be separated into three distinct categories:

1. Endogenous business deviants;
2. Exoteric business deviants; and
3. Exogenous business deviants.

Table 2.1: Shows the parties involved in the three types of Business Deviance

| *Business Deviance:* | *Perpetrator:* | *Primary Beneficiary:* | *"Victim":* | *Example:* |
|---|---|---|---|---|
| **Endogenous** | **Insider or employee** | **Insider or employee** | **Employer Corporation** | Cashier steals from till; pilfering; *input fraud* for personal gain |
| **Exoteric** | **Insider or employee** | **Employer Corporation** | **Third Party** | Misrepresentation to clients; dumping of untreated waste; failure to comply with safety standards; Maxwell; Leeson? |
| **Exogenous** | **"Outsider"** | **"Outsider"** | **Corporation** | *Cracking* and computer fraud; *phantom* corporations; *advance fee & outside fraud* |

[26]The terms *deviant* and *deviance* are preferred to *criminals* and *crime* so as to include activities which incur civil sanctions or that breach non-criminal regulations. A crime requires a law, an act and a criminal sanction, by considering the wider case of deviancy we are able to consider all those acts that may be considered as anti-social and negligent, as well as those acts that have been prosecuted as crimes.

Three points must be made about the terms above. Firstly the victim may not be aware that they have been disadvantaged or, in the case of insider dealing, be hard to identify. This does not mean that they are not victims.

Secondly, the term "*Primary Beneficiary*" has been used as the Insider or employee may also benefit indirectly from the perpetration of *exoteric business deviance* through the improvement of status, performance related pay or other remunerative aspects associated with their job. The direct benefit from the corporate crime is received by the corporation though. The term "*Corporation*" must also be explained, it is taken here to mean a legitimately incorporated enterprise which operates within the parameters of normal commercial activity as distinct from enterprises which are formed with the purpose of defrauding a third party.[27]

The third point to be made concerns the term "*Outsider*". Outsiders may under certain circumstances be employees of the victim corporation. For these employees to be outsiders though, they must no longer identify with the norms of their colleagues, or identify with norms that would be considered deviant by other members of the corporation.

The three main sections of the thesis will look at each of these areas in turn. The chapters on *exoteric business deviance* will consider the issue of *elite deviance* and *white collar crime* and .why it is hard to prosecute such offenders under the current system. The chapters on *computer-related crime* will consider the problem of *exogenous business deviance* and the threat that *outsiders* might pose to corporations as they seek to benefit from the growing power of the computer.

The chapters concerned with crime and bank employees will be used to highlight the factors associated with *endogenous business deviance*. These chapters will consider the factors that motivate an employee to commit

[27]Such frauds have been termed *Long-Firm Frauds* (Levi 1987).

crimes against their employers and what factors prevent them behaving in a deviant manner.

The approach adopted is justified as it is very hard to research the issue of Crime and Management as there is a paucity of data on the subject, other than for mega-frauds that have led to high-profile court cases, and a reluctance to discuss the issue of *computer fraud* because of the embarrassment factor.

The first two categories, *endogenous* and *exoteric*, are made up of company employees. For an *endogenous business deviance* to be committed an offence must be perpetrated against the company by an employee. Embezzlement by the company's chief cashier may be considered as an *endogenous business deviance*. An *exoteric business deviance* is committed by an employee against a third party on behalf of the company. The employee does not benefit directly, although may gain much kudos if successful. The examples of such crimes have made the front pages of newspapers worldwide. They include insurance frauds (Equity Funding Corp. [U.S.A.], Barlow Clowes [U.K.], etc.), pension frauds (Maxwell [U.K.]), tax frauds (Nissan UK [U.K.]), stock market violations (Guinness P.L.C. and Bluearrow [UK], Boesky and Milken [USA], Equitycorp [New Zealand]), the marketing or sale of unsafe products (Ford Pinto [USA]), financial mismanagement (Barings (UK), Orange County (USA)), etc.; the list[28] is long. When a company commits a crime of this nature it requires the collaboration, whether willingly and/or knowingly or not, of its employees. A company may be a legal entity but it has no autonomous physical persona[29].

---

[28]Not all of the above cases resulted in a criminal prosecution so it is arguable that they are not all crimes. From a management view point this is a somewhat spurious conjecture - the fact that cases were made at all is bad enough and in nearly all cases a financial loss was made or lives put at risk.

[29] Many companies have a highly visible public image. They have large buildings or equipment but it is the actions of the individuals they employ that manipulate such for the *good* of the company.

There is a grey area where one employee acts on behalf of the company to the detriment of another employee; avoidance of expensive safety equipment leading to the injury of the other employee for instance. Such a *crime*[30] would be an *exoteric business deviance* by definition. It would not be an endogenous one as the it was not directed at the company, but is perpetrated on the company's *behalf*.

An *exogenous business related criminal* is not employed by the victim company. They commit the crime without any substantial aid or assistance from an employee of the company. If the outsider is acting as an employee of a second company then the crime is not exogenous but exoteric. It is not intended that the *exogenous business related criminal* be offered any differentiated treatment from that offered to a common thief; it is not the purpose of this chapter to advocate special treatment for all crimes which can be categorised as *Business Related*. Some are nothing more than premeditated thefts and should be treated as such, also just because an outsider commits a crime within an economic or business environment does not make it a *business deviance*, armed robbery for instance, is not a *business deviance*. But many *business deviants* are motivated in a way unlike other criminals due to the nature of the environment in which they may spend over half their waking hours. Surely the impact of this environment on the individual should be considered? The key to this chapter is in an understanding of the motivation of the *business related criminal*.

## motivation.

Motivation has perplexed management theorists for the last century-and-a-half. Their theories have offered many estimations and models of the system by which individuals are motivated. Maslow's hierarchy; Herzberg's motivators and hygiene factors; Hunt's six needs (Hunt 1986); MacGregor's X and Y theories (MacGregor 1960); the Rational Economic Man

[30] Not all such actions are criminal! It is an interesting area where morality and ethics meet good business practice and economics.

(Handy 1985); Porter and Lawlers' Motivation Calculus (Porter & Lawler 1968); etc..

In general motivation is about the satisfaction of needs. We are motivated into action when we perceive that an action will lead to an outcome which may be used to meet a need. This implies a rational approach to all actions, which is not always the case, as some are quite clearly reflex actions[31]. Many theorists have concentrated on the categories of needs that require satisfaction. Maslow (1943) argues that as one need is satisfied it ceases to motivate, as the individual puts priority on the next one. His initial hierarchy consisted of: physiological needs; safety needs; love needs; esteem needs; and self-actualization needs. He recognised that this hierarchy was in no way rigid (although many text books insist on crystallising it within a pyramid) and that it would change from age group to age group, country to country etc. He also recognised that some highly irrational behaviour could be explained by the need "*to know and to understand*" which covered "*curiosity, exploration, desire for the facts, [and] desire to know*" (Maslow 1943 page 34). This would obviously explain the irrational behaviour of those that climb Everest or trek to the North or South Poles, or indeed the behaviour of students who forego a salary to obtain degrees.

On the point of the prioritization of needs, Hunt (1986) suggests that the priorities are affected by the age, cultural background and role of the individual. Chapter Two of his book shows this graphically by comparing the need profiles of some 674 European managers. The six needs that they recognises as most important are: *comfort; structure; relationship; recognition; power*, and *autonomy*. The survey showed that the "thirty-somethings" placed more importance on power and autonomy whilst the importance of this need drops drastically for the 38-43 year olds who see comfort, structure and relationships as more important. This profile resorts again to one similar to the 30 year olds for those managers in their mid-forties

[31]Although even here it is possible to argue that the reflex is in response to a safety need.

to mid fifties. The differences are also quite predictably apparent between the profiles of European and Japanese managers.

Katz (1978) supports the view that the efficacy of the motivational aspects of a job, such as job design, may well be dependent on the career stage and position of the employee concerned. His studies show that the length of time spent in one position or job can have a very significant impact on the motivation level of an individual. The recognition that many things influence an individual's actions is very important when you consider the case of the crimogenic organisation. This will be discussed in more detail later in this chapter.

Of particular relevance to the question of fraud is the issue of dissatisfaction. Ross and Zander (1957) found that:

> *"workers whose personal needs are satisfied on the job are more likely to remain in the organisation. While we are unable to evaluate the comparative importance of earnings as a substitute for direct need satisfaction, the satisfaction of needs has values which are worth developing for the establishment of stable work groups." (Ross and Zander 1957 page 71).*

Ross and Zander were more concerned with the propensity of the individual to resign when their needs are not satisfied at work. It is quite clear that there are other courses of action available to the disgruntled employee. Unions can organise strikes and industrial action where the majority of their members feel that they are poorly treated. This may be where they feel that they are being poorly remunerated for their productivity or for the risk associated with their job. In many cases it can be as a result of an "insufficient" pay rise; so when pay is decreased the effects can be quite explosive (Greenburg 1990).

## alienation

One of the most interesting theories, and particularly relevant for the topic under discussion, is Fishbein's (1980) theory regarding intention. Fishbein surmises that intention is the product of the relationship between an individual's attitude toward a behaviour and their perception of the norms

under which they operate. If an individual believes that a certain form of behaviour will yield a certain desirable outcome they will have a positive *attitude toward [that] behaviour*. They may not intend to act in that way as they perceive that others will not view such as acceptable. This perception of social pressure and norms of acceptable behaviour is what Fishbein terms an individual's *subjective norm*. The individual must weigh up the importance of the behaviour for the satisfaction of a need against the importance that they perceive of conforming with their subjective norm. An individual will consider the *relative importance* of both factors, they will have the intention to behave in a certain way if they rank their attitudinal considerations as greater than the normative ones. Alternatively they may behave in accordance with their normative considerations.

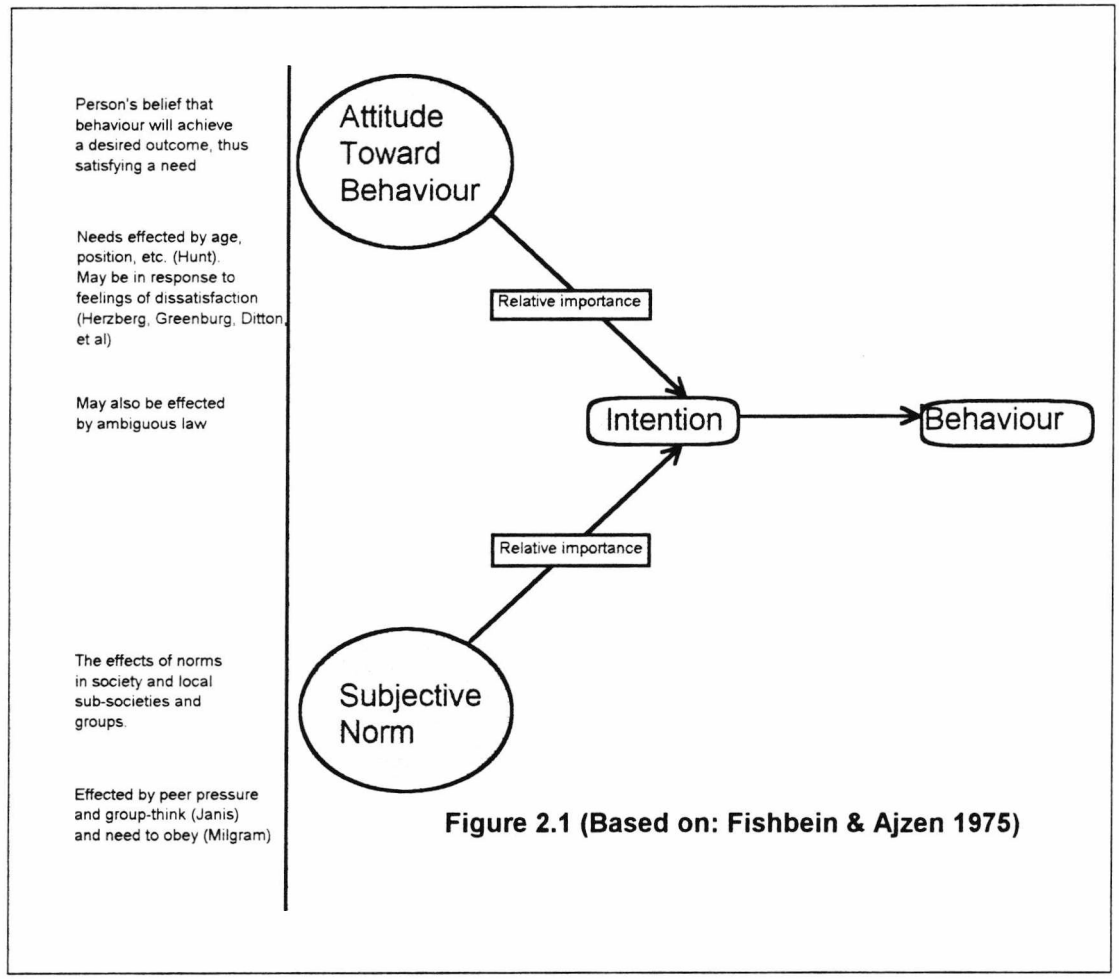



**Figure 2.1 (Based on: Fishbein & Ajzen 1975)**

Fishbein's model may be portrayed as in *Figure 2.1* although it is useful to condense this model to a simple equation:

$$I = \chi A + (1 - \chi)n$$

*where* $A$ = *Attitude toward behaviour;*
$I$ = *Intention;*
$n$ = *Subjective norm; and*
$\chi$ = *Relative importance (between 0 and 1).*

An individual may act in a way that they have a negative attitude toward if they perceive the normative pressure to be great. The feeling of duty can be strong and it is this that gets many up from their beds each morning and into work on time, although for some it may be the fear of punishment or dismissal.

## attitude toward behaviour.

An individual will act in a certain way if they perceive that the action will lead to a desired outcome. Most motivation models suggest that individuals will favour courses of action that satisfy their needs. Hunt (1986) identifies the six most common needs of managers in Europe[32], and suggests that the relative strength of each need is dependent on the life stage, position and cultural background of the manager. It therefore follows that an individual's attitude to certain behaviour will also be affected by such factors.

Herzberg (1968) identified a number of motivators within the workplace but also offered a list of what he termed *hygiene factors*. A hygiene factor is an aspect of the working environment or the job that is likely to dissatisfy the employee if inadequate but does not have the power to motivate the employee if it is satisfactory. Greenburg's (1990) findings suggest that it is the dissatisfied employees who are more likely to commit a crime against their employer. If this is so then Herzberg's hygiene factors are of particular relevance to managers who wish to curtail the criminal inclinations of their employees. The five most stated factors in Herzberg's study were *Company policy and administration; Supervision; Relationship with supervisor; Work conditions;* and *Salary*. Greenburg's study focused on wages as an area of

[32]Comfort; Structure; Relationships; Recognition; Power; and Autonomy.

dissatisfaction for the employee and the findings seem to suggested that most of the effects of a wage decrease may be mitigated by good communication by management as to why the decrease was necessary.

Greenburg (1990) showed that it is not so much the level of pay *per se* that is the crucial factor in determining whether an employee will steal to redress an inequity. Greenburg's study showed that when pay decreases, theft by employees increases, but that this increase is not as large when the management explains the reason for the decrease to the employees. It is possible to contend that money in itself is not the primary motive for theft, and that this status should be awarded to a feeling of inequity.

### money

That is not to say that money is never a motive for financial fraud in general. It is clear that money may be the motive for a large number of financial frauds but that in the majority it is a derived need. The money is stolen to pay debts or to relieve other financial pressures. In the survey by Ditton (1977) the thefts and frauds were committed to ensure a stable salary for workers who had any shortfalls in their books deducted from their salary. The frauds were committed to ensure that there was no shortfall. Breed (1979) found that 85 per cent (74 out of 87) of the non-sex crime offenders that featured in his study had been experiencing financial difficulties.

Two lessons may be drawn from the above. Firstly that communication can reduce the level of dissatisfaction of the employees, and secondly that if managers took more interest in their employees they might be able to identify those individuals with a higher propensity to steal because of external pressures on their finances. For example, for many years the banks insisted that their employees had their personal accounts with them. The office manager would receive a list of all staff accounts that were overdrawn and the member of staff would be spoken to to ascertain the reasons for the discrepancy. This practice was undermined by the Financial Services Act

1986. Whilst other institutions cannot be quite so systematic in their checking of employees' finances managers can be alert to potential warning signs. For instance, the stress of separation can have financial as well as emotional consequences.

Another motive may be status. The individual may commit crime so as to cover up a mistake or to ensure that a plan succeeds. The success of a deal may mean more money for white collar criminals by way of promotion or better performance related pay. It is therefore important to ensure that a company's reward scheme does not distort the *risk/reward* or *impulse/inhibition* equation. Gellerman (1989) offers an example of what happened in a factory when a competitive bonus scheme was introduced. Supervisors were keen to ensure that their shifts obtained maximum bonuses and would take risks with regard to safety etc.

> *"These supervisors were not ordinarily reckless; they played this game of managerial chicken only because they had too much to lose by not playing." (Gellerman 1989 page 76).*

Ensuring an adequate and equitable remuneration scheme is very important in the prevention of internal fraud. Another useful measure would seem to be employee participation (Kelley 1991, Schein 1988). Kelley (1991) indicates that such participation can improve the relationship between managers and workers:

> *"Participatory action can result in management seeing the world from the perspective of workers. When managers are faced with decisions which may harm workers, it is harder to make such decisions in the context of having meaningful social contact with potential victims." (Kelley 1991 page 11).*

By humanising the victims the managers are less able to rationalise their potentially lethal actions or decisions. It is easier to risk the lives of those that you see as *less than human*, as merely part of the machinery. Where participation breaks down the "*Them and Us*" barrier and increases communication and social contact the propensity to commit crimes is lower[33].

[33] That is unless the management and staff conspire to break the law together.

Schein (1988) argues that *participative* management is essential if employees are to realise their full potential within a company. Companies should believe their employees are all *Theory Y*[34] people and if they do not:-

> *"they will end up treating employees as children, expecting them to behave in a dependent, submissive fashion more characteristic of childhood. Managers under those systems should not be surprised, then, if those same employees act like children - rebellious, emotional, and uninvolved in organisational goals." (Schein 1988 page 70).*

This would seem a reasonable approach to adopt to partially deter crime committed by employees.

In general each of the above aspects may affect the attitude that an individual has towards a certain activity. If they believe that they will be able to relieve the pressure on their finances without being caught, or that by acting a certain way they will be "*getting even*" then they may perceive the action as favourable. For example, an
individual may believe strongly that they will be able to pay their debts if they take £100 from the till, they also have a strong norm that encourages them to act in accordance with the belief that stealing is unacceptable. If we assume that for this individual that they have an absolute *A-score* of 1 and an absolutely negative *n-score* of -1 we can see that the individuals intention will be dependent on how important they perceive their attitude toward the behaviour and the norm:

$$I = \chi A + (1 - \chi)n$$

$$I = \chi(1) + (1 - \chi)(-1)$$

$$I = \chi - (1 - \chi)$$

*where* *A = Attitude toward behaviour;*
*I = Intention;*
*n = Subjective norm; and*
*$\chi$ = Relative importance (between 0 and 1).*

---

[34] MacGregor (1957)

If $\chi$ is greater than 0.5 then the intention will be positive. If $\chi$ is less than or equal to 0.5 then in the above example the individual would have no intention to take the £100 from the till, because they consider their subjective norm as more important than their attitude toward the behaviour, "*what would people think?*", "*No, no I couldn't!*"

Of course to argue that taking £100 from the till of the company you work for is any less criminal than taking a car radio worth £100 is ludicrous. It is not the intention of this chapter to argue that such individuals deserve any special treatment from the law. Having said that, were the company to create an environment where such behaviour was rife, and failed to take action to prevent or discourage such behaviour, they could be said to be at least partially responsible for any resultant crimes. Most of the factors that affect an individual's attitude will lead towards the committing of an endogenous crime. The effects that an employing organisation may have on an individual's subjective norms are more likely to lead to the committing of an exoteric crime.

## subjective norms.

An employee of a company is usually expected to satisfy certain conditions of employment. Some are clearly laid out in their terms of contract, others are more vague and require the conformity to a company culture. An individual's norm will be made up from the impact of such pressures as well as their pre-learned norms. As the average employee can expect to spend in the order of 30 to 40 years within such an environment they cannot fail to be influenced by norms prevalent therein. There are a number of major factors that influence the actions of an individual. It is the proposition of this chapter that some of these factors influence an individual to commit crimes by either effecting their subjective norm directly, or indirectly by reducing the importance of complying with that norm.

Under such circumstances an individual must be treated differentially than were they to behave in a similar way but independent of any outside influence. These influences are many but potentially the most important are the following three:

1. Obedience and the effect of Authority;
2. GroupThink and Peer Pressure; and
3. Ambiguous law.

Each of the above is likely to affect the way an individual behaves by effecting their subjective norms or the way that they perceive them.

## obedience and the effect of authority.

The idea of the crimogenic organisation is a strong one. This is especially so when the power and influence that authority and the group can have over the actions of an individual are considered. Perhaps one of the most startling studies of the power of authority was conducted by Stanley Milgram (1963). Milgram created a dummy experiment to assess the effects of pain on the ability to learn and employed volunteers to assist with this experiment. The volunteer was the subject under actual examination and was employed to administer an electrical shock to the dummy experiment's subjects. The voltage of the electrical shock was increased with each wrong answer. Of 40 subjects 26 increased the voltage up to the maximum of 450 volts even though the dial was marked such as to indicate that anything above 300 volts could be fatal; 450 volts was marked "*XXX*". All 40 subjects passed the levels marked "*Strong*" and "*Very Strong*".[35]

> *"Subjects were observed to sweat, tremble, stutter, bite their lips, groan, and dig their fingernails into their flesh. These were characteristic rather than exceptional responses to the experiment.*
>
> *"One sign of tension was the regular occurrence of nervous laughing fits. Fourteen of the 40 subjects showed definite signs of nervous laughter and smiling. The laughter seemed entirely out of place, even bizarre... Upon the command of the experimenter, each of the 40 subjects went beyond the expected break off point. No subject stopped prior to administering*

[35] When the experiment was re-conducted with the new subjects in a room on their own only 9 out of 40 reached the 450 volts mark.

*shock level 20. (At this level - 300 volts - the victim kicks on the wall and no longer provides answers to the teacher's multiple-choice questions.)" (Milgram 1963 page 375)*

The strength of the urge to obey is quite obviously strong, even when it conflicts with an individual's moral code. Authority plays a large part in the process. Individuals seem willing to trust that someone somewhere knows the "*full story*" and is in control. In the example above it is possible to conclude that the individuals acted as they did because they feared the consequences. Their subjective norm encouraged them to avoid inflicting pain whilst they had a positive attitude toward the behaviour as they wished to avoid the consequences of non-conformity.

## GroupThink and peer pressure.

The individual also feels the pressure to conform with group pressure; a pressure which is strongly evident in most organisations[36]. Solomon Asch (1956) in his experimental studies on conformity asked participants to chose between three lines the one which was closest in length to a fourth line. One of the three was quite clearly the right one. When the participants gave answers as part of a group who unanimously chose an incorrect one 32 per cent of the estimates conformed with the group decision. One third of the participants conformed with the group in half or more of the tests. Only a quarter of the participants were completely independent. If one member of the group agreed with the participant then only 10 per cent of the estimates conformed.

Janis (1972) noticed a number of characteristics of a phenomenon that he termed "*GroupThink*". *GroupThink* occurs when too much emphasis is placed on group harmony and where there is a general belief in the infallibility of the group's decision-making capability. The group as a result has a greater belief in the rightness of their decisions and are likely to reject anyone who doubts it. Two characteristics out of the eight that Janis identifies are particularly

[36] If this is an any doubt just consider the effectiveness of the manipulation of corporate cultures in an attempt to improve performance. For examples of corporations with strong cultures one may look not only to the Japanese but also Western corporations such as Coca Cola, Macdonalds and IBM.

crime. The first is Invulnerability, a feeling that can lead a group to make reckless decisions because there are no dissenting voices. There is a tendency for individuals when in the presence of their peers or superiors to avoid admitting ignorance about a topic; they are also less likely to voice their reservations about a subject if everyone is in apparent agreement. The tendency is to believe that someone is in control and knows exactly what is going on even if they themselves do not. They are willing to undertake the tasks that are set them as failure to do so would lead to possible dismissal or failure to gain a desired promotion.

The second relevant characteristic of *GroupThink* is *rationale*. The group is able to rationalise its actions either in attempt to justify the choices they have made or so as to aid their belief that they are conforming with the regulations and laws that govern them. This will help to reduce the relative importance of any norms that may conflict with the action undertaken by the individuals, jointly or severally.

What the three studies by Milgram, Asch and Janis highlight is the effects that corporate organisations and groups in general may have on the actions of an individual. Surely if we combine this with the added uncertainty that ambiguous law brings with it we must concede that the standard legal processes for corporate offences may be inappropriate.

## ambiguous law.

If individuals are unaware of the illegality of their actions or have reason to believe that they are complying with the law when they are not, should they not be treated with an element of compassion? The law in general says not. It argues that ignorance is no defence. That is all well and good when dealing with a burglary or such but what of those criminals who have transgressed laws relating to commerce? Such people often have more detail and law to consider. Hadden (1983) supports this view. He offers three significant differences between City frauds and other crimes. The first is the ambiguous

and unsettled nature of the law governing the activities of City institutions. The second is that the line between acceptable and unreasonable behaviour is far from clear and consequently might be breached in the course of an executive's or firm's ordinary activities. And thirdly that when the fraud is committed primarily by an institution that it is far from easy to establish that it had sufficient corporate *mens rea* to commit the offence. Is it fair under such circumstances to seek an individual to "*bear the blame*". Hadden thinks not:

> *"No single individual is expected to understand all the relevant issues, and those who are ultimately responsible for taking certain decisions are entitled to rely on the competence of others, for instance in the preparation of accounts and other disclosure documents." (Hadden 1983, page 503).*

They may indeed believe that the law does not apply to them, they are "*Masters of the Universe*"[37] who operate within the spirit of the law even if not the letter. It is not the contention of this chapter that such people should escape punishment for their wilful abuse of the law. Such people should be prosecuted as a signal to others.

## summary.

This chapter has offered a model of how an individual might be motivated in a corporate environment, summarised in Figure 2.1. It is a model that highlights how each individual experiences exceptional pressures from the environment. If we conclude that the environment is acceptable and necessary for the functioning of economic society then we must have some compassion for those that are influenced by it in a negative way. It is for this reason that this chapter has proposed a number of circumstances in which an offender deserves special treatment. In summary it is proposed that where an individual commits an *exoteric business deviance* and is unaware of the illegality of their action they deserve special treatment. Such treatment should assess whether they acted under the influence of their employer company

[37] Woolf (1987)

and in general accordance with the wishes of that company. Where they commit a *exoteric business deviance* whilst in doubt of their action's legality they also deserve the same treatment if it can be concluded that they were acting under the influence of their employer organisation, and not merely "*cutting corners*". Those who commit a crime against their employer organisation deserve no special treatment unless it can be proved that their action was influenced by the similar action of their peers or superiors, and that the individual believed that it was acceptable behaviour within the organisation. It is not intended that those outsiders who commit exogenous crimes be offered any of the special treatment advocated here for the other groups.

If it is conceded that the *organisational individual* faces exceptional circumstances then it must also be conceded that the law should recognise this. Much English law is based on the premise of the *reasonable man* (or indeed woman). What would a reasonable man do in such and such circumstance? But before such a judgement is made it is only fair to socialise him in the same way as the accused; the reasonable man must also be subjected to the norm distorting factors that the organisational individual faces in their daily life. This seems a logical conclusion to make. Of course it is only natural that those offended against should seek some justice. For many this process is not complete unless there is a conviction. It is for this reason that more should seek the prosecution of the employer company rather than the employee. Where it is felt that a conviction would be difficult to achieve, the offended party, or those that act upon their behalf, should pursue a civil claim, where there is not the need to prove the case beyond a reasonable doubt as in the criminal case.

If it is still deemed necessary to punish the offender then the law must recognise the punishment that the defender has already suffered. The period between the start of the investigation and the trial must be considered along

with the other losses that the individual and their family will suffer whilst in jail, the pressure on family finances etc.

The next section of this thesis will offer three studies which focus on the three types of category of *business deviance*.

There are a number of broad assumptions that may be made based on the above. Firstly that the major *computer-related crime* threat would seem to come from the employees of most organisations rather than from external sources. The majority of these crimes relate to the manipulation of input documentation. Secondly that the threat from external sources is real and system managers should take appropriate precautions to manage this risk. Thirdly that managers should not ignore the human factors within a system and that a securer system may be achieved if employers focus attention on the motivational aspects as well as the technical aspects.

# Chapter 3

## Golden Crumbs:

## Crimes by the Financial World's "Elite".

*"Out on the floor of the bond trading room, the money madness had reached its peak. As he headed towards his desk Sherman felt as if he were swimming through a delirium.*
*"... October ninety-twos at the buck..."*
*"... I said we strip the fuckers!"*
*"Ahhhhh, the golden crumbs... How pointless it seemed."" (Wolfe 1987 page 468)*

*There is a young fellow named Leeson,*
*Whose lifestyle sounds quite Dionysian;*
*Now he's taken a pull*
*on the horns of the Bull,*
*And discovered the Bear is in season.*
*(Quoted in The Times, 22 March 1995, page 25)*

### introduction

This chapter will examine the lessons learnable from a number of high profile fraud cases that have been extensively covered in the broadsheets in the UK. The lessons that will be highlighted will focus on the risk management aspects as well as considering how the motivation theory proposed may be applied to these cases.

In broad terms each of the crimes considered may be termed City crime. It is indubitably true that the crimes of the City's Elite are the most attractive of financial crimes to the media. These deviancies, and the activities of their committers' more successful counterparts, send interesting signals to other sectors of the financial and commercial community. It is for this reason, it will be argued, as well as for the breaches of trust involved, that insider dealing, fraudulent accounting, tax evasion and other crimes of the so called elite, should be prosecuted to the fullness of the law.

## city crime

There will always be fraud or crime at the margin, there will always be those people who are willing to pick-up some of the crumbs that do not belong to them. The cost of prosecuting such crime is prohibitive, but, as opportunities increase, so do the incidences of fraud and as a consequence so must regulation. People commit crime as the reward increases and changes the cost/benefit of such crime thus increasing the chances that an individual will be motivated to deviate. It is therefore of importance that the costs of such actions should increase to re-balance the scale, to increase the weight of inhibition.

Such re-balancing was imperative following the introduction of the "Enterprise" culture by the Conservative Governments of the 1980's. It is somewhat of a misnomer to term the ethos that they encouraged as "enterprising", as in most respects it was less about enterprise and innovation and more about money. It is perhaps for this reason that the City was the area in which the calls were heard loudest, their business has been about money for many centuries.

The changes that the 1980s and Big Bang (plus its forerunner Little Bang) heralded were more severe than can ever have been expected. Before the deregulation of the City the most important decisions were taken by an elite few at the top of each firm.

> *"This excessive familiarity, though it could be suffocating, had a strong practical benefit. People always knew who they were dealing with and they could therefore thrash out deals verbally without the contracts and legal documentation which tied up every transaction in the United States. The result was a system which though incestuous, gave the City a flexibility which has allowed more quick-witted members full rein to make considerable fortunes. And those who broke their word did so at their peril. The news spread so quickly that there was no one left with whom they could do business." (Hilton 1987, 23-24)*

Big Bang and the globalization of the financial markets led to a greater number of deals involving vast sums of money and requiring fast decisions, the speed of which could determine whether the firm made £millions of profit

on a deal, or suffered a loss. At the same time, and as a consequence of the globalization of financial markets, a huge investment was made in very sophisticated information technology. This meant that many of the former "lions" who had ruled the pride in the old City became increasingly out of touch. Many of the internal auditing systems were consequentially of little use, and the firms' new owners, the Clearing Banks and other overseas institutions, had little idea where to start - having very little knowledge of the businesses that they had acquired.

The increase in business brought its own special problems which complicated things further. More business meant more people; the firms' recruitment policies had to change so as to ensure full trading rooms. The new breed knew the basic rule of the game; Profit Maximization; but they knew little of the moral codes. The role models had also changed; the mean survived and the professionally greedy grew rich. The "Gecko's" and the real life Boeskys and Milkens were successful beyond the previous bounds of conceivability. They played fast and loose and so close to the margin that their eventual fall, in hindsight, was inevitable. But for a few golden years they were the "Merlins" of the financial world and many "young-bloods" were captivated by their spell.

> *"The game is up. We were living in a time of fast money. The press had already their epitaphs... "The Money Society"... "Feeling poor on $600,000 a year"... As the 1980's drew to a close, so the financial fever intensified in which the only score card that counted was the number in your bank account." (Wood 1988 page 1)*

The irony of the introduction of the "Enterprise" culture to the "City" culture was that, in its limited sphere the City culture was innovative and at times enterprising, if at other times it seemed highly conservative. The Enterprise culture was effective less in motivating the de-motivated and unemployed and more in sanitizing money. Lucre was not so filthy. The Conservatives avoided talking about the importance of money directly. Instead they championed wealth creation and targeted inflation (effectively negative wealth) as Public Enemy Number 1.

## insider dealers

Insider dealing is the illicit trading in stocks by an individual who is privy to information which if generally known would alter the price of that stock. This Unpublished Price-sensitive Information has been acquired because of the insider's position of trust, or because of the position of trust that another found themselves in. Is it not therefore immoral to abuse such a trust? According to the law it is illegal in this country[38], but many feel that it should not be an offence. For instance Manne (1966)[39] argues that insider dealing serves an important function in the market, improving the speed of information.

> *"Here we come to one of the most astounding facts in this whole astounding business: the only stock market participants who are likely to benefit from a rule preventing insider trading are the short-term speculators and traders, not the long-term investors who are regularly stated to be the objects of the S.E.C.'s solicitude.*
>
> *"The initial error of most commentators is the assumption that the persons who sold to insiders before disclosure of important news would not have sold at all if the insiders were not in the market. Obviously this is absurd; the average seller has no way in the world of knowing the identity of his buyer." (Manne 1966 page 114).*

It is possible to argue that insider dealing is a tort on one level and a crime on another. Firstly it is a breach of the fiduciary duty that exists in the relationship between the insider and the client concerned. They are rewarded sufficiently for their efforts and have "contracted" to deal with the information in utmost confidence. The breach of this duty of secrecy raises a civil claim. The victims in this context are the companies who employed the insider. When such corporations become the victims of crime it is less likely to lead to a rise in public concern than when crime is committed on a more individual basis.

The second way in which insider dealing may conceivably be considered a crime is from the viewpoint of the buyer/seller of the shares that the insider sells/buys. Such a view is complicated by the fact that in the sale/purchase of

---

[38]. This is not the case in all countries, even amongst those with a recognised stock exchange, the most notable being Germany.

[39] Manne (1966) "In Defense of Insider Trading" **Harvard Business Review** November-December pages 113-122.

shares, the original seller and the eventual buyer never actually meet, the bargain is in most cases conducted through a market-maker. It is not possible to identify the "victims", most are unaware that they are victims, of this type of crime, but using simple demand and supply theory it is possible to show the potential loss thus substantiating the existence of the victims.

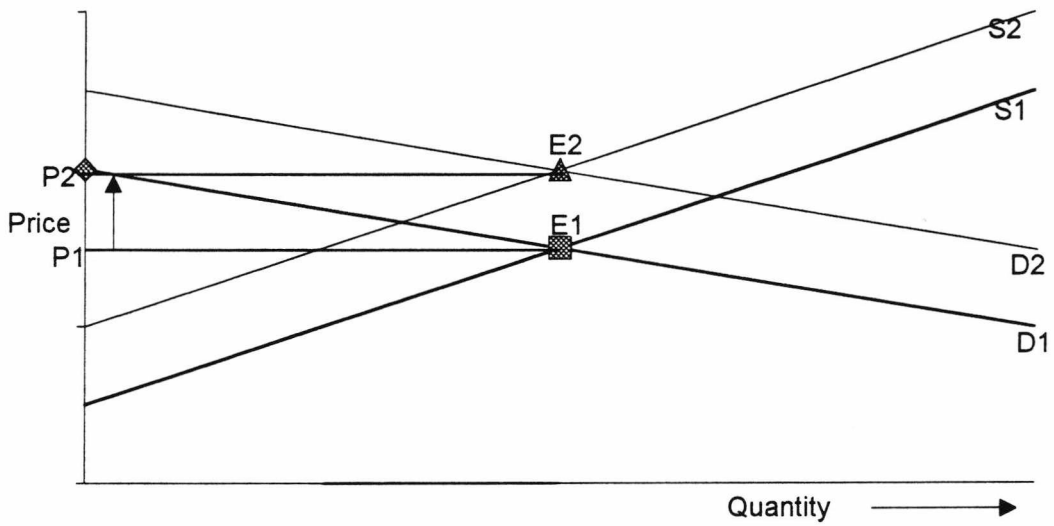



Figure 3.1:Shows the effect on the price as price sensitive information (PSI) becomes public knowledge.

In figure 3.1 D and S represent demand and supply for a company's shares prior to the announcement of a bid for the company, D1 and S1 show how the two are affected by the news. If an insider or "tippee" trades in the shares prior to the announcement, and assuming that their involvement is so small that it has no effect on the price, they will be buying shares of people who would not sell at that price if they were in receipt of the full information. The quantity of shares Q1 - Q in figure 3.2 are therefore owned by possible "victims". It is not possible to say who the victims are, but it is possible to say that there is a profit made by the insider at the expense of the sellers who would not have sold at the price they did were they in possession of the same information as the insider.

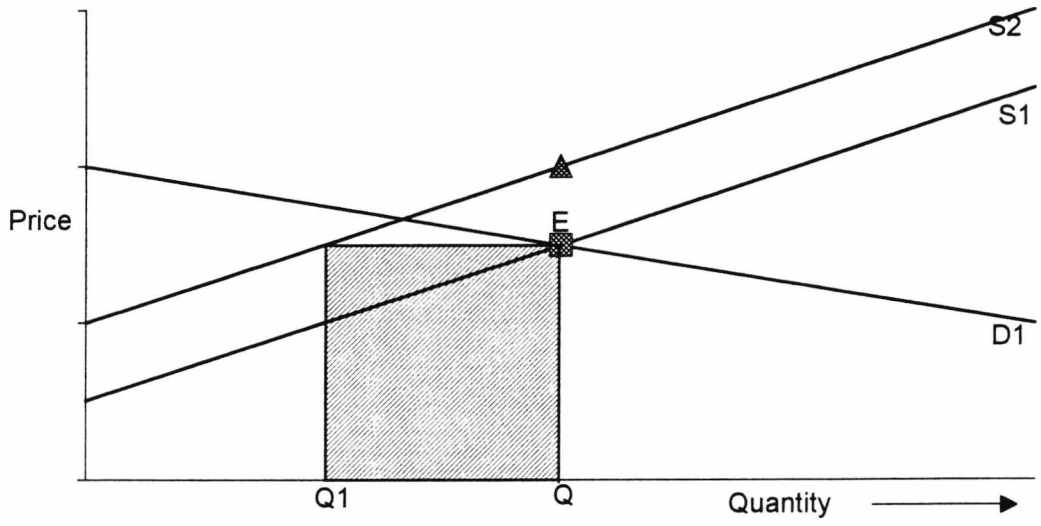



Figure 3.2: The shaded area shows the "victims" of Insider Traders. S1 shows the sellers curve before the PSI becomes public and S2 their curve after the announcement. The buyer is able to buy shares that would not have been sold if the PSI was common knowledge

At the other end of the calculation, the company that has employed the insider may have the advantage of a "dawn raid" eroded by the insiders dealings in the share. This becomes more apparent if the insider is large enough to influence the market leading to bid speculation. Bidders often have to pay a premium of as much as 15 per cent for their prey so they will be keen to keep their intentions secret. Speculation may raise buyers and sellers' expectations for the share thus pushing the price of the share up. Figure 3.1 shows how the price rises with the announcement of the bid from P1 to P2, as the PSI becomes public knowledge. Moyer (1970) states:

> *An acquiring firm normally pays a 15 per cent premium above the market price of the firm to be acquired in order to consummate a merger. Moyer (1970 page 22)*[40]

This means that there is a large potential profit to be gained by an insider. This profit is represented by the shaded area (E2,C,E1) in figure 3.3. The insider buys shares thus pushing up the demand curve and the price that they must pay for the shares. They will not be willing to push the price up to the bid price, but will stop short so that they make a profit on the shares that

[40]"Berle and Means Revisited: The Conglomerate Merger" Business and Society, Spring 1970.

they buy. They then sell these shares to the bidder company at the bid price, effectively the new equilibrium price.

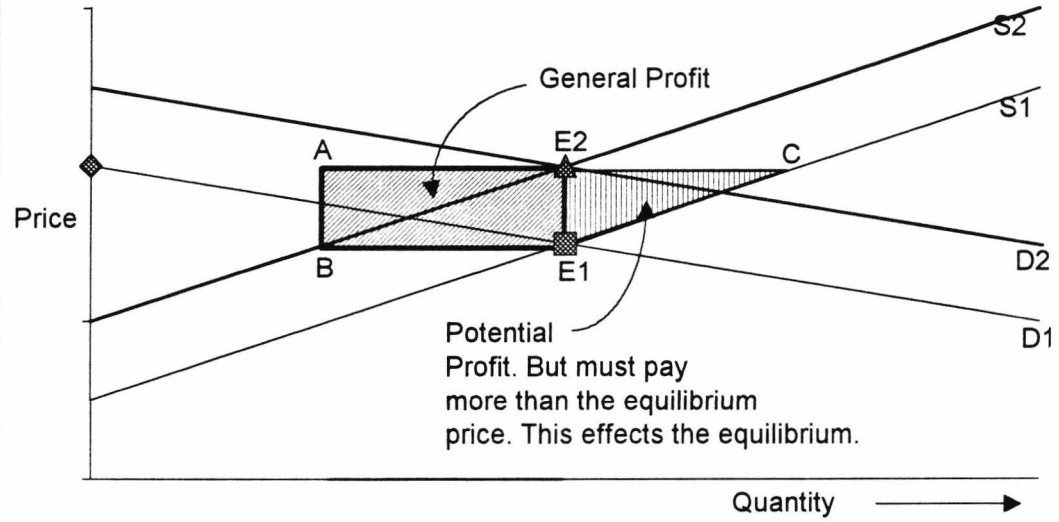



Figure 3.3:Those buyers who buy at E1 benefit from the General Profit (A,E2,E1,B) when thr equilibrium rises to E2. The "tippee" may benefit from this but will also be willing to pay more than the price at E1 and has a Potential Profit (E2,C,E1) if he does.

Manne (1966)[41] argues that this activity and consequent release of information is beneficial to stock markets. He argues that by a slow release of information rather than a sudden one there is less attraction to short term speculators. That may indeed be the case, but logic is sometimes too cold to pursue to its rational destiny. The fact is that on releasing the information the insider has breached his position of trust. We live in a society based on honesty and trust[42] and we should therefore be offered the protection of the law and the remedies it may offer for the occasions when the acceptable norm is deviated from.

## duty of secrecy

It is a well-established principle in banking law that a banker owes his or her clients a duty of care not to divulge information pertaining to that client's affairs. This duty is by no means an absolute duty and the precedential

[41] Ante.

[42] Bhide and Stevenson (1989) "Why Be Honest if Honesty Doesn't Pay" **Harvard Business Review** September-October pages 121-129.

Tournier[43] case lays out four qualifications. The case refers specifically to the operation of clients' accounts but as Atkin L.J.[44] suggests, obiter dictum, this duty should be extended:

> *"I further think that the obligation extends to information obtained from other sources than the customer's actual accounts, if the occasion upon which the information was obtained arose out of banking relations of the bank and its customers - for example, with a view to assisting the bank in conducting the customer's business..."*

If this line had been followed in the prosecution of Geoffrey Collyer[45] it would have been possible to claim, in a civil action, that his employing bank was liable for damages for breach of its duty of secrecy. In allowing the release of the information early they are quite clearly committing such an act, albeit vicariously. If an insider trades in shares which are subject to interest by a company by whom they are employed they should be prosecuted. No excuse should be permitted. If the individual feels that there might be a conflict between his professional duties and his personal financial affairs they should refuse the appointment. In accepting the contract of employment they are being paid to act in a position of confidence and trust. If he breaches this confidence he should be liable to both criminal prosecution and civil action. Profit should not be a necessary element, mere intention to make a profit should be sufficient. Law requires both mens rae and actus reim to be present, for insiders the mens rae should be assumed unless there is evidence to the contrary.

The economic argument above shows how the victims' loss may be identified. It is still not possible to identify the victims themselves but if the loss is identified it is possible to argue about the existence of a victim. There is of course the bidder company which has experienced a breach of confidence and an erosion of potential impact of a dawn raid.

---

[43] **Tournier** v **National Provincial and Union** [1924] 1.K.B. 461.
[44] **Tournier**.
[45] Geoffrey Collyer was convicted for Insider Dealing.

## signal function.

There is also a strong psychological reason why the law concerning insider dealing should be upheld to the fullest and that is to do with the signals that it sends to the other members of the financial community. Were this crime to go unpunished it would serve as a sign that "crime does pay" and would thus increase peoples' propensity to deviate from the social norm. The weight of inhibition would be insufficient for many who would not normally commit crimes.

> *"And Sherman McCoy, he who had now vowed to be his animal self, discovered what many had discovered before him. In well-reared girls and boys, guilt and the instinct to obey the rules are reflexes, ineradicable ghosts in the machine." (Wolfe 1987 page 713)*

The instinct to obey rules is very strong for many and indeed most people, but when the rules are unclear this urge can be stifled by the uncertainty. People are therefore in a position to say that the rule does not apply to them and that they are acting in the spirit of the law even if they deviate from the letter of the law. It must be clear that if you break this law in anyway you will be punished.

## information technology in the city.

The days of the open cry in the City are all but over. The vast majority of trading is conducted now by computers. The information that is available on demand and movements in supply of shares is therefore very impressive compared to ten or fifteen years ago. Consequently the market price for many shares is highly sensitive. This means that an insider is more likely now to affect the price of a share if they trade in it. This "muddies the water" for the insider dealing as a crime argument and supports to some extent the Manne (1966) argument that it is of benefit to the market.

If the share's price is highly sensitive, the insider will be releasing information into the market, thus arguably improving the information efficiency of the market, but at the cost of breaching his duty of secrecy to his client.

The importance of punishment will be considered later in this chapter. The remainder of this chapter is dedicated to an analysis of the Blue Arrow Affair which involved a reputed conspiracy to mislead the market by members of County Nat West and U.B.S. Phillips and Drew.

> *"People of the same trade seldom meet together but the conversation ends in a conspiracy against the public, or in some diversion to raise prices." (Adam Smith, The Wealth of Nations)*

## the blue arrow scandal.[46]

The Blue Arrow Case involved a charge of "conspiracy to mislead" the markets into believing that a rights issue had been successful. On September 28th 1987 it became apparent that the £837 million ($1.4 billion) rights issue by Blue Arrow had been far from successful. Shareholders had taken up only 38 per cent of the shares on offer. County NatWest had arranged the issue and had underwritten 25 per cent of the deal themselves so were obliged to purchase 25 per cent of the 62 per cent of the unsold shares. Had County decided to sell the unsold shares to the other underwriters they would have had to admit the failure of the deal and the share's price would have undoubtably fallen as the underwriters off-loaded their shares on the market. They decided on a different course of action.

County NatWest, UBS Phillips and Drew (Blue Arrow's stockbrokers) and Dillon Read (Blue Arrow's American advisors) bought another eleven per cent of the shares and set about placing the remaining 51 per cent with their clients. On September 29th 1987 County and Phillips and Drew were able to announce the success of the deal.

---

[46] Compiled from a number of articles that appeared in **The Economist**: "If it please yer 'onour" page 118, October 1 1988; "With a little help from NatWest's friends" page 79-80 January 7 1989; "Anatomy of a cover-up" page 84-86 January 28 1989; "The Blue Arrow Affair. The buck stops where?" page 23-26 March 7 1992. As well as a number of headline articles in **The Financial Times** on February 12, 15/16 and 18 1992.

Monday October 19th 1987 has gone down in British history as Black Monday. Its stockmarket crash halved the value of Blue Arrow shares. As a result County was unable to sell the 9.5 per cent of Blue Arrow shares that they still held. They had not declared this holding as required by the Companies Act 1985 as they argued that only 4.9 per cent was potentially declarable. Declaration is only required of holdings greater than five per cent [47]. The other 4.6 per cent they argued was held by their market making arm and was as such exempt under section 209 of the Act. County accepted control of the whole holding in December 1987 and declared the extent of its involvement in Blue Arrow shares. Their announcement was made just prior to their annual audit.

What was not admitted in December was the fact that County had given UBS, Phillips and Drew's Swiss parent company, an indemnity covering any losses incurred as a result of their holding 4 per cent of Blue Arrow shares. County had therefore had an interest in 13.5 per cent of the shares up until December 17th when County and UBS struck a deal to cancel the indemnity. A deal that cost County £32 million but allowed them to make an honest announcement of only a 9.5 per cent involvement. By the time this saga had run its course many influential people had been involved. The cast of players included individuals from the higher echelons of all the major companies involved, as well as the Bank of England. On the Bank's involvement The Economist stated:

> *"Virtually from the start, the Bank had all the information to conclude that County was misleading the market after Blue Arrow's 1987 rights issue. Yet it did nothing. Worse, it aided a cover-up of the affair, and attempted to head off an investigation by the Department of Trade and Industry (DTI)" (The Economist March 7 1992 page 20)*

On September 30th 1987 David Carse a supervisor at the Bank of England was visited by three officers of County who explained what they had done. Having been assured that they had sought legal advice on the question of

---

[47] Now three per cent.

declaration, Carse, according to a note on the meeting by County, offered his congratulation on "the overall success of the deal to date".

On the 14th February 1992 the court found four of the defendants guilty[48]. The case had taken over a year to try and represented the most costly trial in English Legal history, costing some £35 million. The judge gave messrs Cohen, Reed and Wells, all formerly of County Nat West, and Gibbs, formerly of U.B.S. Phillips and Drew, suspended sentences. In view of the cost and time taken to prosecute this case the sentences are surprising. Even now it is still unclear which laws were broken in the weeks after the 28th September 1987. As Hadden points out, the law can be highly ambiguous and is subject to interpretation. But if a court can spend over a year in deciding whether an individual broke such a law, how then can said same individual be expected to decide the legality of their actions in a matter of days or weeks? And should the individual seek legal advice on the matter how much reliance may they place on such advice?

What had the defendents done wrong? Who had suffered as a result of their actions? Had they acted in any way that was inconsistent with their roles (individually or jointly) or indeed with the then new ethos of the post-Big Bang [49] City? The defendants were obliged to act such that their clients were successful. Their obligation stopped at breaking the law. The law does not unfortunately offer a fixed line the crossing of which constitutes crime or unacceptable behaviour. Who was there to turn to for clarification on the evening of September 27th 1987? And if they believed that the deal was a good one for Blue Arrow just prior to the rights issue why should they have believed otherwise just because of a poor take up of their rights by the shareholders? If this is so, did they not act properly in advising their clients to buy Blue Arrow shares? Where they had acted improperly was in not

[48] Quashed in July 1992 by the Court of Appeal on the grounds that "the last-minute decision of the judge, Mr Justice McKinnon, to cut the indictment down to one central issue had been made too late for any convictions to be safe, Lord Justice Mann said." The Financial Times July 29, 1992.

[49] The term given to the process of deregulation in the City of London which occurred in October 1986.

declaring an interest in 13.5 per cent of the shares. But here the law is again unclear as to whether in view of how they held the shares they were obliged to declare. County's solicitors had confirmed in a letter the legality of the UBS idemnity (although this has been since contested) and since section 209 of the Companies Act allows market makers to hold shares without declaration for trading purposes[50] were County's actions not within the letter of the law if not necessarily the spirit? It is also important that not too rigorous an application of the law be applied in areas of innovation, although it is clear that this case does not fall into this category.

It is clear from the failure of the Serious Fraud Office to acquire a safe prosecution of the defendents that a new approach to such cases is required. Had they been able to bring a case against the corporate institutions involved they may have been able to prove as a whole that they had been responsible for a conspiracy to mislead the market. To make the same claim against one individual, or a small group, seems fraught with difficulties, especially if the individuals had been in consultation with their seniors and they with the organisation's legal counsel. It is with hindsight that many have suggested that a favourable civil judgement would have been much easier to secure; such a case would have been feasible against the corporations involved. Penalising them in monetary terms is an effective punishment as it effects their annual results and their all important Price/Earnings ratio. Alternatively, County could have been barred from handling rights issues for a set period, a punishment similar to that meted out by professional bodies whose members transgress laws or regulations.

## prosecution of white collar criminals

Whilst it can be argued that white collar criminals deserve special consideration it must also be conceded that prosecution is very important when an important law is transgressed. The reason that this is so is that it acts as a "signal" of what is acceptable and unacceptable behaviour. If the

[50] Whether 4.6 per cent of the shares of a company the size of Blue Arrow can be construed as consistent with a reasonable level for trading purposes is highly debatable.

legal forces allow indiscretions to go unchecked the law will soon become obsolete in the minds of those whose actions it is supposed to regulate. The higher the profile of the transgression the more important that "justice is seen to be done".

We learn what is acceptable from "corrected bad example" as well as from good example. It may even become part of the "significant other" which directs our actions. It may become part of our morality and affect our intentions through our subjective norms. Such pragmatic morality is of course nothing new, it is the way that society has inducted its members since it began. But is it necessary to jail such non-violent criminals? To prosecute them to the fullness of the law? It is possible to argue a strong case for a response in the negative to this question. The reason for such a response has a lot to do with the complicated nature of such cases. White collar criminals nearly always lose their employment and in the case of professionals will also be disqualified or disbarred from practising. They often have to wait a long time before facing the trial and in many cases they will not be charged until after a long investigation.

## the importance of prosecution

Whilst it is important to recognise the effect that the investigation and subsequent trial have on the white collar criminal it is also important to remember how it relates to the society in general. It is necessary to prosecute such offences as they represent signals to other members of the society. This signal factor supplies information to the society at large; it helps clarify any ambiguity in the law; it reinforces what is considered acceptable behaviour; it ensures that justice is seen to be done. But how should such offences be punished?

Whilst it is recognised that the prosecution of white collar criminals is important it is felt that a certain amount of lenience should be allowed for

"non-harmful" offences[51]. In many cases for first time offenders the whole process can be financially and physically draining. In the case of Roger Seelig, a defendant in the second Guinness trial, the pressure was too much and Mr Justice Henry dismissed the jury after a four-and-a-half month trial, under the advice of two psychiatrists, on 11 February 1992. Mr Seelig was a salaried executive of Morgan Grenfell, the merchant bank, and was not in a position to finance his legal defence. He therefore conducted it himself. In an interview he highlighted his reasons for this:

> *"The expenses are quite, quite beyond any salaried employee, however successful, can possibly sustain in trials that go on for a year or more. To have been represented by a full legal team over the past two-and-a-half or more years would have cost perhaps £3m.*
>
> *"My highest salary at Morgans was only £110,000 before tax, though admittedly there were bonuses. The legal aid regulations are not devised for working professionals. They look at your gross assets without taking into account your gross debts." (Roger Seelig, Financial Times, February 12 1992).*

Mr Justice Henry described Seelig as:

> *"a man at the end of his health, bewildered at his loss of control and his inability to think straight, wondering whether his medication rather than his mental state is to blame, recognising that he seems to have gone funny yet insisting that he was all right and could go on." (Comments made to the jury on their dismissal by Mr Justice Henry. Quoted in Financial Times February 12 1992).*

The Guinness and Blue Arrow trials are perhaps extreme examples to quote in support of the theory that the pressure of the whole legal process should be used to mitigate any sentence. They nevertheless give examples of how the process affects the accused. Breed (1979) studied a much more ordinary sample of white collar offenders[52]. On the matter of punishment he writes:

> *"Prison interferes with the life of any man or woman, but what is interesting when considering white collar offenders is, firstly, that they are in a minority, and secondly, it seems obvious prison affects their way of life more than any other section of the prison population. They have more to lose. They often have neighbours who never thought they would live next to somebody who was actually in prison. They have jobs which often entail trust and*

---

[51] This category includes offences where no physical harm has been done or where the offender was not guilty of premeditated or systematic theft.

[52] On this **Breed** wrote "If there is such a thing as a "typical white collar offender", he is either a self employed man who had a small business or a clerical worker who had a middle-of-the-line job. What he is not, generally, is a high-powered executive or professional man..." (1979 page 35)

*confidence, and prison means that they lose their jobs. They have mortgages, they have cars, often on hire purchase, sometimes even school fees, commitments which still have to be met." (Breed 1979 page 26)*

For many the punishment is in the process. Prison is unnecessary and in many cases represents an unfair addition to what they have already suffered. In the cases of the Blue Arrow and Guinness defendents we have examples of cases which took many years to reach a trial, for white collar crimes this is not exceptional:

*"[The investigation] took two and three quarter years. Long after the money had been paid and the crime no longer seemed significant , Sinclair Martin was arrested... as the judge sentenced him to a term of two years... the main feeling was one of relief." (Breed 1979 page 28).*

Martin was a solicitor who had used £50,000 of clients' money for his own purposes and had repaid the money before the investigation had begun. He would have been, in addition to any punitive action that the law might have deemed necessary, struck from the Law Society's register. A plumber who robs a house is not subject to the same sanction. During the investigation the defendants often lose their jobs and suffer from stigmatism from their former friends. They suffer financial hardship and experience great stress on their family life in general. Employment is hard to get unless they lie about their past, or their present predicament.

On a much grander scale was the Barings Crisis. Whether Barings' downfall was as a result of fraud or not is still in doubt and may remain so; what is clear is that they had the opportunity to reduce an "inherent industry risk" (Huntington 1992) and failed to do so. Such cost saving was initially profitable but ultimately contributed to the downfall of one of Britain's former greats - once referred to as the Sixth Great Power.

Whether Leeson committed a crime is as yet unknown. It is not the purpose of this chapter to judge this. What may be said without apparent contradiction is that the losses associated with one trader led to the financial collapse of a

bank that had stood for 233 years with an almost exemplary record, 1890's rescue by the Bank of England apart.

**The Independent 28 February 1995 - *"The breaking of the bank at Bishopgate"* by Hamish McRae, page 13.**

*The very idea that the actions of one 28-year-old in Singapore should bring down an august merchant bank, let alone threaten the stability of the world's financial system, is so inherently improbable that were it presented as a film script it would be regarded in the same light as Jurassic Park - great entertainment, but mercifully impossible in the real world....*

Leeson had accumulated a substantial long position in Nikkei 225 futures contracts in the belief that the index would reach 19,000 by early March 1995, when the contracts became exercisable.

**The Independent 28 February 1995 - *"Trader evaded sophisticated control systems"* By Stephen Vines, page 2.**

*It could be said that an Act of God brought the mighty baring Brothers bank to its knees. Last month's Kobe earthquake sent the Tokyo market crashing by 1,000 points, crumbling the long run of multi-million profits produced from Baring's Singapore office by Nick Leeson, its chief trader in the high-risk market of betting on the future....*

For business reasons it was necessary for Barings' senior managers to cede more power to Leeson than was prudent. It is arguable that they did not understand the risk they were taking, it is arguable that they were greedy. It is not possible for a review process to occur before decisions are taken. The area of error or negligence on the part of the management was with regard to the back-office, by putting Leeson in charge of the supervision of client account management allowed him the opportunity to create false or dummy clients, thus permitting him greater flexibility when dealing.

***The Times 28 February 1995 - "Rogue trader and wife flee police in yacht"* by Catherine Field and Dominic Kennedy**

*As Singapore police issued a warrant for his arrest, it emerged that the key to the deception was that he was both the deal maker in derivatives and head of the small office's settlement department, which processes all deals. By being allowed to carry out trades and settle them himself, he was given ample opportunity to conceal his activities from his superiors. He is thought to have been given the highly unusual dual role in an attempt by Barings to contain the costs of its international network.*

This is quite astounding if true. They put the fox in charge of the chickens! This cost saving is on a par with those savings made by companies that lead to injuries - failure to install proper safety equipment or ensure that employees follow the safety guidelines, even when this reduces output. Perhaps there is even a case to be made for negligence. The amazing thing is that they were looking to make cost savings in one of their most profitable areas; the employment of a settlement head in Singapore would have been chicken-feed in comparison to the amount of money that Leeson's department made in the first half of 1994. Three questions need to be asked: would reducing Leeson's powers also have curtailed his earning potential? And if the answer to that question is yes: was any move to respond to the warning signals blocked? and by whom?

There are a number of lessons that may be drawn from the events prior to February 27, 1995.

**The Times 3 Mar 1995 "Bank *audit warned of risk last August*" by Simon de Bruxelles, page 1**

*An internal audit at Barings warned as long ago as August of a "significant general risk" that Nick Leeson could override management controls....*

*The 24-page report asks the questions: "Have the rules been broken to make these profits? Have exceptional risks been taken?" And it concludes: "There is a significant general risk that the controls could be overridden by the general manager (Mr Leeson). He is the key manager in the front and the back office... this represents an excessive concentration of powers."*

*It recommended that Mr Leeson be relieved of some of his power and risk limits observed.*

**The Sunday Times 5 March 1995 Insight *"Warning bells rang six months ago"* Frank Kane, David Leppard, Nick Rufford and Mark Skipworth. Page 1 & 2.**

*Singapore officials said the bank was warned three years ago about giving too much power to Nick Leeson, the trader at the centre of the crisis....*

*In Singapore, V K Rajah, a lawyer for Price Waterhouse, the accountants who have been put in charge of Baring's operations there, disclosed details of the warning about a possible disaster, made in a letter written by James Bax, head of Barings Singapore, in March 1992. The warning was made to Andrew Fraser, a senior executive in Baring's investment banking division in London, immediately after Leeson's appointment to Singapore.*

*It said: "My concern is that once again 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."...*

*Further doubt is cast on this claim [the claim that senior management knew nothing of the problems in Singapore] by an internal Barings audit in August 1994 which warned that Leeson had "excessive concentration of power" and that this could lead to "error and fraud". A Singapore investigator said yesterday that the company had failed to follow the audit's recommendation to restructure its futures business....*

**The Sunday Times 5 March 1995 Business Focus *"Lost Barings"* by Kirstie Hamilton page 2.3**

*The largest single sign of trouble at the bank was the cash haemorrhaging out of its London bank accounts. More than £400m was transferred from London to Singapore in the six weeks leading up to the collapse of the bank. The money went straight to the futures exchanges where Leeson invested, either to cover the deposits for original transactions, or to meet margin calls when losses on his contracts began to rack up....*

*Rivals insist banks do not transfer sums like this without authorisation at the highest level.... At Barclays, which is 20 times bigger than Barings, no manager can transfer more than £10m without going to the treasury committee....*

**The Independent 28 February 1995 *"Bonus claim just weeks before bank's collapse"* By Jeremy Warner, John Eisenhammer and Donald MacIntyre, page 1.**

*It also emerged last night that Mr Leeson's trades, which Barings claims only came to light on Thursday, were common gossip among market traders as long as three weeks ago. Certain leading City houses took urgent steps to reduce their credit exposure to Barings...*

The warning signs were apparent if the reports are to be believed and the senior managers were content to do nothing believing that the cost-benefit ratio favoured them.

Figure 3.4 graphical depicts how an individual's attitude might be effect by a environment that views a course of action as positive or where there are few or no signals that indicate that the action is unacceptable. The pressure for high sales may have caused Leeson to place more relative importance upon the outcome of his actions and less on his subjective norms. Many might describe such a stace as Machiavellian or support it by arguing that "*the end justifies the means*!"

The Leeson case offers an exaggerated example of what can happen when the pressure to sell and make the numbers gets too great. Employees may

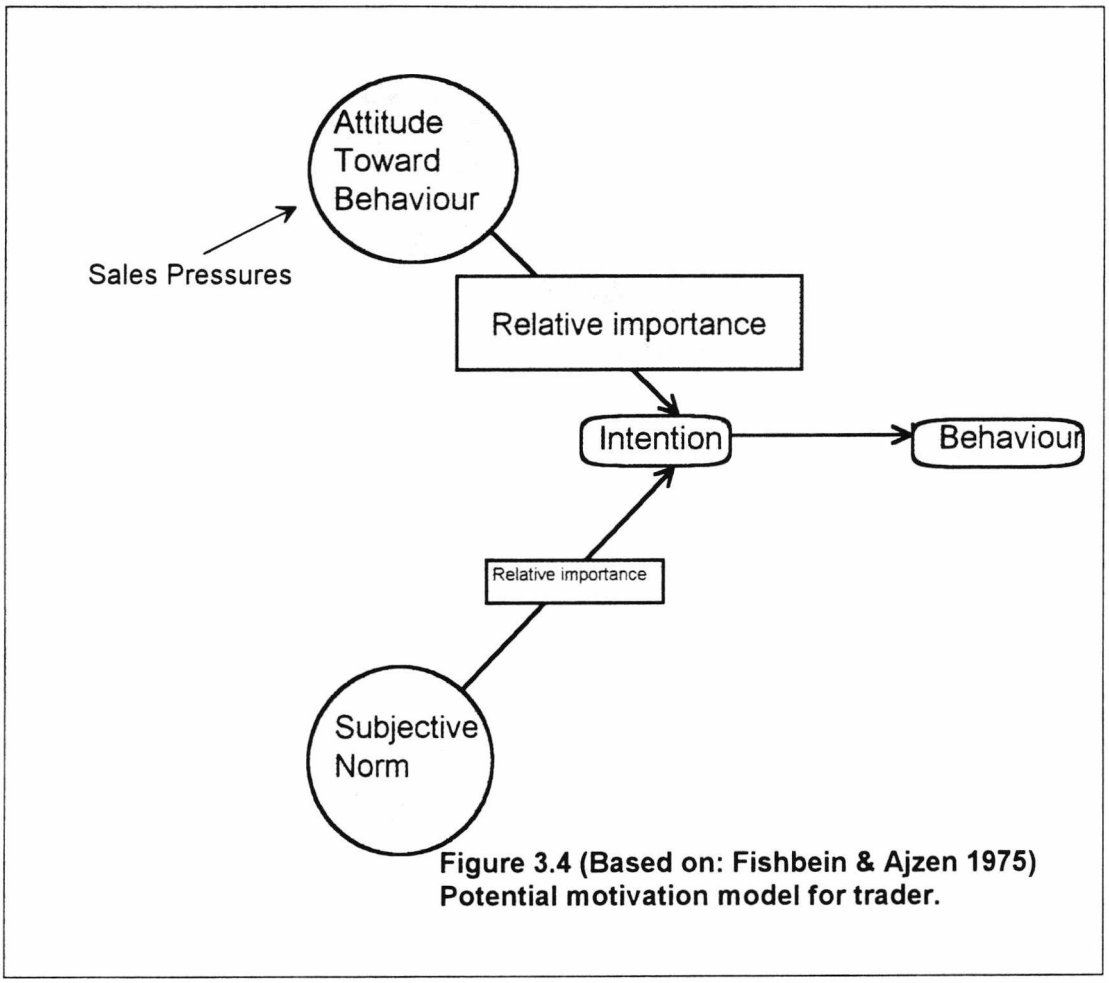



**Figure 3.4 (Based on: Fishbein & Ajzen 1975) Potential motivation model for trader.**

face many similar pressures and bankers are no exception and with all the changes at present evident in the banking sector it would not be surprising if an individual did react under such pressure.

Alternatively, it could be argued that Leeson was experiencing "normlessness". This occurs were an individual has no norm or is insufficiently versed in that behaviour that is acceptable and expected of an individual in their position. The individual could be said to be Culturally Illiterate, some commentators (Stanley 1992) have argued that it is such normlessness that has led to the crimes that racked the City in the 1980s as the norms of the Old-City were submerged by the attitudes of the New.

One lingering doubt remains with regard to any possible fraud - where was the gateway? If Leeson's intentions were criminal how did he intend to realise the financial benefits of his deviant actions? It is possible that he did not view

his actions as criminal - although he did break-rules if the accusation that he set-up false accounts is true - but was doing all he could to improve his figures, thus ensuring quite considerable bonuses. Whether such can be considered as a fraud gateway is doubtful unless you concede that other managers have been equally culpable in their search for higher profits and failed to properly observe and evaluate the risks associated with their actions.

> ***"Barings fiasco gives cheer to Britain's competitors: The debacle will accelerate the trend towards foreign domination of the City"*** **Economic View by Anatole Kaletsky.**
>
> *With luck, the City's philosophy of competitive individualism, its cult of youthful inexperience and its "high-risk, high-reward" star system, may even begin to lose their hypnotic influence over management methods in British business generally and in the public sector. The atmosphere of teamwork and mutual trust that used to be considered a prerequisite in building a large financial institution has been systematically undermined by management methods that focus exclusively on individual performance....*

This offers the banks another lesson in the importance of understanding the culture of the environment that you work within, and when managing people, the culture that effects their behaviour. The Baring's Crisis 1995 can be said to have been persipitated not by the actions of one man but through the lack of actions of a few more senior managers and directors.[53] Had they understood the risks - as well as the rewards - of the operation that they were "managing" they would have either prevented the crisis, or at least limited the losses.

A useful way of considering the effect that culture might have on the performance of a firm is McKinsey's 7S Framework (Peters and Waterman 1982).

> *"The value of this model is that it highlights the need for all consultant advisers to be aware that changing one factor is likely to affect other aspects of the organization. This is often called the "contingency approach" in that one thing depends on another." (Margerison 1988, p 132)*

---

[53]The Sunday Times 5 March 1995 Insight *"Warning bells rang six months ago"* Frank Kane, David Leppard, Nick Rufford and Mark Skipworth. Page 1 & 2.; & The Times 3 Mar 1995 "Bank *audit warned of risk last August"* by Simon de Bruxelles, page 1

It may assumed that if one of the S's must change that this will have an impact on the others. What the Big Bang purchases in the City in the 1980's and the Leeson case show is that control *Systems* and management *Style* must be compatible with *Staff* and their *Superordinate Goals* or culture. Failure to correct any discrepancies in the 7S's alignment may have serious consequences. In the case of Leeson, it may be argued that the Baring's senior management lacked the *Skills* to understand and manage the risks associated with the derivatives market and therefore did not appreciate the importance of keeping the sales desk and the back-office separate, or realise the significance of warning signs.[54]

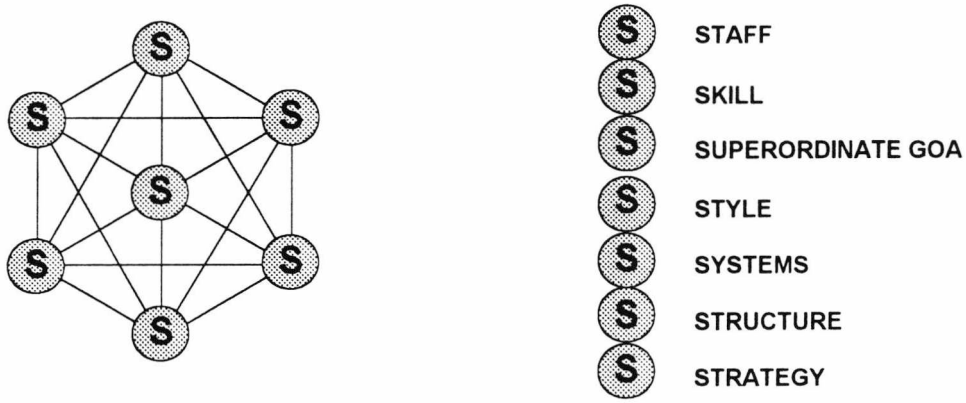



**Figure 3.5 McKinsey 7S Framework (Peters & Waterman 1982)**

The banks are currently facing a similar issue as their internal culture changes from one of *Service* to one of *Selling*. They must understand the risks that this change brings and audit all procedures and processes to ensure that these *Systems* are correctly aligned for the new environment. The changes in the banking industry will be considered in Chapters 4 and 5.

## conclusion

This chapter has looked at two high profile cases and considered the crime of insider dealing. What is clear is that whilst the laws may be clear, their

[54]The Sunday Times 5 March 1995 Business Focus *"Lost Barings"* by Kirstie Hamilton page 2.3

application may be less so. Criminal behaviour must be easily identifiable if the signal function is to work properly.

The case of Blue Arrow highlighted how a simple law can be complicated in its application. It also questions the effects of internal pressures and the role that they may play in the decision process.

The case of insider dealing also questions the control systems of banks and suggests that penalties should be imposed upon the employing institutions where the client's confidentiality has been compromised.

The case of Barings and Leeson highlights two practical lessons - duties must be clearly defined and a "dual-key" system operated where appropriate and the recommendations of your internal audits must be followed-up - as well as raising questions about how to manage "brilliant" individuals and "high-flyers" in risky markets.

The case studies also highlighted the importance of understanding the organisation that you are managing and appreciating the pressures that effect the individuals that work within it. Where management fails to do this they risk large losses from incompetance, error and fraud. This lesson is an important one for any banker as their industry changes into one that is heavily reliant on computers and one that is sales driven.

# Chapter 4

## Changes in the Banking Industry

*"Poor old Daddy - just one of those sturdy old plants left over from the Edwardian Wilderness, that can't understand why the sun isn't shining any more." John Osborne, Look Back in Anger.*

*"Come mothers and fathers*
*Throughout the land*
*And don't criticise*
*What you can't understand"*
*Bob Dylan*
*The Times They Are A-Changin'*

### introduction

The purpose of this chapter is to consider the impact of the changes on the Banking Industry that have occurred during the late 1980s and early 1990s. It will present a history of the period under consideration from a banker's perspective and analyse the potential implications of the changes that have occurred.

In the second part of the chapter the survey, conducted in 1992-3, will be introduced and the methodology discussed. The purpose of this survey was to gather information regarding bank employees' attitudes to the changing culture and environment, the greater use of information technology and their attitudes towards deviant behaviour.

In the final part of the chapter the implications of the changes and the results of the survey will be discussed as well as an assessment of the applicability of the motivation model for bank employees.

### banking in the late 1980s & early 1990s

The 1980s saw an impressive rise in the business of English clearing banks with a substantial rise in pre-tax profits (see Table 4.1). Staff numbers rose; British Bankers' Association (BBA) members employed 444,800 people in 1990 (102,200 more than in 1983) whilst the Major British Banking Groups

(MBBG[55]) employed 355,700 people in 1989 (82,000 more than in 1983)[56]. Some of this rise can be attributed to the inclusion of Abbey National in the figures (13,600 in 1989 & 14,000 in 1990) but it is nonetheless still a significant rise in numbers employed.

*Table 4.1: Shows the rise in pre-tax profits for five major English clearing banks*

| Banks | Pre-tax Profit 1988 (£ million) | Increase 1983-1988 (£ million) |
|---|---|---|
| Barclays | 1.391 | 906 |
| Lloyds | 952 | 553 |
| Midland | 693 | 468 |
| National Westminster | 1.407 | 889 |
| TSB | 420 | 270 |
| Source: Table 2.01, BBA 1994 page 26 | 4.863 | 3086 |
| | | 174 % average increase |

This period also saw an increased use of technology for the processing of transactions. Between 1983 and 1993 Inter Bank Cheque Clearing rose from 1,672.4 million transactions to 2,104.8 million[57] per annum. Between the peak of 2,292.9 million transactions in 1990 and 1993 the annual number of transactions declined by over 188 million. The same period saw a 45 million rise in the annual number of credit card transactions to 738 million in 1993, whilst the annual number of domestic retail transactions using debit cards rose from 192 million in 1990 to 569 million in 1993[58]. The annual number of direct debits rose from 254 million items in 1983 to 1046 million in 1993[59] with their value rising from £49.2 billion[60] in 1983 to £261.8 billion in 1993[61]. These

[55]Includes: Abbey National, Bank of Scotland, Barclays, Lloyds, Midland, National Westminster, RBS, Standard Chartered, & TSB. Formerly the Committee of London and Scottish Bankers, became the MBBG in April 1991 which now also includes Abbey National (BBA 1994, Annex. page 1).
[56]Table 6.04, BBA 1994 page 59.
[57]Source: Table 3.02 page 36 BBA 1994.
[58]Source: Table 6.08 page 64 BBA 1994.
[59]Source: Table 3.01 page 36 BBA 1994.
[60]The American meaning: billion = 1,000 million.

changes are summarised in Figure 4.1 which shows the relative rises in automated payments which are not paper based.

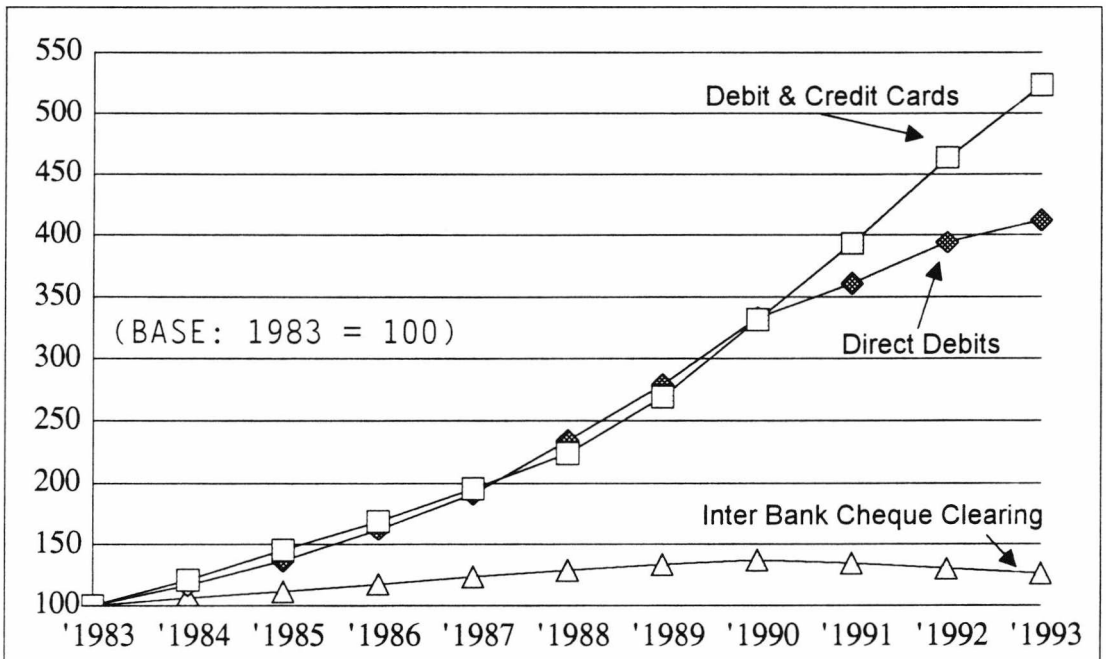



Figure 4.1: Shows the relative growth rates of the volume of transactions involving Debit Cards or Credits Cards issued by Visa/Mastercard; Direct Debits and Inter Bank Cheque Clearing.

Cheque clearing may be automated but the huge amount of paper involved and its processing makes it a more expensive payment method. Encouraging the greater use of non-paper based payment methods such as Direct Debits and "*plastic*" cards has ensured savings for the banks.

There were 527,000 UK outlets that accepted payment by Mastercard in 1993 compared with 431,000 in 1990, and 421,000 that took VISA in 1993 compared with 384,000 in 1990.

One of the major areas of investment in information technology for the banks has been in Automatic Teller Machines (ATMs) and cash dispensers. Between 1983 and 1993 the number of ATMs and cash dispensers rose from 4,902 to 14,094[62]. Of these 1,367 are located away from a branch, for

[61]Source: Table 3.02 page 37 BBA 1994.
[62]Source: Table 6.06 page 62 BBA 1994.

example in a shopping mall. The use of ATMs and cash dispensers has also increased since the early 1980's. Since 1983 the annual number of withdrawals increased over 300 per cent from 206 million to 966 million in 1993[63].

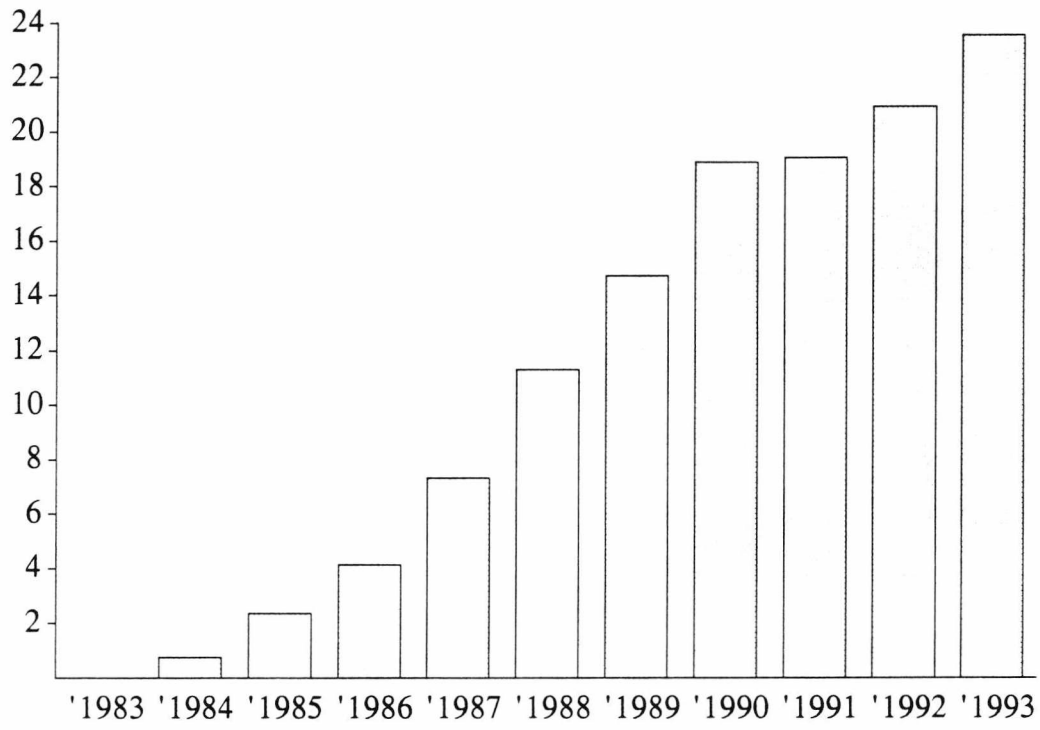



Figure 4.2: Shows the rise in the value of CHAPS payments (£1,000 billion). (Source: Table 3.02 page 37 BBA 1994)

The growth in Clearing House Automated Payments System (CHAPS) payments has seen a greater rise in volume and value than any of the other payment methods mentioned above. In 1984 just over 1.1 million[64] payment instructions were processed with a value of £741 billion[65]. By 1993 these figures had grown to 11 million and £23,545 billion respectively (see Figure 4.2). CHAPS is a computer based inter-bank payment system that allows same-day clearing. When it commenced on the 9 February 1984 it had a minimum transaction value of £10,000 and a maximum of £100,000 (Annex: Page 6, BBA 1994). The removal of these limits - the maximum limit in May

[63]Source: Table 1.15 page 24 BBA 1994.
[64]Source: Table 3.01 page 36 BBA 1994.
[65]Source: Table 3.02 page 37 BBA 1994.

1984 and the minimum in stages culminating in January 1992 - is one of the causes of its greater use. Another cause was the housing boom and the fact that CHAPS payments have become the favoured method of transferring related sums of money between solicitors. The increased use of CHAPS reduced the demand for messengers who would have "*walked*" authorised payments between the branches concerned in the past.

By the end of the 1980s the banks were suffering from a number of problems. They had a large bad debt problem which lead to MBBG members making Bad Debt Provisions (excluding exceptional charges) totalling £24,441 million [66] in the four years 1990 to 1993. In the same period "Plastic" fraud in the UK totalled £583 million[67]. They also faced stiffer competition from a number of directions.

The job of a bank clerk was once seen as very stable and respectable with very good prospects for long-term employment. The salary was never stunning but together with pension schemes, low-interest loans and mortgages, it was quite attractive. The banks sponsored their employees who wished to take the Institute of Bankers' (now the Chartered Institute of Bankers; CIB) examinations and would also allow time off for various civic duties that employees might be elected to undertake. They would also pay membership dues of various clubs or associations if the employee so desired. Bank clerks held positions of responsibility in many of the clubs they joined as they were seen as stable, reliable and above all, trustworthy; Probus et fidelis being the CIB's motto.

A number of changes over the last ten years have ensured that much of this has now changed. From the end of December 1989 to the end of December 1993[68] the total number of the branches run by MBBG members fell by 2,012 branches[69].In the same period the number of people employed by MBBG

[66]Source: Table 2.05 page 31 BBA 1994.
[67]Source: Table 6.09 page 65 BBA 1994.
[68]This is a comparable period to the years 1990 to 1993 inclusive.
[69]Source: Table 6.05 page 60 BBA 1994.

members fell by 48,700 to 300,100 (14 per cent decline) and the number of male employees fell 23,100 to 110,400 (17.3 per cent decline). Staff numbers have fallen largely due to a rationalisation of the way that banks offer their services. Branches are being clustered and grouped so that they may be administered and managed as local profit and cost centres. This has reduced the need for managers in the smaller branches - the managerial functions having been centralised in the larger branch. Some of the banks have centralised their mortgage services so that loans for property and the related security are being processed by a national department. Many other services have been considered for similar treatment but the disadvantages of slower response times and the loss of branch control over the process may outweigh the benefits (Cressey & Scott 1992).

Most of the job losses have been achieved through "natural wastage" and voluntary redundancies but they have nevertheless affected the attitudes of bank employees. As one female employee in her twenties points out: "*Banking has lost the 'job for life' and 'good career' image.*" When two members of staff of one bank branch were made redundant against their will the bank took the precaution of employing counsellors for the remaining staff. The shock was felt by all; "*It was horrible when they had to leave*" one member of staff told the author, "*We all felt so sorry for them.*"

This change has occurred at a time when the banking system has become more competitive. Banks have offered full mortgage services since 1981[70] and the building societies have been able to offer overdrafts since January 1, 1987 with the enactment of the Building Societies Act 1986. This breaking down of the traditional monopolies of the two big types of high street financial institution has inspired stiff competition. Store finance has also increased over the past ten years and Marks and Spencer and other stores have extended their activities into areas that were traditionally the preserve of banks and insurance companies. These moves are steps along the tracks to the

[70]Before 1981 the banks' mortgage activity had been limited to bridging finance, short-term mortgages (less than 10 years) and staff mortgages (Hanson 1987).

"*financial supermarkets*" - a logical step on from Sir Leslie O'Brien's "*all-purpose banks*"[71], predicted for the next century. It has also ensured that the institutions involved must be more innovative and aggressive in their pursuit of business. This has led to the adoption of a new culture in many banks that is alien to that of the traditional bankers who learned their trade in a service environment. As one manager in his thirties pointed out:

> *The banking culture has changed significantly, particularly in the last 6 years. New entrants in this time have not witnessed such large scale changes as those of us who have been working for a longer period. It really could be a case of adapt to survive. (Comments made in response to question in survey)*

A female employee in her thirties commented on the situation by saying:

> *I enjoy my job but the current situation in the world of finance has increased the pressure to "hard sell" products which I disagree with. (Comments made in response to question in survey)*

This has had an effect on the attitudes of bank employees. Some of the older members of staff took early retirement and many volunteered for redundancies when the offer was made. Others have adapted, whilst many find it hard.

> *The Bank is trying to place a sales culture onto all staff - although many of those staff fulfil an administrative role and have little access to customers for selling. Result - Demotivation. (Male, 30 - 39 years old - comments made in response to question in survey).*

It is this "demotivation" which raises concerns with regard to crime. Under different circumstances it might have led to an increase in crime within the banking industry. The reason that this increase has not apparently occurred may be largely due to the type of people that the banks have traditionally employed[72]. The rest of this chapter and the next offers results from a survey that tests the hypothesis that bank clerks are on the whole moral individuals who are extremely law abiding in comparison to other groups. They lack the

[71]A former Governor of the Bank of England. Speech in 1973 to the Institute of Bankers in Scotland. Referred to by Hanson (1987, pages 3 - 4).

[72]It is assumed that bank employees, on the whole, have always been loyal and highly moral individuals. It must be acknowledged though that this assumption has been neither proved nor disputed by previous research.

skill to commit computer exclusive crimes but have many opportunities to commit computer related crimes. The current staff could steal from the till but the majority do not. It would not be particularly hard to achieve. They could alter the account number on credit slips so that the when processed the funds went to another account[73]. The amount at which a credit's number and name are checked is well known and even if the "error" was spotted it would not necessarily arouse suspicion, but would be merely corrected. CHAPS instructions could be manipulated[74]. There are many ways for an insider to steal from the bank they work for but the vast majority do not; why not?

## the survey.

The survey was designed to "measure" the respondents' attitudes to a number of different types of behaviour, in particular computer crime, and their attitudes to their jobs and working environment. The survey sought to identify factors that might contribute to an environment that would increase the propensity for such behaviour. The main sample and pilot sample were given a five part questionnaire whilst two further samples were given a three part one (parts four and five of the first questionnaire were used in the second shorter questionnaire along with a modified personal section).

## the methodology.

The survey consisted of three separate main stages plus two supplementary stages. The first of the main stages involved the design and testing of the questionnaire (the design of the questionnaire will be discussed further later). The test group consisted of ten bank employees - five managers and five clerical and supervisory grade employees - who had all spent at least two years in the employment of their then current banks. Four of the test group, 40 per cent, were female, which was less than the proportion of females in the national banking population - 63.2 per cent of the employees of MBBG

[73]This is arguably a computer dependent crime. Banks allocate account numbers so that many processes may be computerised. It would have been very difficult to perpetrate in the days of manual book-keeping.
[74]A good example of an input fraud.

members were female in 1993[75] - which is not surprising due to the group's bias towards appointing men as managers. There are two reasons for this bias. Firstly it proved an useful introduction to the purposes of the survey and hopefully enlists the interest and support of a number of the managers for the second stage of the survey. And secondly it is easy to isolate such people so that the impact of the second stage on the sample would be more effective. The five members of the group who were not managers were employed at branches away from the area and all members of the sample group were asked not to discuss the questionnaire with anyone else. If members of the eventual sample had seen the questions in advance it might have affected their responses.

The purpose of this test group was to ensure that the questions were not confusing or ambiguous and that the questionnaire was not too long. As a result of this stage a number of changes were made to the questionnaire, but the overall aims and types of questions proved to be sound and many of the questions were interesting to answer as far as the respondents were concerned.

The second stage was a more extensive pilot study than the test study. It was used to test the questionnaire and the alterations made. For this purpose a large branch of between sixty and seventy staff was identified in the area. The branch manager was approached and approval secured for the circulation of the questionnaire to all members of staff. Each potential respondent was asked to answer the questionnaire before discussing any of the questions with their colleagues. The confidential nature of the responses was verbally restated thus augmenting the written statement on the cover of the questionnaire:

> *This survey is totally confidential; no other member of your employing company will see your answers. Should you decide to make further comments at the end of any section of the questionnaire these may be quoted in the eventual PhD thesis, if you do not wish them to be reproduced in this way please indicate accordingly.*

[75]Table 6.04, BBA 1994 page 59.

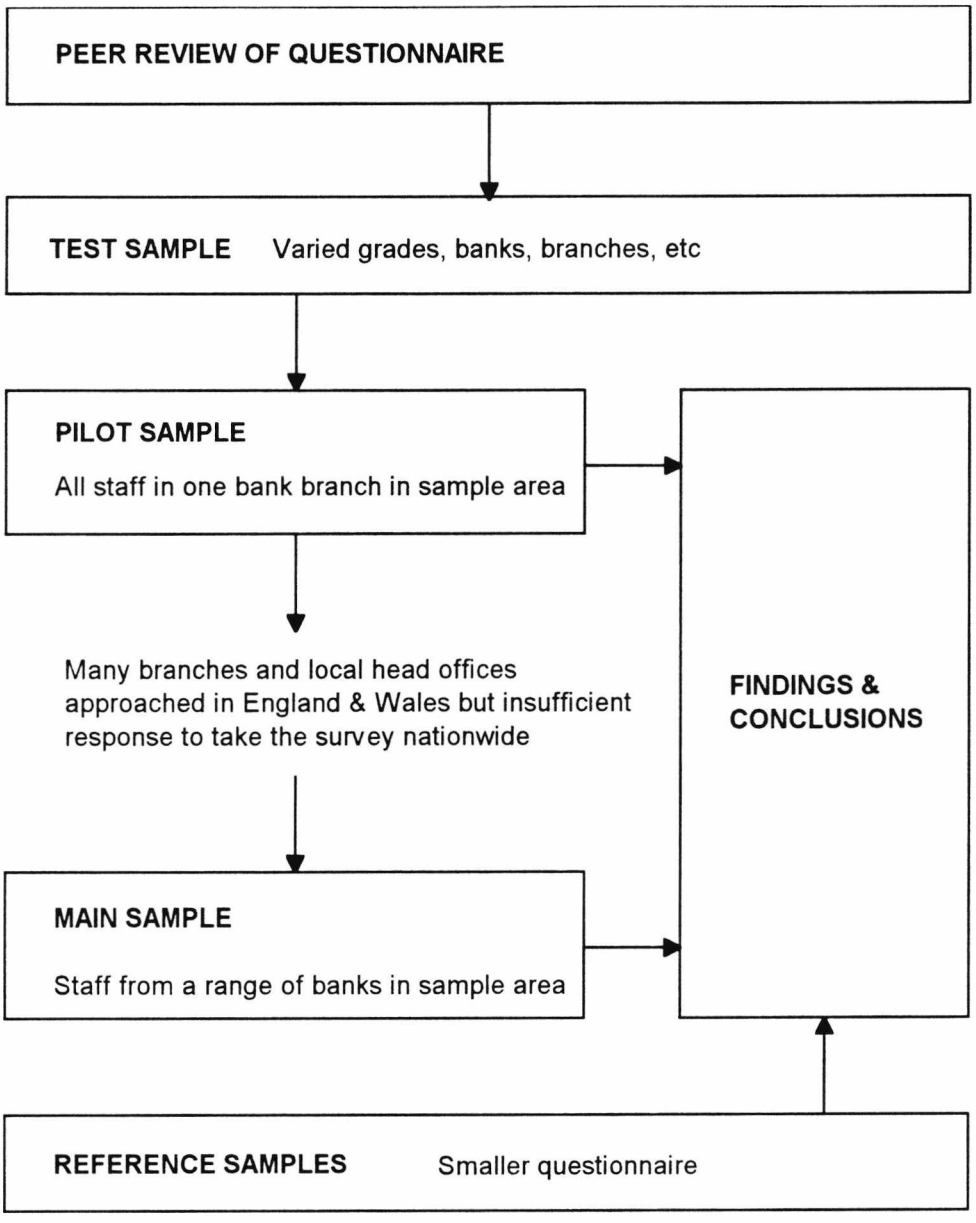



*Figure 4.3. Summary of data collection approach used*

The completed questionnaires were collected in person by the researcher after one week and again after two weeks. Those that had not replied by the second collection were given instructions concerning the postal return of the completed questionnaire.

The third stage of the survey involved the circulation of the questionnaire to other branches in the sample area. The members of the sample were employed by all the MBBG members, with the exception of the Bank of

Scotland and Standard Chartered - they did not have branches in the survey area - and a number of building societies. The initial intention was to test the hypothesis on a national basis. Letters were sent to a geographically diverse selection of bank managers from England and Wales. A copy of a questionnaire was sent with each letter. The responses of those approached were, with one exception, negative. The following quotes were typical of the responses received:

> *Whilst I fully appreciate your desire to acquire information to help with your studies, I regret that the type of information you are requesting, and the nature of the exercise is not one I can agree to. (Regional Director, bank in the north of England).*
>
> *I have had a look at the nature of your questionnaire, and think at the present time when I am sure you will be aware there are many pressures on all Bank staff, that I would prefer to turn aside your request. (Branch manager, bank in the south of England).*
>
> *I regret to advise... that after due consideration we feel unable to assist you with your research on this occasion. (Resource Officer, bank personnel department).*

Follow-up telephone conversations were more informative of the reasons for declining to help. The main excuses given were that their employees faced many demands on their time; and that the branch was in turmoil due to "structural" changes that many of the banks were then currently undertaking. Many were in the process of centralising services; some on a national basis and others on a more local basis (see above). For instance a large town branch might handle all the loan requests for four or five surrounding smaller branches or satellites. This process is also happening with accounts so that they too might be centralised in the near future[76]. This meant that many employees were working overtime to meet the requirements of such changes. Their managers therefore felt that they did not have the necessary time to complete the eight page questionnaire. A more cynical mind might assume that they were worried that some of the questions might excite a disenfranchised staff to be more vocal about their dissatisfactions, and that the managers were concerned about the eventual use of the data. Whatever the true reason, and a mixture of the above two seems likely, this failure to

[76]Centralising on a local basis is referred to as "clustering" by one of the major banks.

secure support from a geographical spread of managers meant that a re-think about the approach was necessary.

The branch of the one manager who had responded positively was used for a pilot study. The results highlighted very few weaknesses and most of the changes needed related to the layout and the clarification of questions. Upon completion of this pilot study other bank and building society managers were approached in the same city, and from 17 institutions approached, 12 managers agreed to the participation of their staff. The managers of three building societies declined outright; one quoted a recent Panorama programme which had criticised her society's handling of changes in employment contracts for some staff. She had had instructions from her head office which precluded, along with other activities, any involvement in surveys of the type being conducted.

Another reason for the single geographic nature of the survey was as a result of cost and control. By conducting the survey in one area the survey could be controlled and managed from a base developed at one point rather than being reliant on more than one base or the postal service. The single location meant that when the questionnaires were prepared they could be delivered to the branches *en masse* and distributed and collected by means of the branches' internal mail system, or in person by the researcher. The single location also meant the researcher could be effectively be on call for questions that might arise about particular questions and to collect completed questionnaires.

This geographical bias represents a potential drawback for the validity of the results. There are two reasons, though, to suggest that this weakness might not be significant. Firstly the retail banks tend to recruit from a similar sector of the population; the average bank employee is probably educated to "O" level or equivalent and joined the bank in their teenage years for instance.

And secondly, banks have a very strong culture and staff ethos that ensures an element of uniformity.

The two supplementary stages involved the collection of two alternative samples involving members outside of British banking. The larger of these involved a group of international business students studying in institutions for an MBA in Europe or North America. And a second supplementary sample was sought consisting of bankers from New Zealand and the United States of America. Due to the distances involved there proved to be many pitfalls in this plan and the responses for this stage were, on the whole, poor.

The purpose of the student sample was to offer a comparison with a differentiated group, one with different norms and a fundamentally different culture. The selected group was intentionally international in nature and all were educated at a higher level than the vast majority of the bank sample. The business background of the group makes them, in the majority, profit and goal oriented, and, it is hypothesised, happier in a sales culture.

## the questionnaire.

The purpose of this questionnaire was to assess whether motivation was high or low within the Banking Industry in view of the uncertainty and changes that it faced. It asked the staff whether they felt that their senior management's plans had been properly communicated and whether management had consulted staff sufficiently. Within the questionnaire were a number of questions enquiring of an individual's willingness to commit petty indiscretions and to assess their opinions of those who did so. It also enquired as to what experience the individual had had with computers; what access that they have had or currently had. It asked them to assess the threat of computer abuse in general; whether the respondents had personal experiences of abuses such as viruses, affecting their work. How great did they perceive such risks to be?

The questionnaire was designed to gather information regarding the respondents' attitudes concerning a number of topics. It asked questions concerning the respondents' job satisfaction; how they felt about their job; their attitudes to computers at work; their attitudes to crime and deviant behaviour; and what factors they felt prevented them from acting deviantly themselves. The questionnaire consisted of five sections.

The first section of the questionnaire addressed the issue of job satisfaction and how the respondents felt about their jobs. The first part of this section consisted of questions to evaluate the respondents' opinions of their working environment and their work in general. It was designed to measure their motivation level and the respondents were expected to respond as to whether they were "Very Dissatisfied" (1), "Very Satisfied" (5), or somewhere in between, for one of ten job related factors including "Job Security" and "Pay". The list was devised so as to include those factors that Herzberg (1966, 1968) identified as being "Demotivators" or "Dissatisfiers".

1. Pay - Including benefits such as prefential rate loans
2. Job Security
3. Number of hours worked
4. General management
5. Direct supervision
6. Relationship with supervisor
7. Bank policy and administration
8. The work itself
9. Responsibility/Autonomy
10. Relationship with peers

The list above is not a direct translation of Herzberg's list of *Hygiene factors* as related in his 1968 *Harvard Business Review* article. *Company policy and administration* has been changed to *Bank policy and administration* for obvious reasons. *Supervision* has been sub-divided into *Direct supervision* and, to a certain extent, *General management* so as to pinpoint any areas of complaint concerning the respondents' seniors, and where the relationship with the direct supervisor was extremely convivial that the effective supervision was considered, i.e. when the relationship was such that much of

the control and authority over the respondent came from a source other than the supervisor. *Work conditions* was substituted for *Number of hours worked* as this was identified as a problem at the time of the survey, and also to clarify what was meant by work conditions, such a term being rather broad and open to much interpretation. Three of Herzberg's list of hygiene factors were excluded and two of his motivators included in the list above. *Work itself* was a motivator in his study with a greater percentage frequency of events on the job leading to *extreme dissatisfaction* than all but two of the hygiene factors, for this reason it has been included above. *Responsibility* was by no means as strong a factor as *Work itself* but was chosen for inclusion in the ten as, with *autonomy*, it can be a cause of dissatisfaction. When respondents answered whether they were satisfied with each factor they were also asked to indicate whether they thought the factor was important or not.

The second part of the first section was used to augment the first part and to give the respondents the opportunity to express their opinions of their working life by way of agreeing or disagreeing with a number of statements concerning their job or the bank in general. The fourteen statements covered pay, job security and general happiness at work:

1. I get a lot from my job[77]
2. My abilities are underused in my current job
3. Others are paid more fairly than me
4. I would leave if I could
5. The bank is well run
6. My work makes me tense
7. The bank's directors are overpaid
8. I feel secure in my job
9. The bank is poorly run
10. I am happy at work
11. I would "*call in sick*" to attend a job interview with another company
12. A bank clerk's role has changed from one of service to one of selling
13. I am only working here because of the poor state of the job market at present
14. If I knew then what I know now I would not have joined this bank

[77]Some of the statements presented in the questionnaire may not be grammatically perfect but are worded such as they echo statements heard by the author during his time as a banker.

Questions 12 and 14 were included to assess whether the respondents agreed with the premise that the banks' cultures were changing and that their orientation was becoming more sales oriented. Question 14 was also asked to see how many members of staff were unhappy with the changes they had seen during their bank careers. Cressey and Scott (1992) sum up the situation for many bank employees:

> *"The banks move towards commerciality, their emphasis upon competition and the drive to sell new and more specialist products means internal changes regarding staff. Staff have now to be coached in social and interpersonal skills, in 'customer care', to be knowledgeable about a range of products and able to promote and persuade the public about the qualities of the products concerned. Rather than administering a set range of tasks they have to be adaptable to new and changing demands." (Cressey & Scott 1992, page 93).*

The second section of the questionnaire gathered information concerning personal details and information about the respondents' careers within the banking industry. After the standard questions on sex, age and marital status the respondents were asked to state what qualifications they held and in what area of the branch they worked:

1. Accounts department
2. Cash tills
3. Enquiries/ Customer service
4. Foreign desk
5. Loans Department
6. Securities Department/Stock Ex.[78]
7. Management
8. Computer department
9. Other (please state)

The respondents were asked to indicate the length of time spent working for their current employers and how long they had spent at their current branches. The reason that this information was sought was to see if there was any evidence that this affects the motivation of staff. Katz (1978) suggests that the time spent in a post effects the motivation of an employee. Bank employees tend to have more general roles within a branch and will be employed in a number of posts with a similar theme; this theme tends to

[78]Stock exchange services - handling the buying and selling of shares for customers as well as dealing with Money Market deposits.

change when the employee moves from one branch to another. The time spent within the branch was requested to see whether Katz hypothesis may be applied more loosely.

The final two questions in this section concerned salary and whether the respondent was a member of full or part-time staff. The questions in this section were largely of an uninteresting nature for the respondents so were kept to a minimum and the section placed after a section of more interesting questions. The answers to this section were useful for correlative purposes and also as a check of the validity of the representative nature of the sample.

The third section of the questionnaire was designed to gauge the respondents' opinions of the role of computers in their working lives. On the whole it was felt that this section would prove that the majority of bank employees did not have a very good knowledge of computers other than a good working knowledge of how to operate their branches' terminals. Some of the questions in this section of the questionnaire was designed to measure the level of computer literacy of the average member of bank staff. It would have been more desirable to use a series of tests to measure the abilities of the respondents but this would have required the full cooperation of both the staff and their employers. It was therefore decided to assess the sample's level of computer literacy on a self-certifying basis. The assumption that general computer literacy was not high in the retail branches of clearing banks was tested by the last two questions in this section which asked:

> *Do you write computer programs?*
> *Please indicate the language you use; What other languages can you use?; Which language would you say you are most competent in?*
>
> *Do you have a computer modem?*
> *What is the speed of your modem? Please indicate what services you use.*

This section as a whole was introduced by the following statement and question:

*The use of computers has increased over the last two decades. What are your views of them in general and on their use in banking in particular? Please indicate whether you agree with the following statements:*

and the respondents were again given the opportunity to indicate whether they agreed or disagreed with each of the following statements:

1. I have had much experience of computers and their possible applications
2. Viruses are a major threat to computer users
3. Hackers are a major threat to computer users
4. If a colleague used unauthorised software or hardware they should be dismissed
5. I would *"turn a blind eye"* if a colleague amended their bank credit card limit using a branch terminal
6. I have a good understanding of computers
7. I would alter the balance of my account if I knew I would not get caught
8. Bank clerks are in general honest
9. Computers make my job easier
10. I enjoy using computers
11. I have acquired a good understanding of computers from bank training courses
12. I have a poor understanding of the computer systems that the bank uses

Questions 1, 6, 11 and 12 are concerned with the respondents' abilities or knowledge of their banks' computer systems. Questions 9 and 10 related to whether the respondents felt that computers helped bank employees do their jobs, whilst 2, 3 and 4 were concerned with the threat to computer systems from viruses and possible attacks from crackers or hackers. Questions 7 and 8 addressed the issue of the honesty of bank employees and the problem of deviant behaviour for the first time in the questionnaire, whilst question 5 aimed to measure the extent that bank staff are willing to over look some element of deviant action by their colleagues.

In the fourth section the emphasis turned towards measurement of how serious they perceived certain types of deviant or criminal action to be. The respondents in the pilot study were asked to score certain types of action against a base of 10 for the *theft of an unlocked bicycle* (Lodge 1980). Levi (1987[79]) used a similar approach in a survey of the attitudes of senior

[79]Reporting a study that he conducted for the Home Office Crime Prevention Unit - *The Incidence, Reporting and Prevention of Commercial Fraud* - unpublished monograph 1986.

executives to crime, although he asked his fifty-six participates to rank the offences on a scale of 0 to 20. The list of scenarios offered to the respondents were in the most part related to the bank employees' day-to-day environment. A few of the scenarios were of a more general nature. Many of the examples are based on actual cases or, in one or two cases, organisational myth. For the main sample the scoring system was altered changing the base to 80 for the *theft of £100 from the till.* The examples were also changed slightly. The section was introduced as follows:

> *Attitude to crime and deceitful behaviour - How would you score the following acts? If the theft of £100 from the till were to score 80 how would the following score relative to that? For instance, if you feel that the theft of an umbrella was only half as bad as the theft of £100 from the till you should score it 40.*

This instruction was then followed by the following set of examples:

| | |
|---|---|
| Theft of £100 from the till | 80 |
| The act is four times as bad as the theft of £100 from the till | 320 |
| The act is only a quarter as bad as the theft of £100 from the till | 20 |
| The act is not a crime. It is acceptable behaviour | 0 |

The score system was changed between the pilot study and the main survey as it was felt that a significant few had assumed that the upper limit for the scoring of behaviour was 20 or 100 due to the use of a decimal score for the base. Also the *theft of an unlocked bicycle* is of less relevance to a banker than a theft from the till. The score of 80 was chosen as it was the log average score (see below) for the pilot study sample, for whom the *theft of £100 from the till* had been one of the scenarios.

1. Robert Maxwell's misues of pension funds
2. The theft of an unlocked bicycle/ theft of £100 from the till
3. A loans officer takes out loans in a false name
4. A junior clerk makes phone calls to a boyfriend in Australia. The total cost of the calls increases the branch's telephone bill by over £100 a month
5. A clerk who is on self certified sick leave spends the day writing a computer programme to help a local charity manage its books

6. A clerk manages to access the computer system and instructs it to pay one penny of interest due to all the bank's customers' deposit accounts to his account instead
7. A bank manager and a junior clerk act together to transfer £1,000,000 via CHAPS and then SWIFT to an account they have opened in South America
8. The Barlow Clowes Affair - the senior official of an investment firm defrauds many millions of pounds
9. A clerk is using a computer at work to write a number of computer programmes for his own personal use
10. A manager transfers £100,000 from a branch sundry account to a large corporate customer's account the day before he must report to his senior manager about the borrowing position of said client, the transfer takes the client below their overdraft limit. The following day he transfers the money back and has the statements retyped
11. Three women attack and mug a man on his way home late at night
12. A clerk takes a box of envelopes home
13. A clerk rings his mother every day. The cost of these phone calls adds £15 to the branch's monthly phone bill
14. A computer operator at the foreign department delays payments to branch customers holding the money on a deposit account for a day so that he earns interest on the money at the customers' expense
15. A clerk uses a word processor at work to prepare her CV
16. A clerk increases her credit card limit without authority. She needs the money to pay a gambling debt
17. A clerk uses the photocopier to make 100 copies of his CV
18. A clerk uses a terminal at his branch to place money on deposit over night in London in the name of a large corporate customer. He completes all necessary procedures but removes the entries before they can be processed and the customer debited. When the branch receives the interest payment from their head office three days later he makes appropriate entries to credit his account with the £4,000 interest earned
19. A clerk telephones his girlfriend to tell her he is working late. The call costs the bank £1.47
20. A clerk uses a terminal to increase his overdraft limit without authorisation. He needs the money to pay the rent
21. A man is shot by a terrorist on a train. The terrorists escapes by jumping from the moving train

The scenarios above are based on the experiences and observations of the author whilst employed by a major British clearing bank. Most of the banking related ones are based on techniques and procedures current in banks during the mid-to-late 1980s. As indicated above, one or two of them are broadly based on cases that actually occurred and everyone will recognise the use of the telephone to tell another person of lateness. The purpose of

this section of the questionnaire is to identify the types of actions which are now acceptable and those that are totally unacceptable. A number of cases are related in some way and purposely differentiated. Three cases, 4, 13 and 19, involve the use of the telephone and involve different sums and circumstances. Five cases, 5, 6, 7, 9 and 20, had a specific mention to a computer or computer based payment system such as CHAPS. Cases 5 and 9 involved unauthorised computer use (considered an abuse by the Audit Commission 1991) and are distinguished by the involvement of a charity in the first of the two. Case 6 involves a probably mythical case of a *hack*[80] to transfer a penny of interest from everyone's account to the perpetrator's account. An event very similar to this is said by some to have actually happened, but it is possible that they are confusing real life with *Superman III* [81]. Cases 11 and 21 involve violent act and two of the cases, 1 and 8, involve infamous public figures. The rest involve theft of some description; from the theft of paper to the theft of £1,000,000.

The survey uses various sums of money so as to gauge the impact on the opinions of the respondents. Some held the view that theft is theft no matter what, and some made comments to this effect, but as hoped, the majority of respondents did distinguish between the various thefts depending on the circumstances (see the results below).

The respondents were given an open range of scores for the various scenarios. If the respondent felt that the action was 10 times as bad as the base action they would score it 800 (or 100 in the case of the pilot study). This allows the respondents to express their disgust at a particular action and also develop their own scale. The drawback with such a method is that very high scores might distort the average score too much. The technique of magnitude scaling (Lodge 1980) is designed to avoid the massive fluctuation caused by such large scores. The effect that a score of 100,000 has on a

[80]A smart piece of programming or trick.
[81]Allen (1975) claimed that a case was being prepared against the perpetrator of a similar act but the case either never went to court or was never reported.

series with a previously much lower average is greatly reduced when using scaled averages calculated using the magnitude scaling technique (MS Averages) rather than mean averages. This effect can be seen in the following example:

| | Score | Log | MS Average |
|---|---|---|---|
| Score 1 | 100 | 2 | |
| Score 2 | 100 | 2 | |
| Score 3 | 300 | 2,48 | |
| Score 4 | 200 | 2,3 | |
| Average before Score 5 | 175 | 2,2 | 156,7 |
| Score 5 | 100.000 | 5 | |
| Average after Score 5 | 20.140 | 2,76 | 570,2 |

Before the magnitude scaling technique is used the average is distorted by nearly 20,000 with the inclusion of the fifth score. When using the technique the change is a little over 400.

The fifth and final section of the questionnaire considers what factors are involved in the motivation of an individual to commit a crime against their employer. It begins by asking the respondent whether they have ever committed a crime and offers them the following list of potential indiscretions:

1. Substance abuse; drug taking etc.
2. Shoplifting
3. General theft
4. Pilfering at work
5. Traffic offence
6. Other - Please indicate.

Some of the categories are more than merely indiscretions but all involve "*breaking the law*" in some way. This list followed the question about whether the respondent had committed a crime, so they were expected to indicate only those acts that they themselves considered crimes. The discussion about whether *substance abuse* is a crime is on-going, and some would argue that it is the deviant aspects and alternative nature of drugs that make

them appealing to many people. Numbers 4 and 5 are very broad in nature but here again it was intended that the respondents indicate only those acts that they considered as crimes. The purpose of this section was not to get the respondents to confess their crimes but to merely identify how many of the sample felt that they had *broken the law* at some stage in the lives. None of the above represent violent crimes as it is supposed that the motivation process is fundamentally different for such crime. That said, there will be times when an individual reacts on impulse or in a reflex manner to commit both violent and non-violent acts. Violent crimes lie outside the scope of this thesis.

The next question asked the respondents whether they had *ever considered taking funds, or other assets,* from their employers. There is obviously a big difference between considering an action and actually perpetrating it, just as there is a distinction between *mens rae* and *actus raem* in English Law. Consideration of deviant action such as this may be an indication of dissatisfaction or perhaps merely as an intellectual exercise when the job becomes boring; an exercise where you try to work out the weaknesses in the system and the procedures employed to mitigate them. It could also represent a risk or threat should disenfranchised individuals decide to implement their considerations. It was followed by a question designed to gather information about what factors might motivate the respondents to commit a crime against their employer:

> *It is acknowledged that the chances of you committing a crime against your employer are very slim, but if you did what would be most likely to motivate you? Please rank each of the following for their relative strength (5 being the strongest motivator, 1 being the weakest):*

1. If a friend or member of your family needed money
2. Revenge
3. Peer pressure
4. Boredom
5. If you needed money

There is a scenario where a non-deviant individual places more relative importance on the outcome of their actions than on the norm that usually governs their actions. An example of this might occur when a significant other person for the individual is in need of help. *The end justifies the means*, and any harm or damage done may be rationalised by the *good* done, it is easier to rationalise an act that helps another than one in which the beneficiary is also the perpetrator of the act.

The disenfranchised individual mentioned above may not feel any pecuniary need but may be motivated by a revenge need. The idea that boredom creates criminals, or at least facilitates the decline in an individual's moral code, is an interesting one which Nobel Prize Winner[82] Saul Bellow introduced in one of his novels. Bellow's character, *Charlie Citrine*, the central character in his 1975 novel *Humboldt's Gift*, surmises that had Hitler not been bored he would not have motivated the mayhem that he eventually did. Had Hitler achieved his aim and secured a place at art school his infamy could now be fame but for other reasons and the world would be a totally different place. To consider the idea on a more practical level parallels may be drawn with the idea of job satisfaction, and directing individual's abilities toward the achievement of corporate rather than personal goals.

The final question asked the respondents to indicate what factors prevented them from acting in a negative manner:

> *Please rank the following for their importance (9 being the most important and 1 being the least) in preventing you from acting criminally:*

1. The belief that such behaviour is immoral
2. The knowledge that such behaviour is illegal
3. Security measures
4. Procedures
5. Fear of being caught
6. Fear of prison
7. What my family would think
8. What my friends would think

[82] 1976 Nobel Prize for Literature.

9. What my peers would think

This final section was intended to gather information with which to develop the motivational model proposed earlier.

## conclusion

What motivates an individual to commit a non-violent crime? A financially related crime against or for an economically oriented organisation? More to the point what is the propensity to commit fraud or computer related crimes of those individuals currently being employed by the banks? This question is especially pertinent in view of the increasing reliance that the industry as a whole places on information technology and also in view of the uncertainty of those members of staff now facing an increasing possibility of redundancy as all the high street banks announce job cuts.

The next chapter will present the results of this survey and discuss the findings. It will also consider what conclusions may be drawn as well as applying them to the development of the motivational model proposed in the chapter on motivation.

# Chapter 5

## Bank Employee Motivation Survey

*"All conservatism is based upon the idea that if you leave things alone you leave them as they are. But you do not. If you leave a thing alone you leave it to a torrent of change." G.K. Chesterton "Orthodoxy."*

*"When work is pleasure, life is a joy! When work is a duty, life is slavery." Maxim Gorky "The Lower Depths"*

### introduction

The purpose of this chapter is to present the results and findings of the survey conducted to investigate the attitudes and opinions of bank employees regarding their working environment, motivation and job satisfaction, computers and crime. This chapter should be read in conjunction with the previous one in which the purpose, background and methodology of the survey were discussed.

### the survey results.

The survey data was collected from the latter part of 1992 until the summer of 1993, in total 104 responses were received, representing a 40.8 per cent response rate. The six largest banks had agreed to participate so that 81.7 per cent of responses were from bank employees. This bias is not surprising due to the fact that banks employ more people per branch than building societies do. The average number of employees per society branch was less than seven compared with 15 staff in the smallest bank branch. 60.6 per cent of respondents were female compared with a national average of 63.2 per cent. Of course such comparison does not prove anything conclusively but does strengthen the assumption that the sample is not sexually biased. Secondly, the results enabled the building of a profile of the "average" employee. The results indicated that they were unlikely to have a degree (only two respondents had indicated that they had) although they were likely to have qualifications of "O" level/CSE/GCSE standard or higher (95.2 per

cent of respondents). They are likely to be over 21 years old (85.6 per cent, see Table 5.1), with a long term partner (61.5 per cent), and to have been employed by their current employer for more than five years (72.1 per cent, 47.1 per cent more than ten years).

*Table 5.1: Ages of the respondents*

| Age of respondent | Percentage of respondents |
|---|---|
| 16 - 21 years old | 14.4 % |
| 22 - 29 years old | 35.6 % |
| 30 - 39 years old | 25.0 % |
| 40 - 49 years old | 22.1 % |
| 50 - 59 years old | 2.9 % |

*N = 104; Missing = 0*

The majority of the respondents earned more than £10,000, with more than 43 per cent of them earning between £10,000 and £15,000 at the time of the survey. (Table 5.2) Less than one in five indicated that they earned more than £20,000 a year.

*Table 5.2: Salaries of the respondents in 1992-3*

| Salaries of respondents | Percentage of respondents |
|---|---|
| <£10,000 | 28.2 % |
| £10-15,000 | 43.7 % |
| £15-20,000 | 10.7 % |
| £20-25,000 | 6.8 % |
| >£25,000 | 10.7 % |

*N = 104, Missing = 1*

The results of this survey will be presented in a different order to questionnaire sections. Having already presented the results of section two it will be followed by the presentation of section one. This will be followed by sections five then four and finally section three. It is hoped that this will make for a more logical presentation.

## section one - job satisfaction

The first section of the questionnaire considered the issue of job satisfaction and attempted to identify what factors were important to the respondents. The respondents were asked to indicate whether the aspects were *important*, *very important* or *not important* at all to their overall job satisfaction. A summary of the results is presented in Table 5.3:

*Table 5.3: How important each of the aspects is to the respondents.*

| | Not Important | Important | Very Important | *Valid Cases* |
|---|---|---|---|---|
| Pay | 0 | 32 | 68 | 97 |
| Job Security | 0 | 19,8 | 80,2 | 96 |
| Number of hours worked | 21,1 | 58,9 | 20 | 95 |
| General Management | 8,4 | 47,4 | 44,2 | 95 |
| Direct supervision | 27,7 | 45,7 | 26,6 | 94 |
| Relationship with supervisor | 6,5 | 48,4 | 45,2 | 93 |
| Bank policy and administration | 3,2 | 67,4 | 29,5 | 95 |
| The work itself | 1,1 | 41,1 | 57,9 | 95 |
| Responsibility and autonomy | 3,2 | 62,1 | 34,7 | 95 |
| Relationship with peers | 3,1 | 54,2 | 42,7 | 96 |

*N = 104*

It is clear from Table 5.3 that all the aspects listed were of importance to the majority of the respondents. Three dimensions stand out though, as the majority of the respondents considered them as *very important*, *The work itself*, *Pay* and *Job security*. It is no surprise that over four in five respondents considered *job security* as *very important* in view of the job losses suffered by the banking industry.

*Table 5.4: How satisfied the respondents were with a selection of work related aspects.*

| | Very Dissatis | Dissatis | Neither | Satisfied | Very Satisfied | *Valid Cases* |
|---|---|---|---|---|---|---|
| Pay | 9,3 | 12,4 | 32 | 34 | 12,4 | 97 |
| Job Security | 13,3 | 24,5 | 28,6 | 24,5 | 9,2 | 98 |
| Number of hours worked | 6,2 | 7,2 | 25,8 | 34 | 26,8 | 97 |
| General Management | 6,2 | 16,5 | 40,2 | 29,9 | 7,2 | 97 |
| Direct supervision | 3,1 | 6,2 | 32 | 44,3 | 14,4 | 97 |
| Relationship with supervisor | 4,2 | 4,2 | 24 | 40,6 | 27,1 | 96 |
| Bank policy and administration | 9,3 | 21,6 | 44,3 | 22,7 | 2,1 | 97 |
| The work itself | 4,2 | 7,3 | 21,9 | 43,8 | 22,9 | 96 |
| Responsibility and autonomy | 5,3 | 10,5 | 27,4 | 41,1 | 15,8 | 95 |
| Relationship with peers | 2 | 1 | 20,4 | 54,1 | 22,4 | 98 |

*N = 104*

The respondents were then requested to indicate how satisfied they were with the various aspects. From Table 5.4 it can be seen that the majority of respondents were *satisfied* or *very satisfied* with the interpersonal aspects of their job (*Direct supervision, Relationship with supervisor* and *Relationship with peers*) and the job specific aspects (*Number of hours worked, The work itself* and *Responsibility and autonomy*). Of some concern is the fact that two of the three aspects considered as *very important* above were considered as less than satisfactory by the majority of respondents. Of course, the reason that the majority considered them as *very important* could be because they are not being satisfied, in a similar process to the one proposed by Maslow (1943). That said, it is clear that *Pay* and *Job Security* are considered as problems for a number of the respondents.

The other two aspects considered as less than satisfactory by the majority of respondents were *General management* and *Bank policy and administration*. This is possibly a reflection of how the staff felt about the job losses and a series of bad results - some as the result of the banks' bad debt problems in South America - which lead to much negative media comment and criticism of the banks. It could also relate to the policies concerning job profiles,

performance related pay, etc., that were being implemented as a result of the shift from a service orientation to a sales culture.

Table 5.5 shows that over 80 per cent of the respondents had noticed a change in the role for bank clerks from *one of service to one of selling*; whilst less than 20 per cent disagreed with the statement "*I am happy at work*". This satisfaction with work is possibly linked to the satisfaction gained from the interpersonal aspects (*Direct supervision, Relationship with supervisor* and *Relationship with peers*) along with the fact that over half the respondents felt that they got *a lot from* their *job*. Over a quarter of the respondents would not join the bank with their knowledge of the system given a second chance, whilst a quarter considered that they were only working for their current employer due to a poor job market, and over 35 per cent would leave *if they could*. Nearly a quarter would "*call in sick*" to attend an interview if the opportunity arose.

Nearly 67 per cent of respondents felt that their banks' directors were being overpaid, whilst only 32 per cent disagreed with the statement: *The bank is poorly run*. Such feelings could be inspired by the problems of job losses and branch restructuring, combined with poor results.

*Table 5.5: How do you feel about your job? How strongly do you agree with the following statements? Percentage of respondents agreeing/disagreeing with each statement.*

| | VSA | Agree | Neither | Disagree | VSD | *Valid Cases* |
|---|---|---|---|---|---|---|
| I get a lot from my job | 15,4 | 39,4 | 28,8 | 11,5 | 4,8 | 104 |
| My abilities are underused in my current job | 19,2 | 29,8 | 28,8 | 17,3 | 4,8 | 104 |
| Others are paid more fairly than me | 8,8 | 13,7 | 44,1 | 25,5 | 7,8 | 102 |
| I would leave if I could | 14,7 | 20,6 | 19,6 | 22,5 | 22,5 | 102 |
| The bank is well run | 2,9 | 13,6 | 35 | 30,1 | 8,4 | 103 |
| My work makes me tense | 8,8 | 25,5 | 33,3 | 15,7 | 16,7 | 102 |
| The bank's directors are overpaid | 39,4 | 26,9 | 26,9 | 3,8 | 2,9 | 104 |
| I feel secure in my job | 6,8 | 20,4 | 31,1 | 23,3 | 18,4 | 103 |
| The bank is poorly run | 10,7 | 23,3 | 34 | 15,5 | 16,5 | 103 |
| I am happy at work | 9,9 | 49,5 | 20,8 | 9,9 | 9,9 | 101 |
| I would "*call in sick*" to attend a job interview with another company | 4,9 | 19,4 | 19,4 | 20,4 | 35,9 | 103 |
| A bank clerk's role has changed from one of service to one of selling | 53,4 | 27,2 | 9,7 | 6,8 | 2,9 | 103 |
| I am only working here because of the poor state of the job market at present | 8,7 | 16,5 | 18,4 | 14,6 | 41,7 | 103 |
| If I knew what I know now I would not have joined this bank | 13,6 | 12,6 | 28,2 | 17,5 | 28,2 | 103 |

*VSA = Very Strongly Agree*
*VSD = Very Strongly Disagree*
*N = 104*

## section five - crime at work

In the last section of the questionnaire the respondents were asked whether they had ever committed any crime and they were provided with a list consisting of both major and minor crimes but excluding violent acts. In total 34.7 per cent of respondents admitted to having committed at least one of the crimes (see Table 5.6). For the majority this involved traffic violations, and despite the fact that a few admitted to several offences the vast majority seemed to be minor in nature. On the whole, bank employees are extremely law abiding, and it is safe to assume that they are more law abiding than the national average[83].

[83]"... Home Office figures indicate that 35 per cent of males will have a conviction for a recordable offence by the age of 35..." The Times, August 6, 1993, p 6.

*Table 5.6. Whether respondents admitted committing offences*

| Type of crime committed. | Number | Percentage |
|---|---|---|
| Substance abuse | 7 | 6.93% |
| Shoplifting | 4 | 3.96% |
| General theft | 3 | 2.97% |
| Pilfering at work | 8 | 7.92% |
| Traffic offence | 32 | 31.68% |
| Other offence | 1 | 0.99% |

*N = 104; Missing = 3*

This hypothesis is supported further if we compare these results with answers given by a group of graduate business students[84] where 65.2 per cent admitted to one or more of the offences cited.

Table 5.7: Offences admitted by a sample of graduate business students.

| Type of crime committed. | Number | Percentage |
|---|---|---|
| Substance abuse | 14 | 21.5% |
| Shoplifting | 13 | 19.1% |
| General theft | 7 | 10.8% |
| Pilfering at work | 20 | 30.8% |
| Traffic offence | 32 | 49.2% |
| Other offence | 3 | 4.6% |

*N = 68; Missing = 3*

Of course comparing a group of graduate students with a working population has a few drawbacks. The most important one is the age factor and the work experience of the graduate student population is another. The latter issue is less of a concern when dealing with M.B.A. students, as the vast majority have had some work experience before attending the course. The issue of age may be mitigated by considering only responses from those respondents under the age of 30 years old in both samples (Table 5.8).

[84]A total of 68 responses were received from graduate business students studying for MBAs. The sample was multinational and responses were received from Asian, European and American students. They were given a questionnaire consisting of sections four and five of the questionnaire given to the main sample along with a section designed to gather personal details.

*Table 8: Responses from those under 30 years of age.*

| Type of crime committed. | Bankers | Students |
|---|---|---|
| Committed a crime | 26.0% | 66.0% |
| Substance abuse | 6.0% | 20.8% |
| Shoplifting | 6.0% | 22.6% |
| General theft | 6.0% | 11.3% |
| Pilfering at work | 8.0% | 26.4% |
| Traffic offence | 24.0% | 49.1% |
| Other offence | 2.0% | 3.8% |
| | *N = 52* | *N = 53* |

[1]*It would have been of interest to gather information on a national basis but initial research into the possibility of this revealed that it would be difficult if not impossible to achieve.*

A follow up question asked whether they had ever considered taking funds, or other assets from their employer. Less than two per cent of bank respondents replied in the affirmative here. This is rather low compared to the response rate of the sample of graduate business students where 20.6 per cent of the respondents indicated that they had considered such action. The low rate for bankers can be explained by some of the comments made by the respondents about the subject. The words honesty, morals/morality, loyalty, trust and upbringing appeared with marked regularity. The following samples are indicative of those received as a whole:

> *It is morally wrong, creating guilt and a feeling of worthlessness. I could not look my children in the eye if I was thieving and endeavouring to bring them up to be honest. (Female, 30 - 39 years old).*
>
> *As we work so tightly as a team, the fear of letting yourself, your colleagues and the [building] society down would be too great. Also, the fear of dismissal and the personal shame would prevent me, together with the guilt! (Female, 22 - 29 years old).*
>
> *Loyalty; Trust; Honesty; Upbringing. I want to keep my job and provide a future for myself, my wife and children. I have unfortunately seen people who could not resist temptation! They got caught! (Male, 30 - 39 years old).*
>
> *The type of trust that people place in you when you handle their money each day. (Female, 22 - 29 years old).*
>
> *People trust you in dealing with all aspects of their finances. (Female, 30 - 39 years old).*

*The majority of people working for the bank are honest and have an understanding of what is right and what is wrong which would prevent them even contemplating the behaviour. (Male, 22 - 29 years old).*

*It is morally wrong to steal, I think that most of us would not be able to live with ourselves or the guilt. Its not how we are brought up. (Female, 22 - 29 years old).*

*Honesty and moral duty when dealing with other people's money. (Female, 22 - 29 years old).*

Other than the content of the quotes, two things are notable about them: the sex and age of the respondents. The majority of people who wrote comments were female; a majority that was out of proportion with the percentage of female respondents as a whole. The comment makers were also mostly under 30 years of age. When we consider the number of females under 30 who had committed a crime we find that only 17.6 per cent indicated that they had. All bar one of the percentages for the six categories of crime was less than half for the male population and no female admitted to pilfering, one jokingly questioned the source of the paper used for the questionnaires! The hypothesis that females might have less propensity to commit crime is well accepted:

*That females commit markedly fewer crimes than males, of a generally less serious character, and are less likely to persist after a first conviction, has been acknowledged by criminologists (with the single exception of Pollak) for most of the past century. Recent work[85] has suggested that women have a lower threshold of shame and guilt than men, and are more prone to 'deviance disavowal' as a result. (Downes & Rock (1988) page 283).*

Downes and Rock go on to suggest that subcultural theories might explain this gender gap. These theories support the idea that females are socialised in a different way to their male counterparts. If it is true that females behave in a different way it will be of interest to see how these factors affect the behaviour of bankers.

When the sample is split into groups depending on the area of work we end up with three groups; two of which are almost opposites. These two groups consist of staff working in the accounts departments, the "computer"

[85]Footnote acknowledges the work of Morris (1964 & 1965)

department[86] and the tills in one group (Juniors) and those working in the lending and securities department with the managers in the other group (Seniors). The Juniors fulfil the functions that a new recruit can expect to do. The tills are considered a promotion in comparison with processing "waste" or entries in the "computer" department, or compared with the menial work involved in the accounts department. The supervisors' and assistant supervisors' jobs are considered to be promotions for cashiers hoping to "climb the ladder". The Seniors fulfil more complex work and their departments definitely represent promotions to those in the Junior group. Most Juniors will not make it to these departments and even if they do they cannot guarantee that they will get to handle the more complicated work involved in the taking of mortgages, etc.

The results revealed that these two groups are distinctly different in profile as Table 5.9 shows:

*Table 5.9: Profile of Junior and Senior Groups*

| | Juniors | Seniors |
|---|---|---|
| Female | 81.3% | 40.0% |
| Male | 18.8% | 60.0% |
| Under 30 years old | 55.5% | 42.0% |
| Time with bank: Less than 5 years with bank | 43.7% | 17.7% |
| Salary: Less than £10,000 | 58.1% | 6.7% |
| Part-time employee | 9.7% | 0.0% |
| | *N = 59* | *N = 45* |

The junior group is predominately female and this will have some effect on the induction process. The early life of a banker, unless on a fast track programme, will be strongly feminine in orientation. It is only once they have been promoted into the senior group that they may expect to be in a more masculine environment with management being the most male dominated area. The results make interesting reading when we review the crimes admitted to by each of the groups, as Table 5.10 reveals:

[86]By computers it is assumed that the respondents mean that they operate computers within the branch. It is doubtful that this would involve more than the inputting of credit and debit entries ("waste") for processing.

*Table 5.10: Offences admitted by the Junior and Senior Groups*

| | Juniors | Seniors |
|---|---|---|
| Committed a crime | 20.7% | 48.9% |
| Substance abuse | 0.0% | 8.9% |
| Shoplifting | 0.0% | 6.7% |
| General theft | 0.0% | 4.4% |
| Pilfering at work | 6.9% | 11.1% |
| Traffic offences | 17.2% | 48.9% |
| Other | 0.0% | 2.2% |
| | $N = 59$ | $N = 45$ |

It is possible to suppose that crime levels are low in the Junior group due to the strong feminine influence that a female majority undoubtedly has. This will have implications for an induction process that positions new recruits into this environment. The majority of staff will spend their time in the Junior group when first employed by a bank. It is only the fast-track entrants who will spend only a short period of time here. The socialising effect should not be underestimated. Add to this the selection process that targets certain characteristics and we may be confident that crime is low because the hypothesis that bank employees are generally moral is well supported. The number of "crimes" confessed by the Senior group is more significant but is not high enough to undermine the strength of the hypothesis.

## factors preventing deviant acts

We should not read too much into the difference in traffic offences as the number of drivers in the junior group is likely to be less than in the senior group. Also the seniors have had more time to commit the other offences. That said, these results are gathered at a time when crime amongst the young is perceived by many to be rising. The absence of any admittance of crimes other than pilfering at work is somewhat surprising viewed against this backdrop. One possible reason for this is the high proportion of females in this group. When asked to score a selection of reasons why they would not commit crimes or act in an unacceptable way the female bankers scored "*The belief that such behaviour is immoral*" at an average of 7.31 - where the

highest score possible was 9 - indicating that is was very important, and "*The knowledge that such behaviour is illegal*" was a close second with 7.30. Their male counterparts scores were 6.38 and 6.49 respectively. The scores for the student group were similar for the first but they did not view legality as important; 5.96 from the females and 5.56 from the males. Based on their scores, male bankers tended to fear being caught and emprisoned more than their female counterparts.

Table 5.11: factors that the respondents considered as important in preventing them from committing deviant acts. The figures given are the averages of the scores given to each factor. A score of 9 indicated that it was the most important factor; a score of 1 the least important.

| | Bankers | *Valid Cases* | Students | *Valid cases* |
|---|---|---|---|---|
| The belief that such behaviour is immoral | 6,95 | 100 | 6,92 | 65 |
| The knowledge that such behaviour is illegal | 6,98 | 99 | 5,71 | 65 |
| Security measures | 3,94 | 99 | 4 | 65 |
| Procedures | 3,23 | 99 | 3,08 | 63 |
| Fear of being caught | 5,82 | 99 | 5,98 | 65 |
| Fear of prison | 5,16 | 99 | 5,4 | 65 |
| What my family would think | 6,29 | 99 | 6,55 | 65 |
| What my friends would think | 5,04 | 99 | 5,32 | 65 |
| What my peers would think | 4,3 | 99 | 4,55 | 65 |
| | | *n = 104* | | *n = 68* |

Table 5.11 shows the average scores for the total group of bankers compared with the student sample. The scores indicated that work procedures and security measures were the least important factors in the prevention of unacceptable behaviour. This is not to say that they are unnecessary, just that they do not factor in the equation for the prevention of criminal motivation for moral individuals.

## factor analysis

From these results it is possible to conduct *factor analysis* to identify general factors that act in the motivation of individuals *not* to commit deviant acts. Using *SPSS*[87] it was possible to identify three factors that were significant[88].

| *Factor Matrix for Bank Employees:* | Factor 1 | Factor 2 | Factor 3 |
|---|---|---|---|
| Procedures | .97084 | | |
| Security measures | .89584 | | |
| Fear of prison | .44746 | | |
| What my family would think | | .96921 | |
| What my friends would think | | .85435 | |
| What my peers would think | | .76377 | |
| Belief such behaviour is immoral | | | .79427 |
| Knowledge such behaviour is illegal | | | .64009 |
| Fear of being caught | | | -.49806 |

*N = 104*

[87]SPSS Inc.

[88]The following instruction was used:

*factor variables = immoral to peers*
*/analysis = immoral to peers*
*/ format = sort blank (0.4)*
*/plot = eigen*
*/print correlation default kmo aic*
*/criteria = iterate 70*
*/extraction = ml*
*/rotation = varimax.*

And for those individuals who had considered taking funds from their employer:

| *Factor Matrix for those who had considered taking from their employer:* | Factor 1 | Factor 2 | Factor 3 |
|---|---|---|---|
| Security measures | .80621 | -.58997 | |
| Belief such behaviour is immoral | -.73770 | -.67438 | |
| Fear of prison | .66501 | | |
| Procedures | .63998 | | -.60383 |
| Fear of being caught | .50202 | | |
| What my peers would think | -.57736 | .60324 | .53439 |
| What my family would think | -.41803 | .50249 | |
| What my friends would think | -.51072 | .46867 | .61073 |
| Knowledge such behaviour is illegal | | | -.50800 |

$N = 15$

The factors for the bank employees are better defined than for those who had considered taking from their employees[89], and they fall into three broad groups. *Factor 1* includes the technical measures designed to deter potential criminals - *procedures, security measures* and *prison*; *Factor 2* includes the interpersonal aspects - *family, friends* and *peers*; and *Factor 3* includes the facts that the action is *immoral* and *illegal*, and with a negative correlation, the *fear of being caught*.

The final section of the questionnaire tried also to investigate potential motives for criminal behaviour by bank employees. To overcome the respondents' inevitable reluctance to admit offending behaviour, the question was worded as follows:

> *"It is acknowledged that the chances of you committing a crime against your employer are very slim, but if you did what do you think would be most likely to motivate you? Please rank each of the following for their relative strength (5 being the strongest motivator; 1 the weakest)."*

[89]This group included all those who had indicated that they had considered taking funds from their employer from all samples, including the business student sample.

The responses indicated that financial pressures would be the greatest motivator; a finding supported by Breed (1979). The average scores indicated that if a friend or member of the family needed money the respondent would be most likely to consider illegal action, whilst personal financial need was second greatest. Revenge scored reasonably highly in this limited selection of motives, suggesting that revenge may play a part in the motivation of some crimes against employers. Many City firms make it standard practice to lock-out sacked employees, thus preventing vengeful acts; these findings suggest that this is a wise policy.

## attitude to crime and deceitful behaviour

Having identified the factors that the respondents consider as important in preventing them from acting in a deviant manner, it is perhaps of interest to consider the actions that they consider as immoral or criminal. This will help identify what is conceived as acceptable action. The respondents were given a list of 21 scenarios and asked to judge them against a base. From the responses it is possible to compile a league table ranking the actions from acceptable to unacceptable (Table 5.12).

| *Table 5.12: Ranking of cases from acceptable 1 to unacceptable 20.* | Student | Main | Pilot |
|---|---|---|---|
| A clerk telephones his girlfriend to tell her he is working late. The call costs the bank £1.47 | 1 | 1 | 1 |
| A clerk uses a word processor at work to prepare her CV | 2 | 2 | 2 |
| A clerk who is on self certified sick leave spends the day writing a computer programme to help a local charity manage its books | 3 | 3 | 3 |
| A clerk uses the photocopier to make 100 copies of his CV | 4 | 4 | 4 |
| A clerk rings his mother everyday. The cost of these phone calls adds £15 to the branch's monthly phone bill | 5 | 5 | 5 |
| A clerk takes a box of envelopes home | 7 | 6 | 6 |
| A clerk is using a computer at work to write a number of computer programmes for his own personal use | 6 | 7 | 7 |
| A junior clerk makes phone calls to a boyfriend in Australia. The total cost of the calls increases the branch's telephone bill by over £100 a month | 9 | 8 | 8 |
| A clerk uses a terminal to increase his overdraft limit without authorisation. He needs the money to pay the rent | 8 | 9 | 9 |
| A computer operator at the foreign department delays payments to branch customers holding the money on a deposit account for a day so that he earns interest on the money at the customers' expense | 12 | 10 | 12 |
| A clerk increases her credit card limit without authority. She needs the money to pay a gambling debt | 10 | 11 | 10 |
| A clerk manages to access the computer system and instructs it to pay one penny of interest due to all the bank's customers' deposit accounts to his account instead | 11 | 12 | 13 |
| A manager transfers £100,000 from a branch sundry account to a large corporate customer's account the day before he must report to his senior manager about the borrowing position of said client, the transfer takes the client below their overdraft limit. The following day he transfers the money back and has the statements retyped | 13 | =13 | 14 |
| A loans officer takes out loans in a false name | 15 | =13 | 15 |
| A clerk uses a terminal at his branch to place money on deposit over night in London in the name of a large corporate customer. He completes all necessary procedures but removes the entries before they can be processed and the customer debited. When the branch receives the interest payment from their head office three days later he makes appropriate entries to credit his account with the £4,000 interest earned | 14 | 15 | 16 |
| Three women attack and mug a man on his way home late at night | 16 | 16 | 11 |
| A bank manager and a junior clerk act together to transfer £1,000,000 via CHAPS and then SWIFT to an account they have opened in South America | 17 | 17 | 17 |
| The Barlow Clowes Affair - the senior official of an investment firm defrauds many millions of pounds | 18 | 18 | 19 |
| Robert Maxwell's misuse of pension funds | 19 | 19 | 20 |
| A man is shot by a terrorist on a train. The terrorist escapes by jumping from the moving train | 20 | 20 | 18 |

*Ignores question 2 as this one differs between the pilot sample and the others*

The top five cases are not particularly surprising. The worst five have a few interesting differences between the three groups. The mugging was considered rather humorous by the pilot sample but a series of news items subsequent to this study removed some of the levity pushing it into the worst five category. The theft of £1,000,000 is there along with Clowes and Maxwell. The media coverage of these two affairs was rather more current when the pilot study was conducted and it is probably because of this that they were considered as worse criminals than the terrorists. Many of the cases were similar to others but differentiated by a small vignette. The closest two cases concerned the altering of personal credit limits. The respondents considered it more acceptable to increase an overdraft limit without authority if it was to pay rent than to increase one's credit card limit to pay for a gambling debt. For some this could be considered as "*borrowing the money*", arguing that they are still liable to repay the sum; the Theft Act 1968 would contradict them as indicated in the *obita* of such cases as *Metropolitan Police Commissioner V Charles 1976*. Surprising, also, was the fact that the activities of the clerk who delayed foreign payments was considered as more acceptable than the clerk who placed a deposit on the Money Markets in the name of a large client , and netted £4,000 interest for himself. In the former case there are clearly customers who suffer as a result of the clerk's activities whilst it is the bank which incurs the loss in the latter case (they have to pay interest on money that does not really exist, or rather exists in two places at once). Perhaps loyalty played a part in the respondents' decisions?

The manager who manipulates the balance of a major customer is considered on a par with the dishonest loans officer by the respondents in the main sample. This is somewhat unfair and probably indicates that many of them did not understand the implications of, or the possible reasons for, his action. Confusion may have been caused by the fact that the case quotes a sum of money - £100,000. It is unclear from the case whether he was concerned for his own reputation with his seniors or merely trying to avoid

putting pressure on his customer. It is of interest to compare the scoring differences between the student sample and the main sample (table 5.13).

| *Table 5.13: Differences between Main sample and student sample. The scores given are the averages for the samples scores using magnitude scaling.* | Student | Main |
|---|---|---|
| A clerk telephones his girlfriend to tell her he is working late. The call costs the bank £1.47 | 1,8 | 2,3 |
| A clerk uses a word processor at work to prepare her CV | 2,7 | 8,5 |
| A clerk who is on self certified sick leave spends the day writing a computer programme to help a local charity manage its books | 8,3 | 12,3 |
| A clerk uses the photocopier to make 100 copies of his CV | 10,7 | 25 |
| A clerk rings his mother everyday. The cost of these phone calls adds £15 to the branch's monthly phone bill | 14,5 | 28 |
| A clerk takes a box of envelopes home | 17 | 38 |
| A clerk is using a computer at work to write a number of computer programmes for his own personal use | 15 | 68 |
| A junior clerk makes phone calls to a boyfriend in Australia. The total cost of the calls increases the branch's telephone bill by over £100 a month | 66 | 78 |
| A clerk uses a terminal to increase his overdraft limit without authorisation. He needs the money to pay the rent | 53 | 170 |
| A computer operator at the foreign department delays payments to branch customers holding the money on a deposit account for a day so that he earns interest on the money at the customers' expense | 178 | 182 |
| A clerk increases her credit card limit without authority. She needs the money to pay a gambling debt | 93 | 186 |
| A clerk manages to access the computer system and instructs it to pay one penny of interest due to all the bank's customers' deposit accounts to his account instead | 174 | 224 |
| A manager transfers £100,000 from a branch sundry account to a large corporate customer's account the day before he must report to his senior manager about the borrowing position of said client, the transfer takes the client below their overdraft limit. The following day he transfers the money back and has the statements retyped | 214 | 257 |
| A loans officer takes out loans in a false name | 302 | 257 |
| A clerk uses a terminal at his branch to place money on deposit over night in London in the name of a large corporate customer. He completes all necessary procedures but removes the entries before they can be processed and the customer debited. When the branch receives the interest payment from their head office three days later he makes appropriate entries to credit his account with the £4,000 interest earned | 234 | 288 |
| Three women attack and mug a man on his way home late at night | 347 | 331 |
| A bank manager and a junior clerk act together to transfer £1,000,000 via CHAPS and then SWIFT to an account they have opened in South America | 813 | 398 |
| The Barlow Clowes Affair - the senior official of an investment firm defrauds many millions of pounds | 977 | 589 |
| Robert Maxwell's misuse of pension funds | 1.000 | 832 |
| A man is shot by a terrorist on a train. The terrorist escapes by jumping from the moving train | 2.089 | 851 |

*Ignores question 2 as this one differs between the pilot sample and the others*

The most interesting ranking is for the clerk who commits the computer-crime when stealing a penny of interest from all the bank's accounts. As most banks have accounts numbering in six figures, if not seven, the sum involved would not have been insubstantial. It is perhaps indicative of the honeymoon the public is still experiencing with the elite computer criminals.

## computers at work

The third section of the questionnaire focused on the opinions of bank employees about computers and attempted to gather some information about the respondents' computer competences and their attitudes toward computers in the work place. Over 70 per cent of respondents agreed that they enjoyed using computers. Less than 31 per cent felt that they had a good understanding of the computer systems that their bank or building society used; over 43 per cent agreed that they had had much experience of computers but only one respondent claimed to write any form of computer programme, and that this was for a computer course taken through the Open University. This last question was asked to gauge the threat that insiders might represent when considering computer exclusive crimes. The majority of employees would have used a computer but only with regard to the inputting of entries on the terminals in the accounts and "computer" departments, or in making account enquiries. The average branch level employee would never get involved in anything more. The managers and seniors might be expected to tackle spreadsheets, but very few will acquire any of the skills necessary to hack or write viruses. At a branch level, the main threat is insiders committing input frauds and computer related crimes, not computer exclusive crimes.

*Table 5.14: Percentage of respondents agreeing/disagreeing with each statement*

| | VSA | Agree | Neither | Disagree | VSD | *Valid Cases* |
|---|---|---|---|---|---|---|
| I have had much experience of computers and their possible applications | 15,4 | 27,9 | 27,9 | 14,4 | 14,4 | 104 |
| Viruses are a major threat to computer users | 11,5 | 22,1 | 56,7 | 6,7 | 2,9 | 104 |
| Hackers are a major threat to computer users | 17,5 | 25,2 | 46,6 | 7,8 | 2,9 | 103 |
| If a colleague used unauthorised software or hardware they should be dismissed | 20,4 | 22,3 | 45,6 | 10,7 | 1 | 103 |
| I would *"turn a blind eye"* if a colleague amended their bank credit card limit using a branch terminal | 5,8 | 4,9 | 10,7 | 19,4 | 59,2 | 103 |
| I have a good understanding of computers | 10,6 | 20,2 | 38,5 | 18,3 | 12,5 | 104 |
| I would alter the balance of my account if I knew I would not get caught | 2 | 2 | 7,8 | 7,8 | 80,4 | 102 |
| Bank clerks are in general honest | 54,8 | 35,6 | 7,7 | 1 | 1 | 104 |
| Computers make my job easier | 52,9 | 35,6 | 7,7 | 3,8 | 0 | 104 |
| I enjoy using computers | 31,7 | 38,6 | 20,2 | 5,8 | 3,8 | 104 |
| I have acquired a good understanding of computers from bank training courses | 6,7 | 16,3 | 30,8 | 22,1 | 24 | 104 |
| I have a poor understanding of the computer systems that the bank uses | 9,6 | 13,5 | 26 | 27,9 | 23,1 | 104 |

*VSA = Very Strongly Agree*
*VSD = Very Strongly Disagree*
*N = 104*

## discussion

There are three aspects to a crime that must be present before the act will be committed: skill, opportunity and motivation (see Figure 5.1). Without all three the act will not be committed. With computer crime the temptation has been to focus on the opportunity aspects of the situation. Security systems can be used to tackle the problem of computer crime by reducing the number of opportunities available to the potential computer criminal. This works to a

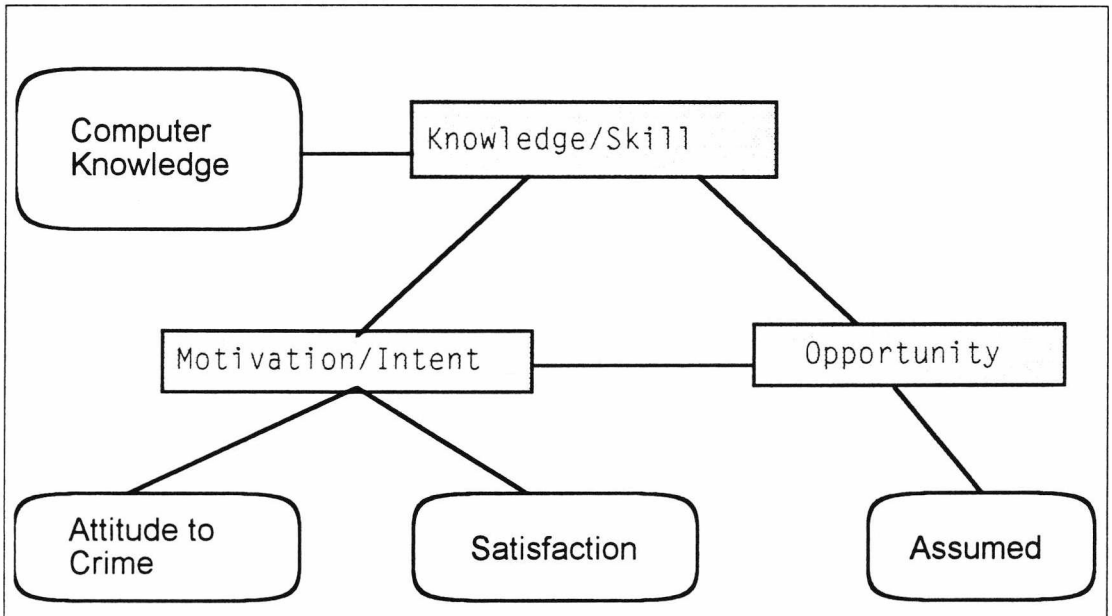


Figure 5.1: Shows the relationship between theTrinity required for a crime.

great extent and it is certainly true that provided that procedures are properly observed that the system will be hard to compromise. These procedures must be supervised and such has been the preserve of supervisors and middle management in the major banks for many years. But with the increasing use of computers these roles are being rationalised, therefore delegating greater levels of trust to junior staff, along with a greater reliance upon computer systems to monitor activities The number of potential opportunities have therefore increased, and yet crime (including computer crime) - although it is difficult to say for certain - does not seem to have responded. Why? The answer seems to lie with the type of staff that have been employed and their moral beliefs. The results of the survey above tend to support the hypothesis that bank employees are moral, law abiding individuals who are concerned about what their family, friends and peers think. The results of the survey also suggest that the main threat is from input frauds or computer related crimes as branch level bankers lack the skills to commit high-tech computer exclusive crimes.

Banks can and do protect themselves against the technical categories of computer crime with varying levels of success Most have been operating computer systems for some years now and spend vast sums of money on

security each year. The security of the systems is important for the credibility of the banks as well as for pure security reasons. A potentially more worrying area of "Attack" though is that of the banks' own staff perpetrating fraud. As it is suggested that insiders could be responsible for 90 per cent of computer fraud[90], this group could represent a much greater threat in the future, and because of their position, can perpetrate their crimes at the low-tech end of the computer-related crime spectrum. Greenburg (1990) suggests that dissatisfied employees offend against their employers. The bank staff questioned may suffer dissatisfaction for a number of reasons:

1. Loss of jobs. Expectation of more cuts.
2. Change from service orientation to sales orientation.
3. Change from salaries to commission based remuneration, or an expectation of such a change.
4. Press criticism.
5. Changes in working practices and new technology.

The loss of jobs plus the fear of further cuts, along with the other four main changes listed above, has had an effect on the attitudes of bank staff. Bank staff had considered their jobs as potential jobs for life in a highly respectable industry; many of their perceptions have been rudely overturned in the last few years. Many now fear redundancy; a move to a sales culture and commission based income; and more technology at work. The indications are that the press criticism is far from over. Rumours at the beginning of the 1990s suggest that it will not be long before the reintroduction of bank charges, even for those customers in credit. This is bound to incite some negative media comment[91].

Many of the major banks' strategies aim to optimise the use of technology. Customers are encouraged to use ATMs in preference to the traditional counter services offered by the banks. Indeed many branches that offer

[90]Bankers' Monthly, April 1989, page 42.

[91]When banks lose money they are criticised; when they make money they are seen as greedy. "*Consider this: Unilever is almost the same size as Barclays; a £10 billion company, making £2 billion a year. But when did you last hear critics sounding off about avaricious Flora-manufacturer plundering the purses of impoverished pensioners?*" Jeff Randall, Agenda, The Sunday Times, March 12 1995, page 2.2.

Saturday morning services now rely on their "cashpoints" or "speedtills", with minimal human support. The clerks present operate as sales or customer enquiry staff. Many banks are now situating ATMs at locations other than branches; they may be found free-standing in airports, on ferries, in train stations, in superstores, etc.

The banks are also centralising many of the administrative and non-sales functions that were performed at a branch level previously. The two most notable areas are those of Securities[92] and Loans, which offered a path to management in the past. A junior clerk could prove their worth in securities with work that required a knowledge of banking and land law, as well as the ability to deal with some of the branch's more influential customers. Success in this department could lead to a position as the head of securities in a branch, or a turn as a lending officer, before gaining a junior appointment as an assistant manager. With all the changes that have occurred such paths are far from clear and now lead to fewer middle management positions[93] (Scase & Goffee 1989).

Banking is a profession and as such involves a high degree of trust. Junior members of staff handle vast amounts of cash every day, or administer the transfer of payments many times their annual salary. They make amendments to account details using computer terminals and in some cases are branch key holders[94]. They all have many chances and opportunities to commit illegal acts, but they do not, in most cases, do so. But, with all the changes, how long will this remain the case?

As the use of computers grows so will the incidence of computer-related crime, it is said that the "probabilities of fraud vary inversely with the technical

---

[92]Also referred to as "charging", involves the perfecting of mortgages, guarantees, and other deeds used to secure the lendings of a branch.

[93]The number of managerial positions is expected to decrease further. Rumours in one of the major banks suggested that as many as 20 per cent of managers would be made redundant, by voluntary means or otherwise.

[94]Whilst able to enter the branch premises after hours a key holder would still require at least a second key holder to access any of the secure areas.

skill necessary to pull them off" (Comer 1985, 142). If we assume that this is so, then we can also assume that the number of Elite or Copy-Cat Computer Crimes will be low. It is most probable that the number of these crimes will be far outweighed by the incidence Computer-Aided Crimes, which require a relatively low level of technical knowledge. The major threat of such crime being probably from insiders.

The situation may be encapsulated as in Figure 5.1 above. The bank employee can be assumed to have a low level of computer knowledge, such that they are unlikely to commit a more sophisticated computer crime without assistance. For reasons that have already been stated, it was assumed that all bank employees have the opportunity to commit crime (although due to their lack of computer knowledge this is likely to be a Computer-Aided Crime) yet they do not. Why? To answer this it is important to consider Motivation/Intent. Indeed it is possible to assume that the Motivation/Intent of the individual is the major factor that determines the frequency of Computer-Aided Crimes.

The Motivation/Intent of an individual is affected by their Attitude toward that relevant behaviour and the individual's Subjective Norms (Fishbein & Ajzen 1975). One particular factor that may be related to their action is the individual's satisfaction with key job related stimuli. Greenburg (1990) shows that there is a possible causal link between employee dissatisfaction and theft at the work place. It has also been said that "[a] loyal staff reduces the risk of fraud" (Collier, Dixon & Marston 1991, page 56). Is loyalty dependent on employee satisfaction? Is it safe to assume that whilst satisfaction may not generate loyalty that dissatisfaction will erode any feelings of loyalty that an individual has towards their employing organisation?

This is arguably as a result of the type of employee profile that banks have sought to meet the requirements of a service culture. What then will happen with a different employee profile, one more attuned to a full sales culture? An

extreme case would be if banks employed only graduate business students. Assuming that the sample taken were indicative of this population as a whole, we would have a situation where there was more chance that the employee had committed an offence of some description. The sample results showed for instance that over 30 per cent of respondents admitted to pilfering at work compared to less than 8 per cent for bank employees. The results also show a greater percentage of respondents who had considered taking funds, or other assets, from their employer. Less than 2 per cent of bank employees had considered such action compared to over 20 per cent of the graduates. These figures could have been higher but for the fact that a group of the graduates had never worked before having enrolled on their MBA course straight after graduation. Of course this does not prove that one group is more criminal inclined than the other. Before too many conclusions may be drawn from these results a number of further questions should be asked of the respondents to gauge whether there are any fundamental differences in what they consider constitutes pilfering, etc.

Another reason for the difference may be to do with the organisations rules and their implementation. Many organisations display a leniency towards certain behaviour that creates acceptance for it; behaviour that would not be considered acceptable at another organisation.. The high level of graduate respondents who had considered taking funds or assets from their employers begs the question of whether there is a link between crime and intelligence; it can certainly represent an interesting academic exercise to "*plan*" a crime against one's employer, but that is not to imply that the thinker is more likely to perpetrate the deed. But more likely it is to do with loyalty and the bank employees' knowledge of what is right and wrong.

It is difficult to say whether crime in banks has increased or not. Banks have been guarded in revealing the information necessary to make such judgements. It is possible to make three conjectures though. First, that the use of more computers will yield more opportunities for abuse. It is true to

say that computer crime has increased with the increasing use of computers, but that is not to say that computers have caused this increase. This rise is due in the main to the greater reliance of many functions, such as book-keeping, on computing. This is also partially a reason for the second conjecture, that the change in bank structures has reduced the middle management layers that were responsible for many of the supervisory roles. This affects the situation in two ways: 1) it increases the chances of avoiding detection as there are fewer supervisors to check on the activities of their subordinates, and those that remain often have other responsibilities; 2) there are fewer promotional opportunities thus increasing the chance that an individual will feel demotivated. A third conjecture is that the move from a life-time employment strategy has created a discontented minority in some banks, which might make them more amenable to deviant activities.

> *As a career in the Bank becomes less likely and the systems are centralised, the opportunity and availability of fraud will become greater. Cost savings mean less work is double checked and supervisors have less time to fully monitor their staff. Junior staff are already adopting an attitude of "I don't care", which I consider will increase. (Male, 30 - 39 years old).*

The banks' senior management have made decisions with the aim, in the main, of providing more effective and efficient services. They must ensure that they communicate their plans to their subordinates and that they make sure that these staff are motivated in a positive manner. They must also ensure that their subordinates are clear about what constitutes acceptable behaviour, especially as they expect them to be more "entrepreneurial" in their pursuit of sales and sales commission, rather than providing a service for a salary; a lesson that Barings have learnt to there cost.

It is possible to suppose that were the respondents on the whole demotivated and that they were also on the whole computer literate that there would be a serious risk of computer abuse by bank staff against their employing institutions. If we now consider Fishbein's model of intent it becomes clear that the demotivated member of bank staff will not act deviantly unless they perceive their actions to be acceptable.

The banks have been very good at employing honest individuals with a strong moral code. It is this moral code that has ensured that the average bank employee is more likely to discover a cure for cancer than commit a crime against their employer, or indeed society at large. In return for this commitment they were rewarded with a job that was theirs until they retired into a bank pension at the age of 60/65. Each year they received a Christmas bonus and profit sharing when the company's results were announced. In return they were expected to be polite and curteous; helpful and neat.

Over the last few years, and one can assume increasingly so in the future, staff have begun to question this "arrangement". Will they also start to question the moral code that prevents them acting in any way other than correctly, and if so, will they act with the aid of a computer?

# Chapter 6
## Computer Misuse

*"Applied Science is a conjuror, whose bottomless hat yields impartially the softest of Angora rabbits and the most petrifying of Medusas." (Aldous Huxley, "Tomorrow and Tomorrow and Tomorrow" (1956))*

*"The fool's crime is the crime that is found out, and the wise man's crime that is not. If I could give you an instance, it would not be the instance of a wise man." Count Fosco in the Woman in White by Wilkie Collins (first published 1859, reprinted 1984 page 254).*

### introduction

The computer, and the system on which it relies, the integrated circuit or microchip, have revolutionised the way we live Since the first vacuum tube reliant computer, ENIAC (built for codebreaking by the Americans during the Second World War) computer technology has advanced at an unprecedented speed. The first computers were vast in size filling many rooms in some cases. They had very little memory and their principle attraction was their accuracy with large calculations. It is inconceivable to think that the technology can advance again at such speed from the present point in time as it has done over the past fifty years.

Computers alacrity and ability to process large amounts of data have ensured that they are now indispensable to modern business. But the principle behind the computer is a simple logic reliant on a series of yes/no switches, or in the binary language it uses, 1/0. These switches are operated by programs which are highly prone to human interference, both benign and not, consequently they may be abused in a variety of ways as this chapter will illustrate. The potential dangers are as yet inestimable. The integrity of payment systems such as SWIFT and CHAPS and many other commonplace systems in business, defence, finance, medicine, traffic control, etc. is of utmost importance for the functioning of developing society. The extent to which we rely on computers is now staggering. Were society deprived of their use the consequences could be dramatic:

*"Not so long ago someone who knew what he was talking about said that if all computer systems were simultaneously abolished the number of people immediately needed - literally*

*the same hour - with exceptionally high skills.. would be 100 million in Western Europe alone.*

*"Science fiction. Put like that, of course. But now add the criminal element and it ceases abruptly and unpleasantly to be anything but plainly possible." (B. Levin "A terminal case of Virus" The Times, January 3, 1991).*

This view is supported by Coldwell (1990) who considers what might happen if integrity of our society's information systems became suspect.

*"It is interesting to think for a moment what it would be like if these sources of information became suddenly devalued because of their unreliability"(Coldwell 1990, page 220).*

Coldwell suggests that it is a possibility should terrorists direct their attention to such an approach and draws a parallel with the Germans' World War II policy of disinformation. Coldwell's essay highlights the effect of information, albeit correct information, on the NY-SE. Some investors actually shot their accountants in response to a particular spate of bad news.

*"One might argue that the stability of the capitalist economic system relies on the reliability of a communication system which is a primary user of information technology." (Coldwell 1990, page 220).*

The computer has brought developed societies many related benefits which it has rightly been applauded for. But there are also related costs, many of which are related to computer abuse and computer related crime, the extent of which have still to be revealed :

*"The police (Royal Canadian Mounted Police) are convinced that crimes perpetrated by the use of computers are far more prevalent than even statistics would indicate. Sergeant Peter Clarke... has stated: "About 85 percent (sic) of computer crime is going undetected..."." (Webber 1984, page 225).*

The calculation of just how prevalent it is is complicated by many factors. In the first place, many incidents are still going undetected. Secondly many computer system managers are unwilling to admit that their security systems have been beaten and are consequently loath to report incidence of such. Thirdly, there is as yet no central recording systems for such incidents.

There are many forms of computer misuse that attract attention from the general public, but there are two in particular that cause more excitement that the others combined, these being "Hacking" and the creation of "Viruses".

## hacking

The term "hacker" is now generally accepted to mean an unauthorised user of a computer system. The media has largely ensured that this meaning is the one understood by the general public. Although the term "hacking" can be more broadly ascribed to activity relating to computer systems generally. the Hacker's Dictionary offers the following definition of the term hacker:

> *n.1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities , as opposed to most users, who prefer to learn only the minimum necessary.*
> *2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.*
> *3. A person capable of appreciating hack value.*
> *4. A person who is good at programming quickly.*
> *5. An expert at a particular program, or one who frequently does work using it or on it; as in a "UNIX hacker". (Definitions 1 through 5 are correlated, and people who fit them congregate).*
> *6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.*
> *7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.*
> *8. (deprecated) A malicious meddler who tries to discover sensitive information by poking around. Hence password hacker, network hacker. See cracker[1] (Raymond 1993, page 218).*

It is intended that for the rest of this thesis references to the term hacker will be with the understanding that it be in regard to meaning 8 above. the main reason for this is that outside "hackerdom" this meaning is prevalent.

The difference was largely academic up until 29th August 1990 when the Computer Misuse Act 1990 came into effect. This act provides for the creation of an offence of "hacking", or more properly "Unauthorised access to computer material" when it states[2]:

> *"A person is guilty of an offence if -*

[1]The Hacker's Dictionary offers the following explanation for Cracker. "n. One who breaks security on a system. Coined ca. 1985 by hackers in defence against journalistic misuse of **hacker** (q.v. sense 8). An earlier attempt to establish *worm* in this sense around 1981-82 on USENET was largely a failure."
[2]Section 1. - (1).

*(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;*
*(b) the access he intends to secure is unauthorised; and*
*(c) he knows at the time when he causes the computer to perform the function that that is the case."*

Up until the enactment of this act the act of "electronic trespass"[3] had not been remediable in law unless the perpetrator had caused damage, in which case prosecutions could be secured under the Criminal Damage Act 1971[4] or the Theft Acts 1968 and 1978. But such an approach was far from successful; of 270 cases verified by the Department of Trade and Industry in the years 1984 to 1989 only six had reached the courts[5]. This highlights the difficulty that the authorities face when trying to prosecute such offences. The new act goes some way to remedy the problems but falls short.

The arguments marshalled against the criminalisation of the act of hacking are various but can be summarised as follows. Firstly, the principle of creating an offence of "electronic trespass" must be questioned in view of the lack of any general offence of trespass. If a trespasser does damage or steals from the premises they may be prosecuted. Likewise under the old law a similar case could be bought against a hacker. The onus should remain with the systems' owners, to whom it can be argued the merely curious hacker offers a service:

*"We get a lot of useful information about gaps in the security of computer systems from hackers, which are often suppressed by manufacturers. Hackers are being made the whipping boys for generally lax computer security." (Alistair Kelman cited in "How a Hacking Law Could Weaken Security" by M. May, The Times, April 20, 1989).*

The problem is that hackers can cause damage (whether wilfully or not) and their mere presence within a system undermines the integrity of that system. Also with the apparent rise in the virus as a major computer problem it could be argued hat even the curious hacker has the potential to cause major damage within systems.

---

[3]There is no general offence of trespass in English law, only a crime of conspiracy to trespass.
[4] As in the case of Nicholas Whiteley. Reported in The Times: May 2, 1990; May 25, 1990, June 8, 1990; February 6, 1991.
[5]Parliamentary comments made by Mr Colvin, reported in The Times, February 10, 1990.

The second problem with the new act is that whilst it creates a "hacking" offence with the provisions of section 1, it fails to offer any measures to assist the police's implementation of it:

> *"Det. Supt. Barry Donovan, of the Computer Crime Unit at Scotland Yard, said the Bill (from which the Act was drawn) was excellent in creating three new crimes "but is sadly lacking in giving us any chance of enforcing them. "One of the several crucial areas in which the Bill fails is in monitoring and surveillance of suspected criminals he said... " (The Times, May 7, 1990).*

The problem revolves around the use of the telephone system. A hacker can commit the new crime from the comfort of their own home. The problem of surveillance need be approached from a difficult angle that that of other crime. As the hacker relies on the telephone system for perpetrating their crime the police's most effective surveillance technique would be to tap their line and monitor the suspected hacker's activities. Here lies one of the problems; the new Act makes no provision for such activity by the police. The police may of course obtain warrants for such activities via other statutes. Also the police have found that British Telecom can be far from helpful at times:

> *"The police, who are reliant on the goodwill of British Telecom, are also finding that requests to trace calls are being ignored and claim that some requests are taking an inordinate long time to process." ("BT policy on hacking criticized by Police" N. Nuttall, The Times, May 28, 1990).*

Part of the problem is that British Telecom have their own investigation team to "police" their own telephone system and have been known on at least one occasion to tell a "victim" that they were wrong to contact Scotland Yard to report a case of hacking.[6]

## blackmail and other similar criminal activities

Many crimes which are executable in a non-computer environment are achievable in a computer environment. In this category sit such crimes as blackmail, eavesdropping and theft of information, each of which are

---

[6]N. Nuttall, The Times, may 28, 1990. See above.

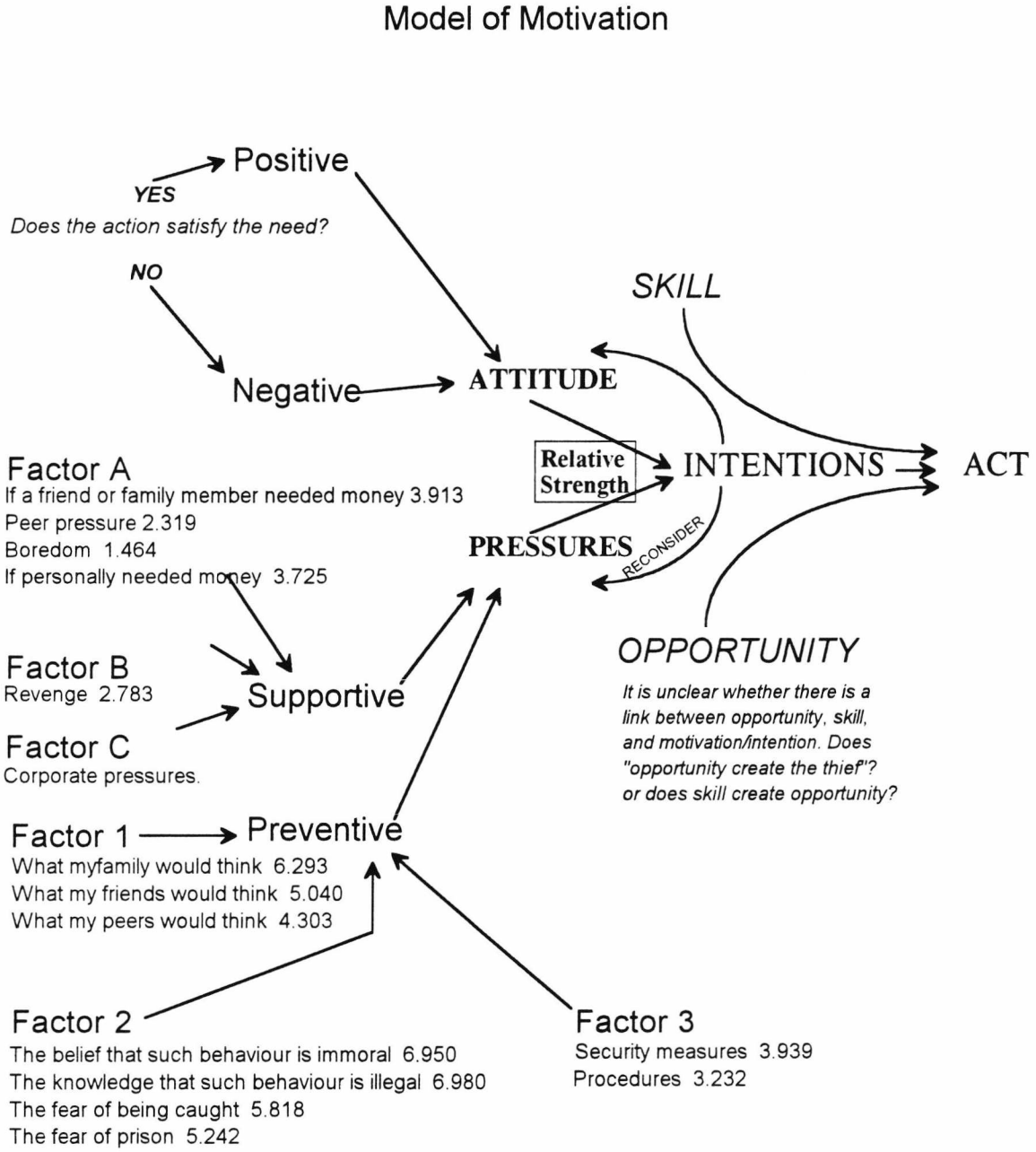



**Figure 9.1: Model of white collar criminal motivation.**
A distinction should be made between "Individual" WCC and "Corporate" WCC. An individual WCC will be motivated by a different set of goals and therefore effected by different attitudes and different. supportive factors, but both will be influenced by similar preventive factors (Factors 1,2 and 3).

arguably easier in the computer environment. The 3½ inch floppy disk can store large amounts of data including photographs, thus allowing those employees disposed to do so the opportunity to steal and sell information to competitors or future employers, or to use for their own commercial

purposes. It is perhaps for this reason that computer abuse by employees is viewed harshly, no matter how apparently innocent the transgression by the employee. Where an employee misuses passwords to gain access to areas of the computer system for which they have no authority their employer is quite within their rights to summarily dismiss them, as held in a recent case.[7]

This is perhaps an area of great conflict. The average computer programmer (whether by occupation or merely by inclination) is an inquisitive type. They are hackers, in the broader sense of the word (see the definition above, meanings 1 through 5 above) and may well cross over the "line" at which normal inquisitive activity threatens the integrity of the security of the system. they acquire access to unauthorised areas, but should they then fear dismissal and possible legal reprisal under the Computer Misuse Act 1990 if they were to bring their achievements to the attention of their employers? If the precedent[8] is limited in its application then this conflict will not rise. The action justifying dismissal is analogous to stealing a key so as to enter a room which is out of bounds; the hacker's action on the other hand would be informing his employers that the doors hinges were weak or that the back door was wide open.

The role of the hacker within companies should not be underestimated. Indeed some companies employ hackers to test their security measures (Lundell 1989). The service they do the systems' security managers[9] is undeniably great. But the risks are also great and nobody likes to feel that their secrets are unsafe. It is for this reason that they are willing to spend large amounts of money on security measures.

In one recent incidence reported in The Times[10] a gang of hackers were believed to have broken through the security systems of a number of leading banks. They then offered to reveal to the institutions concerned how they did

[7]Denco Ltd. v Joinson Court of Appeal case reported in The Times, November 22, 1990.
[8]Denco Ltd. v Joinson
[9]May also be referred to as "sysops", sysadmins" and "admins".
[10]The Times, October 15, 1990.

it in return for money. The report suggested that the hackers had been seeking employment as computer security consultants by the banks concerned so had decided to "blackmail" the banks to realise their wishes.

A case of blackmail potentially more harmful was that of the "Aids Doctor". Dr. J.L. Popp has worked as a medical researcher for the World Health Organisation. He was arrested[11] by the FBI on behalf of Scotland Yard in connection with a fraud in which 20,000 virus infected computer disks purporting to contain educational information was distributed. The disks contained a demand for money, in the form of a cash payment to a post office bow in Panama, in return for an antidote to the virus.

## use of computers for personal use

Parallel with other activities in the work place; use of the telephone for personal use, or the firm's van used to "drop-off the kids" at school on the way to work. Many employees bend the rules to their advantage at some time or other. Some may feel that the have a precedent to do so, arguing that some employers and managers use company property as if it were their own. The boardroom might be furnished in an opulence far above that required for its function. The directors' dining room might serve a cuisine little dreamed of in the employees' cafeteria. The marquees at Henley and Wimbledon are a must for a few as is the debenture at Twickenham. With this kind of example at the head of some corporations it is not surprising if employees "borrow" stationery, or use the telephone for personal calls arguing that "*managers know it will happen and pay people less to compensate. If I didn't use the phone I would be underpaid!*"

It is not that such action should be considered as acceptable but it is understandable if the signals sent by the top end of the employing organisations "encourage" such an action. As has been previously stated in the chapter on motivation, signals are an important element in the motivation

[11]Reported in The Times, February 3, 1990.

calculus. Add to this the fact that many companies never punish the petty abuses, the supervisors often being as "guilty" as their subordinates, and you arrive at a criminogenic environment[12] where the "use" of company property is the norm. The first individual to be punished, should the company "clamp down" can surely feel aggrieved. But is it just organisations that create such environments? Or does society as a whole condone such behaviour, because morality in general has declined[13]?

## viruses

Indubitably the most pressing problem facing computer users of all shapes and sizes are viruses Viruses are basically programs which are run on a system and have the ability to transfer between environments when exchange of software or data occurs. At some future moment the program will be activated causing the computer to run the viral sequence, the output of which can vary from the harmless (a display message) to the disastrous (causing the system to crash or wipe memory drive). The Hacker's Dictionary describes the phenomenon as follows:

> *"Virus... n. A cracker program that searches out other programs and "infects" them by embedding a copy of itself in them, so that they become Trojan Horses. When these programs are executed, the embedded virus is executed too, thus propagating the "infection". This normally happens invisibly to the user. Unlike a worm[14], a virus cannot infect other computers without assistance. It is propagated by vectors such as humans trading programs with their friends (see SEX[15]). The virus may do nothing but propagate itself and then allow the program to run normally. Usually, however, after propagating silently for a while, it starts doing things like writing cute messages on the terminal or playing strange tricks with the display (some viruses include nice display hacks[16]). Many nasty viruses, written by particularly perversely minded crackers, do irreversible damage, like nuking all the user's files." (Raymond 1993, page 437).*

---

[12]Is a crime a crime if the victim is a willing victim?

[13]A Marxist might conclude that this is because we have become more commercial in our personal outlooks.

[14]A worm is a program with the abiliy to propogate itself over a network, no software exchange is required. The program reproduces as it goes and has the ability to fill up hard drives and cause systems to crash. Often referred to wrongly as a virus.

[15]SEX is an abbreviation of Software EXchange.

[16]"A program with the same approximate purpose as a kaleidoscope: to make pretty pictures" (Raymond 1993, page 143-4). Some can be very elaborate whilst others may only consist of messages.

The extent of the problem is unclear. Estimates of the number of different viruses, excluding their variants, range into the hundreds[17] and indications are that the figure is growing[18]. Viruses can cause a computer system to do any number of things. The Armageddon virus from Greece causes the system to dail the speaking clock in Crete. A New Zealand virus which causes a display message calling for the legalisation of cannabis, or the Joker from Poland which displays a message advising that the computer is hungry and needs a hamburger. Various viruses may be written as "time bombs", the most popular trigger being Friday 13th, or in one case Saturday 14th, which attacks a system destroying the file allocation table. Other new viruses are emerging. Names such as Whale, Tiny, Dark Avenger and Frodo abound, and they originate from all over the world.

> *"Tokyo - computer viruses developed by a group of 40 Japanese hackers, including a school pupil, were found in video games software after a warning, officials said." (the Times, May 3, 1990).*

Some viruses are triggered by a sequence of events. Such programs are often referred to as "logic bombs". It is said that such viruses may be used by some software programmers in an attempt to inhibit the copying of their programs[19]. The most notorious case was the "Brain". The Brain virus eventually infected an estimated 100,000 personal computers (Lundell 1989). The software was sold through an outlet in Lahore but the virus was benign unless the software was copied. Many students who bought the programmes allowed friends to copy them on their return to the USE. Other programs may be written so as to attack other programs (Core Wars), or with the ability to protect itself against examinations (Whale), whilst "worms"[20] have the ability to propagate through systems without the necessity of SEX.

---

[17]"David Frost, a computer security expert at Price Waterouse, says he has counted 190 viruses, not including variants." "Friday 13th Virus Alert" (N. Nuttall) The Times, July 12, 1990.

[18]Edward Wilding of "The Virus Bulletin" quotes a sevenfold rise in one year. reported by N. Nuttall, The Times, May 1, 1990.

[19]"Software manufacturers often protect their copyright by inserting a virus or bug into their programme which is activated only when the programme is illegally copied several times." David Young, The Times, April 13, 1990.

[20] Strictly speaking a worm is not a virus and is a potentially more lethal problem. The most infamous worm to date is the "Internet Worm" invented by Robert T Morris Jnr. For a full account of his worm and how it evaded security measures the reader is directed to Appendix

The problem of viruses is potentially the most invidious the corporations' computer systems now face. Viruses and worms have the ability to cause inestimable levels of damage with the costs already running into the hundred-thousands of pounds, if not millions, each year[21]. Corporations must ensure that their procedures and rules regarding the exchange of software are rigorously observed and that the consequences for those individuals who fail to do so are well known by all employees. Many firms have made it a dismissable offence to use unauthorised equipment, whether it be hardware or software. This is action which will indubitably become standard practice in those industries which rely on computers to process their work. The credit card companies have already suffered the consequences of "bugs in the system". On December 15, 1989 Barclaycard suffered such with the result that "many thousands of transactions were processed without the narrative details. It is the first time it has happened in 25 years.[22]" The costs are also potentially high for other, non-financial, industries. The Police, hospitals and other institutions that rely upon records now stored on computer cannot risk the consequences of not having adequate security, with disaster provisions, should the need arise. Disaster management must become as much a part of systems as the security provisions. Files should have back-ups which are isolated from the originals and are stored in such a way that they are not susceptible to attack themselves.

It is unclear exactly what motivates an individual to write a program designed to "vandalise" another program or a computer's operating system. What is clear is that such programs are extremely virulent on the whole and that

---

A of "Virus by Lundell (1989).

[21]"Coopers & Lybrand (C&L)... estimates that Britain's losses from "computer failures and deliberate action against information systems" could have cost £1 billion last year (1989), and that 80 per cent of fraud is by employees." L. Tilley, The Times, January 13, 1990.

"Computer viruses... could be costing businesses more than £5 billion a year. Reported incidents of computer viruses have risen from 3,000 in 1988 to 30,000 in 1990, Norton Antivirus Survey... claims." N. Nuttall, The Times, September 24, 1990.

[22]Spokeswoman for Barclaycard quoted in The Times, January 13, 1990.

unless the users of computers become more aware and considerate of the risks in their practices they could very well become a problem of gigantic proportions. Users must become extremely conscious of the problem when exchanging software and similar activities.

The law has gone only a short way in the redress of the legal inadequacies evident in the area of computer related law and security managers must not get complacent with the creation of a crime of unauthorised access to computer material. The law only criminalizes the act; it in no way prevents it. In some respects hacking is not the problem it used to be and does not require as much attention now as does the creation and circulation of viruses and such like. These rogue programmes have the ability to destroy whole databases and cause untold damage, the extent of which is still to be revealed.

## netiquette

For many years the Internet was a little known and understood metanetwork of military, academic and corporate research departments networks. The Internet was sponsored by the government and was run and maintained by the users for the users. Data traffic was free and took the best available route via the various user networks from A to B. There were theoretically no boundaries to this electronic environment and its size was limited to the computer power of the systems involved. It was a new frontier and the users were only limited by their imagination.

Now commercialism has arrived and many of the original frontiersmen are disturbed by the new uses that the Internet is being put to. There is a fear for some that because of these forces the Internet represents another Lost Eden, that many of the standards that were seen as acceptable behaviour will be ignored by the users, a feeling supported by incidents such as the Green card Incident[23]. The purists have more time for the likes of Robert Morris than

[23] A firm of lawyers in Californis offered their services to anyone interested in applying for a Green Card, or work permit. They did this by making multiple postings on the Internet. Many

the lawyers involved in the aforementioned; at least he had an interest in the system itself.

The Internet now faces the possibility of being regulated with complaints about the information available on the system. Many fear those that seek to use the system for immoral purposes and are calling for laws to protect to innocent. This is something that obviously upsets a society that was built around "an atmosphere of craftsmanship and information exchange" (Press 1994, p. 20). It is a society that has sustained an "open culture" which supports:

> *"open communication. People answer questions, make suggestions, and freely discuss a myriad of topics for the satisfaction of participation and some enhancement to their reputation - the payoffs are not explicit...*
>
> *"I understand that volunteerism and information exchange are difficult to sustain, and commercial enterprises are very effective. The capitalization and blazing growth of the personal computer industry would be impossible by any other means. But, something has also been lost in the "Microsofting" of personal computing." (Press 1994, p. 20)*

## opportunity and security

The question of opportunity is an interesting one. It has been argued that when skill and motivation meet opportunity that a fraud will be committed. This is broadly speaking true but "opportunity" must include not only the opportunity to commit the crime or fraud, but also the opportunity to cover up the fraud (Comer 1985). This is where poor "management" and inadequate procedures assist perpetrators in the execution of their crimes. With this in mind it is possible to say that the management involved in case 22[24] in the Audit Commission's report (1987) were bordering on the incompetent. The accountant who defrauded the company had previously advised the management of flaws in their systems and procedures; flaws he capitalised on at a later date.

---

other users saw this as an abuse of the system and reacted angrily, some even "mailbombed" the host system from where the messages originated.

[24]The case of a professional who warned the managers about a loop-hole in their procedures. When they failed to do anything about it he took advantage of it.

Internal management systems are the best security against the vast majority of computer-related fraud and misuse, as the vast majority of detected incidents are committed by employees (Levi (1986[25]) suggests that three quarters of attempts are by employees). This figure could well be higher:

> *"Coopers & Lybrand (C&L), the management consultancy firm, which made a study, co-funded by the European Commission, into IT security estimates that in Britain, losses from "Computer failures and deliberate action against information systems" could have cost £1 billion last year, and that 80 per cent of fraud is by employees." (The Times, January 4, 1990).*

Figures from a West German study (cited in Wasik 1991, page 61) found that 90 per cent of detected perpetrators were employees of the victim company and that of these, 60 per cent had no special computer skill. They were able to commit their computer-related crime because they knew the flaws in the procedures.

In the Audit Commission's report (1987) each case is followed by a summary of the flaws in the system that allowed the fraud. From these it is possible to suggest a short list of those measures that should form the heart of any effective security system:

- Adequate division of duties - the authorisation, input, and checking of entries should be undertaken by different individuals for instance;
- Output verification by users - users should confirm entries, this avoids the possibility of output manipulation;
- Adequate control over access to data files and programs[26] - measures should be employed to ensure that programs are difficult to retrieve and alter except by authorised individuals;
- Ensure that input documentation is completed in such a way that it does not allow easy alteration[27];
- All transactions should require authorisation and such authorisation should be checked;
- Suspense accounts should be ratified on a regular basis and those items outstanding should be investigated;

---

[25]"The Incidence, Reporting and Prevention of Commercial Fraud", Summary of Findings, Cardiff: dept. of Social Administration, 1986, cited in Wasik (1991).

[26]See section on passwords.

[27]In banking law there is now the possibility for banks in cases involving cheque fraud to claim a partial defence of contributory negligence where an individual completes a cheque in such a way that it allows the perpetration of a fraud - Lumsden & Co v London TSB (1971) 1. Lloyd's Rep. 114;9 LDB 198 and s 47 Banking Act 1979.

- Reliance should not be put on one individual. It is important that more than one person have access to the system and that they are conversant with the programs. These individuals where possible should be independent;
- Errors should be checked and investigated where necessary;
- Passwords should be frequently changed. They should not be easy to guess or widely known. Where they are used the access system should prohibit further use by an individual who attempts to "guess" the password and fails three times say; and
- Comparison of file contents against the transaction and file dump.

All of the above measures should be known and understood by the employees. staff should be adequately trained in their use and the systems should be properly supervised. Where staff are responsible for certain functions they should be allowed a "holiday" from their duties. This allows others to become conversant with the necessities of the post and also ensures that any irregularities may be highlighted.

Of course the above measures aim to stem the fraudulent activities of the insiders; what of the outsider, the hacker who accesses the system from a remote location? What measures can be employed to stem their attempts to "break-in"?

## security hardware

> *"... the evidence is that the vast bulk of unauthorised access to a computer occur in circumstance where quite inadequate security precautions have been taken. It is relatively cheap and simple to install these defences, which will effectively deter the majority of attempts to gain unauthorized access." (Wasik 1991, page 43).*

The measures available to help secure the system are many in number but not totally "hacker-proof". Only an isolated unit with no connection with other systems can be completely safe from the devious activities of outsiders. The lack of connections must be absolute and any employee who uses unauthorised software or hardware will often be summarily dismissed. These apparently draconian measures are necessary if the system is to stay virus free. There is as yet no computer equivalent of the condom[28]! So what

[28]Virus software is now available that screens software for recognised viruses and sequences contained within them. This is more akin to a vaccination as the software will not identify new viruses unless they contain a previously identified sequence.
Networks may protect themselves from outside threats by means of "firewalls". This is a

measures may the managers of open systems install to ensure that hackers are not allowed to run riot through their systems?

## passwords and other log-on measures

The first measure is a simple one and that is that passwords and log-on details be changes frequently. In the case of Gold and Schifreen[29] the defendants had gained access to a number of electronic mailboxes run by Prestel because the passwords were extremely easy to guess (eight 2s then 1234). Hackers are also able to "guess" more complex words with the use of electronic dictionaries that are used so that all words may be tried systematically[30].

Secondly a system could be installed which returns the call of any user after log-on. The user would call in requesting access to the system, they would complete an initial log-on and the computer would then disengage and call the predesignated telephone number. This would ensure that only authorised users would have access to the system. Unauthorised users would not be granted access and even if they are their attempt would fail when the computer failed to ring them back, ringing instead the pre-designated number for the user it thought had requested access.

## checksumming

The third measure is a far more sophisticated measure. the method called "Cryptographic Checksumming" is used to identify data that has been caused to lengthen by the addition of a virus to the program code:

> *"When a virus enters a computer it causes data to lengthen. Cryptographic checksumming defines a healthy level of information carried by a computer and alerts operators to the increase in data which occurs when a virus enters." (The Times, May 1, 1990).*

---

computer that limits traffic between two networks those reducing the chances of "attacks".

[29]Gold & Schifreen v R. (1988) AC 1063.

[30]"Victim of computer hackers fights BT over £8,000 bill" N. Nuttall, The Times, July 1, 1991.

Such a measure is designed to combat the threat of viruses which, as already stated in the previous chapter, could be a very major threat in the next few years.

## passive and active attacks

Security breaches in computer communication systems may be defined as either "passive attacks" or "active attacks" (Muftic 1989). In a passive attack the intruder, or cracker, only views information and data, identifying other parties using the system and analysing their operations. In an active attack the intruder will attempt to alter, steal or delete data; they may also rearrange the stream of messages between parties using the system ("message stream modification attacks" (Muftic 1989, page 22)) or in some cases discard messages completely ("denial of message service attack" (Muftic 1989, page 22)).

Passive attacks, whilst easier to detect than active attacks, are harder to prevent. Measures are available to minimise the consequences of such attacks though. Muftic (1989, page 31) lists the following:

> *message content protection;*
> *prevention of traffic analysis;*
> *subliminal channel;*
> *digital pseudonyms.*

For the more malign active attacks on communication Muftic (1989) suggests the following:

> *Message Stream Integrity*
> *Continuity of Communication Process*
> *Authenticity of Associations (Peer-to-Peer Authentication).*

Computer communication systems are very important within a financial sector reliant on payment systems such as CHAPS and SWIFT. Corporations must also protect their databases from attack, especially within the Banking Industry where the "Duty of Secrecy[31]" is one of their fundamental principles.

[31]See Tournier v National Provincial and Union Bank of England (1924) 1 KB 461.

the number of services available to do this are many. Muftic (1989) lists the following seven:

> *Data content protection*
> *Access Control Security Services*
> *Security-consistent Flow of Data*
> *Prevention of Inference of Individual Values*
> *Consistency Control of Database (Value-dependent Restrictions)*
> *Context-oriented protection (History-dependent Restrictions)*
> *Controlled Information Generation. (Muftic 1989, page 35)*

Most security measures are about limiting the access achievable to that level of authorization conferred upon the user, the principle of "least privileges" whereby users are given minimum access rights (Muftic 1989, page 100). Files should be located within such a system to ensure that they are as secure as they need be. The measures discussed above are to be with the procedures adopted within the system for the protection of the communication systems run and the databases maintained within the systems. Of a far more mathematical nature is the application of Cryptography for the security of the systems.

## cryptography

> *"Cryptography plays an important role in the security of computer networks. Each cryptographic algorithm depends on the security of the keys it uses, so the management of the cryptographic keys require special attention. Key management involves generation, distribution, storage and regular changing of cryptographic keys... Because a key becomes more vulnerable the longer it has been used, data encrypting keys[32] should be changed regularly. It is advisable to change the key at least once per session..." (Muftic 1989, page 46).*

The two main types of cryptographic systems are Symmetrical and Asymmetrical. In a symmetrical cryptographic system the enciphering codes are one and the same (or determinable from each other). It is very important therefore, that the keys for such systems are secure if the system is to maintain its integrity. The most popular symmetric cryptoalgorithm is the American Data Encryption Standard (D.E.S.). D.E.S. is the standard recommended for use in the design of the encryption units used by non-military Government Agencies and by the American Bankers'Association

[32]For the protection of data. The other type is the key encrypting key for the protection of the keys.

(Muftic 1989, page 47). The Asymmetrical cryptographic system relies on two keys which are not mutually determinable. The encrypting key may be made public whilst the decrypting key must be secure. For obvious reasons therefore this system would not be used for the transfer of electronic payments unless both keys were secure; it would be unwise to rely on a system in which anyone could "initiate" payment instructions.

Just as important for the security of a system as the cryptoalgorithms is the secrecy protocol or the key distribution protocol. How the key to the cryptoalgorithm is distributed is just as significant for the security of the system as is the strength of the cryptoalgorithm[33].

> *"the strongest encryption system is useless if the encryption keys are stored on vulnerable computers, or implemented in the form of weak passwords. The bottom line is the threat model underlying most security work which was largely inappropriate to that of any non-top-secret-spare-no-expense-on-security environments." (Ganesan & Sandhu 1994, page 30)*

This threat model was originally developed for the defence industry and assumes that attacks on the system will be technically sophisticated, and yet of "the hundreds of documented failures of ATM security... only two involved such attacks" (Anderson 1994, page 34). ATMs, or automatic teller machines, rely on encryption techniques to secure the user's PIN, or personal identification number. Anderson claims that the development of security systems for such processes has been slow because of a lack of feedback. Cryptographers require information about failures so as to be able to design better systems and to improve protocols. Whilst there have been obvious weaknesses in some of the cryptoalgorithms and protocols used they do not represent the major threats for the banks'ATM system managers:

> *"The three main causes of phantom withdrawals[34] did not involve cryptology at all : they were program bugs, postal interception of cards, and thefts by bank staff." (Anderson 1994, page 34)*

---

[33]Can be "unconditionally secure", "computationally secure", "provably secore" or "insecure". (Simmons G.J. 1994, page 56).

[34]A withdrawal from an account, using an ATM, that the account holder claims they did not make.

The weaknesses in ATM systems having been exploited by a number of innovative criminal gangs in many countries. Anderson offers a number of examples whilst Rushkoff (1994) recounts how he spent an evening with one gang in Marin County, California. The gang used a video camera in a van to record PINs and a:

> *"card reader just over the slot where you normally put your card in. It's got a RAM chip that'll record the ID numbers of the cards as they're inserted. It's thin enough that the person's card will still hit the regular slot and get sucked into the machine". (a gang member, Rushkoff 1994, page 76)*

The gang then use the information from the RAM chip and record it on to blank cards. In this case they used hotel keys that have a similar magnetic strip on the back. The gang had purchased them, along with the encoder, from a surplus store who had in turn purchased them from a hotel that had gone out of business. Such exploits are becoming more common and it is no surprise that at least one of the major banks in the UK saw fit to warn its cutomers not to use their ATMs if they saw anything strange.

> *"We found that almost all attacks on banking systems involved blunders, insider involvement, or both. High-Tech attacks are rare, and the two that did occur were possible because in one case PINs were sent in an obvious manner, and in the other the authorization responses were sent; so these can be seen as the effect of the absence of security rather than some particular problem with it". (Anderson 1994, page 37)*

## physical protection methods.

Whilst it is quite clear that internal system security can be quite comprehensive many institutions are prone to "attack" from a more physical location. Computers give off electromagnetic radiation (E.M.R.) which may be picked up with quite simple "spy" equipment similar in nature to that used by television detector vans. This radiation may be converted into a visual image allowing the eavesdropper to monitor the inputs and outputs of the user. Such an operation in itself is not illegal as they are merely translating data which has effectively leaked from the system. It is important for systems requiring utmost security to prevent this leakage.

The Tempest system has been used by some military and government installations in the United Kingdom and provides complete screening, but at a price (Wasik 1991, page 47). Pilkington have designed a new type of window pane which blocks leakage of data via E.M.R. The window panes consist of : "...two panes of coated glass... stuck together as a laminated sandwich and electrical connections are made between the layers and the walls of the buildings creating a Faraday[35] cage with no holes".[36]

## conclusions

The security measures mentioned above are but an introduction to an industry which is growing as the, as yet unsubstantiated, fear of computer abuse and crime rises. Only isolated systems which are free from any contact with other systems can be free from internal intrusion but they may not be safe from interference by more physical means.

As yet the full risks of abuse are unknown, although the consequences of such abuse are public knowledge with much talk of viruses, worms and the like. There is also a tendency to blame them for systems failures, whether justly or not.

It is possible to purpose a system or security that includes good organisational method and systems as well as a dependance on HRM or more particularly MTM - Management Through Motivation. Ensuring that the organisational systems do not allow "gateways" supported by a H.R. policiy that attacks dissatisfaction may be more effective than a fortress approach.

---

[35]Michael Faraday (1791-1867) is responsible for the discovery of electromagnetic induction and the classical field theory (as well as Benzene).
[36]P. Wright, The Times, April 12, 1990.

# Chapter 7

## Survey to gather experienced computer users' opinions of the motivations and characteristics of hackers/crackers.

*"In the Country of the Blind the One-eyed Man is King." H.G. Wells, The Country of the Blind.*

*"As you read these words your computer or communications systems may be under attack. If your personal or corporate cyberspace has been penetrated, what damage could a malicious intruder cause? Destroy your records? Steal the customer records and sell them to your competitors? Intercept communications between your troops during battle? Forge your digital signature? Alter your credit or medical records?" Ganesan & Sandhu 1994, page 29.*

### survey

The purpose of this survey was to highlight some of the issues involved in the hacking/cracking debate. Its methodology touched upon a nerve for some of the recipients of the questionnaire which was e-mailed to some 400 potential addresses. This second survey considers the problem of computer misuse, in particilar the problem of cracking. To address this issue a questionnaire was devised which asked questions of computer professionals around the world. this questionnaire was then e-mailed to every address on the list of contributors in The New Hacker's Dictionary (Raymond (1993)). The responses were very encouraging on the whole but included a number of negative comments alluding to misuse of the Internet. Such comments make interesting reading when considering the question of the Lost Eden.

The main purpose of this second piece of research was to identify dimensions associated with the committing of computer crimes, or more appropriately the committal of acts of computer deviance as crime per se is measured by law whilst deviance need not necessarily be illegal. the purpose of trying to uncover the dimensions involved was to show that on the whole they were incongruent with the average bank employee. this allows us to make the assumption that the average bank employee is not likely to commit a pure computer crime or computer exclusive crime. That is not to say that they will not commit a coputer crime just that it is unlikely to be of the category of crimes that require a high level of computer knowledge. They are

more likely to commit a computer crime that falls into the category of frauds known as input frauds.

> *"Computer abuse is committed by people, not technology. Understanding the technology is less important than recognising the importance of the application of fundamental control process." (Audit Commission 1994, page 4).*

The issue is discussed further in other chapters.

## methodology

The questionnaire kept short on purpose and used five open questions with supplementary questions where appropriate. The questionnaie was ftp-ed to UNIX then e-mailed to the addresses of all the contributors to the second edition of "The Hacker's Dictionary". It was felt that this list represented a cross-section of experienced users who had at least a reasonable level of knowledge of the issues involved. E-mailing allowed a cheap and efficient distribution process which would have been very expensive to duplicate without the aid of UNIX and the Internet. In total between 300 and 500 potential participants were approached. The exact number is unknown as many of the addresses listed may have become dormant and a number of the accounts closed.

Two important issues were raised by this approach. Firstly, was it ethical to use the "thank you" list at the back of The New Hacker's Dictionary, and secondly, should the questionnaire be e-mailed directly, or following a request for volunteers? The first issue is still grey, even in the mind of the author who has had quite a time to mull it over. Much time was spent thinking about and discussing this topic before any action was taken. It was decided that the list of Internet addresses represented a valuable resource which would be hard to duplicate in physical form. Also, if the survey was successful, the information gathered would be useful to the computer community as a whole. The second area is also still grey and will probably remain so for quite some time. The problem is one of cultural clash between

the computer community and the commercial world. E-mailing questionnaires represents an exciting step for social scientists and the like as it represents a fast and efficient way of collecting data for a fraction of the price of other communication systems. The problem is that such mail may also have a striking resemblance to junk-mail for the unwilling recipient. the survey thus received a number of negative responses. Some were polite:

> *I'm sorry, but I decline to answer this sort of questionnaire, unsolicited, over the net. EM*
>
> *I don't exactly appreciate such unsolicited junk mail. I would be grateful if you didn't send such things to me again. Thank you.*
>
> *Please keep surveys out of my mailbox. I have no interest whatsoever in answering them. I don't know who told you that it is perfectly acceptable to ask questions about illegal behaviour, but I find it offensive.*
>
> *I do not appreciate people sending me crap in my mailbox that I didn't ask for.*

Some not so polite:

> *Please go away and do not bother me again.*

And some not worth repeating here.

A number of recipients e-mailed the sysop at the University of Kent at Canterbury, from where the e-mailed messages containing the questionnaires originated, to complain. this prompted the following communications:

> *1. Subject: Unsolicited Email complaint*
>
> *We have received a complaint from a user at another site that you are sending out unsolicited Email ("junk mail") to "random" addresses. Whilst I understand that this questionnaire may be important to your research can you please be more careful about who you mail to. It is much better to send out a request in a suitable public forum (such as a suitable USENET newsgroup) then to mail people directly with a whole questionnaire.*
>
> *There may also be questions concerning the data protection act if you are intent on keeping answers on computer. Thanks,*
>
> *2. Subject: Another complaint about your Email questionnaire*
>
> *We have received another complaint about your unsolicited Email questionnaire. Please do not send out any more unsolicited messages. If you do so then we will have to withdraw your account.*

*Thank you,*

On the receipt of the second of the above two messages the survey was complete to the end of the first phase[37] of stage one but a second stage was planned and was subsequently cancelled to comply with the above requests. This second stage was to be the continuation of the Delphi Study mentioned in the introduction to the questionnaire. Whether the sysops threat to withdarw the account was a reasonable one is perhaps easy to answer when you consider the response of a few irate Internet users during the Greencard Incident (see Chapter 7). Annoyed by what they considered an abuse of the Internet, they "mailbombed[38]" the host system from where the messages had arisen, causing it to crash.

The issue of junk-mail is merely the tip of a debate concerning the Internet and its use. Some of the respondents suggested that the survey was of value but that its place was in a "Usenet" where volunteers could respond. this is a valid point but would undermine the validity of the survey as little can be done to assess the experience of the respondents. Using the list of contributors ensured that most of the respondents would have been users for a reasonable period of time and were of a reasonably high calibre; they are, it is hoped, mostly serious-computer users rather than Windows-users and game players who may have a knowledge about the topics addressed but do not necessarily have the expert knowledge required.

## the questionnaire

As the questionnaire was unsolicited and was to be e-mailed to many addresses it was kept short and started with the following request:

> *Please could you help me with a Delphi study I am conducting as part of work for my PhD. I would be grateful if you could answer the following short questionnaire:*

---

[37]Response rates may be improved by sending a reminder to all potential respondents who are still to reply. The response for the econd mail-shot is often as good as the first so that an initial 20 per cent response rate may be improved to an overal 36 per cent response rate. This second phase was not available for this survey because of the sysop's "threat".

[38]Where a user sends multiple e-mail messages to another user or system. the massive number of messages causes the system on which the account is held to crash.

A balance between politeness and brevity was sought, it was impossible to explain in detail the purpose of the survey and to address some of the issues that might arise from the methodology used. In turn, each of the questions has its weaknesses, although many of these are due to their generally open nature. These weaknesses could have been addressed but only, it was felt, with the creation of others.

## question 1 & 2.

*1a. How long have you been using computers?*
*1b. What major operating system, such as UNIX, would you say you are most experienced with?*
*1c. Are you male or female?*
*2a. Have you ever hacked into a computer system on which you do not have authorised access? Your answers will be treated in strictest confidence!*
*2b. If YES, do you feel that your activities were ever illegal?*
*2c. Immoral?*
*2d. Do you feel that such activities fulfil a positive purpose?*

Questions 1a and 1b were used to gauge more precisely the length of experience of the respondents. It would have been preferable to test their experience in other ways but this was precluded by the fact that other methods would have seemed "nosey" or too time consuming for the respondents to "bother" answering. As it was some still found reason to complain.

Question 2, and its supplementary questions, was not intended as the main question of the survey. It was asked to gather further information about the respondent's experience of using computer systems. It was not asked as an opening question for a "list of confessions" and the auther did not expect details where the respondent indicated that they had cracked a system. A number of respondents did qualify their reponses though, a few claiming that they had cracked systems as part of part of tiger teams, or individually, in an attempt to identify security weaknesses at the behest of the sysop. Question 2a offered the respondent confidential treatment of their responses. This was

with regard to the treatment of the responses. As a number of respondents indicated, complete confidentiality is impossible on the Internet:

> *Addendum: *NOTHING* on a computer, or on a computer network, can be treated "in strictest confidence," unless it's been prime-key encrypted using a larger key than any potential hostiles have the computing capacity to break. Your assertion of confidentiality denotes either specious intent on your part, or limited familiarity with system and network security. (male, over 30 yrs exp, UNIX, yes (but paid to do so as part of security evaluation procedures).)*[39]

Others showed a streak of paranoia, and sometimes humour, in doubting the offer of confidentiality:

> *Why should I trust you to keep a confidence? I've never heard of you. Are you an AI program at the NSA? (19, male, 45 yrs exp, Unix, ?.)*
>
> *(This is a silly question, isn't it? Why should I trust a "strict assurance" from someone I know nothing about? And why should you trust a reply negative OR affirmative from someone you know nothing about? I was seriously tempted to answer "Yes, thousands of times...", just for the fun of it...) (36, male, 25 yrs exp, unix, no.)*
>
> *By the way, if I had anything juicy to reveal, the assurance of strict confidence from a stranger out in netland would not carry a whole lot of weight. (55, male, 29 yrs exp, Unix, no.)*

Two points must be made in this regard. Firstly, the respondents' addresses and names are not attributed to any quotations cited and no attempt has been, or will be made, to ascertain the true identity of their authors. Secondly, it is very doubtful that a conviction could be secured for an activity confessed by one stranger to another over a network especially as no specifics are quoted.

## question 3.

> *3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)*
> *3b What would you say their main motives are?*
> *3c What percentage of crackers are male?*
> *3d Do you feel that their activities are beneficial or harmful to society? & 3e Why?*

---

[39]Each quotation is followed by information about the respondent's gender, years of experience (yrs exp), which operating system they prefer/use most frequently, and whether they have ever crack a system.

This was intended as the most important area of the questionnaire. When the survey was originality devised it was intended that the answers given to these questions be used to create a structured questionnaire to garner further information concerning the characteristics and skills considered most important. this second stage of the Delphi Study was cancelled for the reasons noted above so the results given below are based merely on the first stage. Whilst this is regrettable it does not undermine the value of the results by much.

The term "cracker" was used to distinguish it from the more traditional definition for "hacker". Hackers are more than systems crackers, they are more interested in the operation of the system than anything else[40]. Levy (1994) refers to them as the "heroes of the computer revolution" in the title of hid book on the subject. the media has taken this term and used it for a very narrow area of activity involving unauthorised access to computer networks and systems. It was as an attempt to save the term from the misuse that cracker was coined. this misuse is possibly as a result of the crackers themselves using the term "hacker". they may have a claim to it but that would only further cloud its definition. Levy (1994) indicates that there have been a number of distinct generations of hackers whoc have contributedto the evolution of the computer. Each generation is distinctly different from the others. In deference to the early generations of hackers the term cracker is used for those who attempt to gain unauthorised access to computer systems.

These questions aimed to build a profile of a cracker. The responses, it was hopes, would highlight the characteristics of those members of the computer community who deviated from what was considered as acceptable behaviour.

---

[40]Although that does not mean that hackers cannot be crackers also.

## question 4 & 5

*4a What activities would you class as Computer Crimes?*
*4b Do you have any examples of such?*
*5 Do you have any further comments that you wish to make?*

These final questions were asked as a means of gathering further background information on the subject. Many respondents felt compelled to maintain the confidentiality of their systems and refused to reveal information regarding cases of security breaches involving their present or former employers. Such loyalty is commended. Some have argued that security may only br improved with a better structure for information sharing regarding deviant behaviour. The flip-side of this argument is that such databases of abuse offer future offenders an insight into what is available. Whether the answer is greater information and readiness to prosecute or not is still very much a debate in progress.

## results

E-mail messages containing the questionnaires were sent to all the contributors listed in the back of "The New Hacker's Dictionary" (Raymond 1993). A number of messages were received from postmasters indicating that the account that the message was addressed to was no longer current. A total of 326 messages were sent to potentially current addresses, although, as noted above, some of these could be dormant.

Seventy responses were received of which 60 were constructive rather than messages of annoyance at having been sent "junk-mail". Of the positive responses, 52 were from males, six from females and two from individuals who did not indicate either way. Forty-three of the respondents indicated that they used, or had more experience of the UNIX operating system, four indicated that they used MS-DOS, three Mac DOS, and ten that they used another system such as Novell or VMS. When asked how long they had been using computers for more than 15 years. This would seem to support the

argument that the list of contributors represented a list of experienced users whose opinions would be of value.

Of the 60 respondents 23 claimed that they had cracked a system at one time or another. A number mitigated their actions by claiming that they had done so at the express wish or desire of the sysadmin or authorised user. At least one respondent claimed that they had cracked into the system when the action was not strictly legal. The question of illegality has been, until recently, a cloudy one. the issue in England has been partially addressed by the Computer Misuse Act 1990 which makes it an offence to access computer material without authority. Whether it is immoral to access computer material without authority. Whether it is immoral to access a system is far from clear on the other hand.

The debate about morality falls into five broad categories:

1. The end justifies the means;
2. For the sake of knowledge;
3. Increases knowledge about computer security weaknesses;
4. The cost to legitimate users and system operators; and
5. Why should people have to lock their doors.

## 1) the end justifies the means

As long as the intentions of the individual are honourable then so are their methods. One respondent indicated it was acceptable when emergencies arose whilst another drew an analogy with an office environment when questioning the term "authorised":

> *Have you ever had to break into someone's desk to retrieve a vital document they accidentally left there before going on vacation? (61 male, 12 yrs exp, unix, yes, no, no, yes.)*

A second likened being able to "crack" to being able to "lock-pick":

*It is a good skill to have, when your friends lock themselves out of their computers, but I would not hack into someone's account any more than I would break into someone's home. (72, female, ? yrs exp, unix, yes (but with an authorised users permission))*

This respondent goes on to criticise what she refers to as "sporting hackers" who hack with no end in mind other than the fun of eluding security systems.

## 2) for the sake of knowledge

This reason is becoming somewhat redundant with the greater availability of computer processing power to a greater number of people. There are fewer reasons now why an individual needs to crack a system to gain access to the opportunity to use a mainframe and gather more information about its use and operation.

*When I was doing cracking back in the mid 80s, it fulfilled a purpose in that I didn't have access to the types of machines that I wanted access to. So, it filled a gap. Unfortunately, I didn't learn as much as I had hoped I would. (77, male, 18 yrs exp, unix, yes, yes, no, yes.)*

Individuals may still feel the urge to crack but they have fewer reasons to justify their actions. They may still crack as a means to gather information but it is more likely to be information of a very different nature than that relating to computers and their operation.

## 3) increases knowledge about computers' security

Some argue that by having benign crackers around improves security. They argue that they should be encouraged to find weaknesses and holes in security systems and to report them to the sysops and sysadmins concerned. This helps to ensure that the systems are as secure as they can be thus minimising the risk from malign crackers.

This argument has a similar basis to the logic of the tiger teams used to test security for many companies and universities. Such teams keep logs of their activities and audit their findings with the sysops so that improvements may be made.

## 4) the cost to legitimate computer users and operators

The opponents of the previous argument would propose that if security requires testing then it should be achieved through the use of tiger teams and the like and not through the encouragement of sporting hackers and crackers. Any intrusion, they argue, no matter how benign, costs time and money as sysops must check for damage. The intruder's mere presence, regardless of activity or intent, undermines the integrity of the system. Integrity is paramount in systems where money or people's well-being is involved. Modern life is extremely dependent on computer power.

The proponents go on to argue that in wasting the sysop's time, crackers are preventing them from considering ways to improve the operation of the system in other ways.

## 5) why do we have to lock our doors?

> *I grew up in a society where someone could go away for several weeks and leave their house unlocked. It was not even a consideration that someone might choose to burgle the house. I do not consider living in a fortress an improvement.*
>
> *Preventing accidental access is reasonable. But having to actively defend against intruders is a diversion of valuable resources, and constitutes theft from the owner of those resources. (50, male, 18 yrs exp, VMS, no.)*

For some the computer revolution offered the opportunity to create an environment free from the problems of the outside world. A meritocracy where knowledge and ability were the deciding factors. It is probably for this reason that some of the respondents felt that a cracker had a lack of respect for others and that many had an "underdeveloped conscience".

At this point a distinction should be made between a variety of different types of crackers. It is possible to categorise crackers into three broad groups:

1. Hackers who crack systems with a legitimate purpose;
2. Sporting hackers/crackers who crack for the challenge or for profit; and

3. Copy-cats who gain a feeling a power or a thrill by accessing a system but who lack the skill to crack without relying on the work of others or without cracking software.

For the purpose of question 3 a "good" cracker would fall into the first two categories. It is possible to sub-divide the categories furthrt should the need arise, for instance there are indubitably individuals with good social skills who have the ability to collect information and guess passwords for systems which have little or no real security measures or procedures. Such cracking requires few real computer skills but require more social skills than the average copy-cat.

> *Most crackers today either concentrate on systems with fairly trivial security measures, or they take advantage of the work of others who have the above skills. Research skills, the ability to find relevant previous work and take advantage of it, are important! (13, male, 25 yrs exp, Unix, no.)*
>
> *There is also a potential category for the opportunist "cracker" who cruises around networks looking for "unlocked doors". As one respondent states:*
>
> *There are so many unlocked doors lying around that safecrackers are not necessary. (32, male, 22 yrs exp, unix, no.)*
>
> *Others aknowledged the need for different categories of cracking. Highlighting the various levels of skill required for cracking one respondent steted:*
>
> *Cracking varies from Real Hacking, in that anybody who has the persistence can do it. However, if you're the one going out, reading the tech manuals, coming up with new logins and code to patch the OS, etc, then you're doing some of both (doing Real Hacking to crack a system).*
>
> *I'd consider myself more of a hacker than a cracker any more. There's not much sport in it, and I'm over 18. :) (77, male, 18 yrs exp, unix, yes, yes, no, yes.)*

## cracking skills

Many of the skills necessary to be a good cracker are the same as to be a good hacker. For a cracker, though, social skills are of particular importance, and some of the respondents indicated that many of the crackers around had few other skills. The skills of a "good" cracker (a potential oxymoron as one respndent pointed out) fall into three categories:

1. General skills
2. Computer skills

3. Social skills

## 1) general skills

By far the most popular characteristic mentioned was Patience, followed closely by Persistence, Perseverence and Determination. These skills are especially appropriate to the Hackers and Sporting Crackers who must solve original problems when cracking a system. Thomas Edison is said to have stated that "Genius is one per cent inspiration and ninety-nine per cent perspiration." This is possibly also true for the more able crackers. they must also have a curious mind, a "willingness to experiment" and "to try new things". Intelligence, mathematical aptitude and puzzle-solving skills are pre-requisites for the better crackers but these are augmented with an "eye for details" and good record-keeping skills. Of equal importance is discretion, caution and the "ability to keep your mouth shut".

> *To crack requires either knowledge of security weaknesses in the computer system of the ability to acquire legitimate user ids and passwords via weaknesses in other systems or human errors. A good cracker will have access to a wide range of other crackers, a fair amount of technical skill, and the ability to peek over other people's shoulders. (60, male, 15 yrs exp, unix, y, n, y, n.)*

## 2) computer skills

Computer knowledge and programming skills were considered to be important for a good cracker but a knowledge of the operating system, potential "back-doors" and other security weaknesses were mentioned more often by the respondents as a whole. This cold be because the respondents considered general computer knowledge as an accepted minimum requirement for a "good" cracker. That said, knowledge of an OS and its weaknesses are very helpful for a cracker:

> *... you have to understand networks and root systems, most of the hacking people do is by finding out passwords to systems which a regular user doesn't know about. If you can log in to a system as root, using the root password, you are recognized as a "superuser" by the system and are given special permissions with the system. There is a program called "Supercrack" which is available which can crack an password using english words and common names in a matter of seconds or minutes,... If I install a security system for your company, I would probably install an extremely complex backdoor password such as Ctrlaltf 2Y67UI333 Alt8 2290TYU (which nothing can figure out) this is a master key. It would let me in to do anything to your system. If I told this to anyone in my circle of friends,*

*it might get out, it might not. (72, female, ? yrs exp, unix, yes (but with an authorised users permission))*

*Knowledge of the operating system, a creative mind in terms of finding loopholes in the software, or the ability to guess someone's password. (15, Female, 22 yrs exp, Unix, no.)*

A cracker at the top end of the scale may also have a good understanding of information theory and a good working knowledge of cryptography and other such area of mathematics and computer science on which security systems now depend.

### 3) social skills

Whilst computer skills may be important to crackers, social skills are probably more important. A good cracker is part social engineer with good telephone manners and charisma. With the aid of a little bit of information and a knowledge of the personnel structure within the target it is possible to gather further information. The more information that the cracker has the easier it is to crack the system. This "Ability to psychologically manipulate users and administrators of the target system" (male, VMS, 25 yrs exp, no.) allows the cracker to reach a point where personnel within the target are willing to divulge sensitive information about the system that may even include passwords. Even if passwords are not directly given the information collected may make it easy for the cracker to guess what one may be. The moreinformation about password habits, the easier it is for the cracker.

*A friend of mine was working at Raytheon and was asked if their system was secure. He said he would let them know and brought in supercrack over the Internet. He was able to break 80% of the passwords in half a day. He sent everyone whose account he could access a note, over email, that they should change their password. Also, there are "people leaks."* ***(72, female, ? yrs exp, unix, yes (but with an authorised users permission))***

That crackers have "social" skills may be somewhat ironic as some respondents indicated that many are social misfits:

*The crackers I have been involved in tracking down seemed to be uniformly dissociated from the mainstream of their culture, socially isolated , and occasionally a bit psychotic. Two were sociopaths with police records. Several were simply kids with high I.Q.'s looking for challenges where they beat grownups. (male, 30 yrs exp, UNIX, yes (but paid to do so))*

## the potential motives of crackers

When the participants were asked whet they thought the main motives of crackers were two words appeared more than any others - Curiosity and Challenge. There were of course many other offerings and it is possible to divide the responses into five broad categories:

1. Knowledge Seeking;
2. Thrill Seeking and Mountaineering - the "because it's there" syndrome;
3. Power Tripping;
4. Glory Hunting; and
5. Profit Oriented Motives.

Cracking can be considered a good way to gather information about the operating of a system. It may be merely for the sake of the knowledge itself or because the knowledge is useful. Sometime it might be because the cracker is curious what he will find. It is often the challenge of a good puzzle that drives them to crack. One respondent referred to it as "a form of crossword puzzle competition". The cracker is matched against the person or people who created the security system and it is a "game" that they cannot resist, especially if they are "thumbing their nose" at an institution at the same time.

> *Improve their selfesteem. To prove their value and importance to themselves and their friends who are impressed by these actions. They feel it is safe to perform these actions because nobody is harmed, or at least nobody they care about like 'the big faceless corporation' or 'the oppressive government'.* ***(43, male, 20 yrs exp, unix, no.)***

Institutions and big corporations are not the only targets though as many crackers seem to find voyeurism fun:

> *Mostly fun and a secret joy of the power to look into other peoples secret things. Sometimes, when I listen to them, their glee of breaking into a system sounds like the prankish glee of boys who have managed to steal something from a woman's underwear drawer without being caught. I look on both activities with the same puzzled disdain.* ***(72, female, ? yrs exp, unix, yes (but with an authorised users permission))***

Whilst others gain pleasure from the idea of trophy collecting:

*"Hey, I hacked into A last night!" "Oh, I got in there months ago. But I did B and C as well. Easy."* ***(65, female, 14 yrs exp, unix, y, n, n, n.)***

or behave like graffiti artists:

*It used to be almost exclusively for the pursuit of knowledge. Maybe as a stepping stone to other things back when computers were very expensive. Now it seems to be mostly glory seekers like the kind of people who spraypaint graffiti.* ***(29, male, 18 yrs exp, unix, yes, yes, depends, depends.)***

Many crackers gain a feeling of success from their cracking "achievements". Cracking can be a source of "cheap thrills" and fun for an adolescent or immature mind. Many enjoy the notoriety gained from their exploits and experience "egoboo" or "ego-gratification" when they successfully avoid detection. Many crack for the "feeling of power" at being to access sensitive areas.

*Different people have different motives. I'd say largely thrillseeking, but some people now do it for profit or pure spite. These ratios are changing rapidly.* ***(45, male, 20 yrs exp, yes, no, yes, depends.)***

Cracking would seem to be a youthful phase that many "grow-out of", but some do not and as they age their motives change, often becoming malicious or profit-seeking.

*It depends. Most of the oldstyle (as in 10 to 15 years back) crackers seem to have been motived mainly by curiosity and the intellectual challenge of cracking a protected system. As far as I can tell many of them still feel this way, though I would not be surprised, given the exponential growth of network use and the expansion of the user base from the researchlab coterie to the more general public, if more venal and malicious motives (theft, various forms of deliberately causing trouble for other people) were reaching significant proportions.* ***(71, female, 20 yrs exp, unix, no.)***

A number of respondents suggested positive motives of revenge and one suggested that crackers might crack in an attempt to attract the attention of a potential employer.

Throughout this essay, wherever appropriate, the masculine pronoun has been employed for the crackers. This is not to imply a sexist bias on the part of the author but merely reflects the responses of the participants who

indicated that the ration of male to female hackers was probably greater than nine to one:

> *I have encountered so few female crackers that I regard cracking as essentially an adolescent male pursuit. (Note that older crackers often seem to be cases of arrested maturity, psychologically still children fiddling around.) (male, 30 yrs exp, UNIX, yes (but paid to do so))*

Of 37 responses 33 guessed at a figure of 90 per cent with an overall average of 91.31 per cent.

> *It used to be 99%ish. I'd say, probably, 95%ish now. There were some female hangers-on (we used to call them "hacking groupies"), but they were generally the same girls who'd date the math club. ;)* ***(77, male, 18 yrs exp, unix, yes, yes, no, yes.)***

It is therefore worth noting at this point that one of the characteristics of a cracker is that they are likely to be male.

## beneficial to society or not?

When asked whether cracking was beneficial to society the respondents gave one of three distinct answers: Yes, No and Depends. Those who thought that it was beneficial argued in the main that it improved security by strengthening it against attack by highlighting weaknesses, and often also the remedies for these weaknesses:

> *Although there are a few honest-to-God malicious crackers, most of them are either just trying to see if they can break system security or just want to harmlessly access something. At worst they alert sysadmins to security holes and often make it obvious as to how to plug these holes.* ***(15, Female, 22 yrs exp, Unix, no.)***

This pressure, the argument's proponents state, forces the "user community to look for robust systems."

> *It is a bad thing that a great many programs and programmers rely on security-through-obscurity or are careless about security; the threat of crackers helps keep this from being even more prevalent.... Good security design, however, can lead to both networks that are relatively open and relatively secure.* ***(17, Male, 20 yrs exp, Unix, yes, ?, yes&no, yes.)***

Some supporters of the "crackers are beneficial" argument likened crackers to germs:

> *You might ask the same question about germs. Are germs harmful or beneficial? They are certainly harmful in the sense that they can cause disease, but if you consider the fact that is impossible to eliminate them entirely, then it becomes clear that their presence in moderate numbers is necessary for the development of the immune systema system which can later save you from more serious threats.* ***(73, male, 14 yrs exp, yes, yes, no.)***

or to an inoculation or vaccination:

> *Better that we deal with it piecemeal, now, rather than discover in the year 2020 that the world economy has become a playing board for a few dozen crackers who are using nations as game pieces.... (male, 30 yrs exp, UNIX, yes (but was paid to do so))*

By focusing attention on weaknesses in the system the cracker offers society a valuable service.

> *We, as a society, are moving to wards becoming completely computerized. Should we trust our lives to such poor;y designed systems? I think not!* ***(59, male, 7 yrs exp, unix, y, n, n, y.)***

Crackers waste the time of sysops and sysadmins, and cost the computer community a lot of money as its members atempt to deter them. Even when they do no harm their presence can undermine the integrity of a system:

> *It is like someone entering your house uninvited. Even if he means no harm, he will scare you, disturb your peace of mind, disrupt your work, and waste your time if nothing else, by forcing you to check whether any harm has been done.*
>
> *Besides, he will quite often *do* unintentional damage, sometimes very serious. Last year, for example, a Rio research lab suffered a "benign" cracker attack by two of our students, which resulted in the loss of their entire network file system. (They weren't doing backups, of course...)*
>
> *As a matter of fact, I cannot think of any beneficial aspect of computer cracking.* ***(36, male, 25 yrs exp, unix, no.)***

A cracker's intentions may be honourable but his methods may be destructive in the extreme. When their presence has been incovered the sysop must, in most cases, assume the worst and evaluate what damage has been done. One respondent asked the question of how you would feel:

*if you came home and found a "guess what I did" note taped to your refrigerator: you know someone has been in your house [and you might even be able to figure out how they got in], but you have no hint as to what [if anything] they did.* ***(02, Male, 25 yrs exp, Unix, No)***

Such an auditing process is time consuming and in many cases action will be taken to alleviate the uncertainty:

*even if they do no actual harm at all, if they have meddled into a system that contains any private or confidential information, or any information that could lead to [or weaken] other systems they will have left a LOT of uncertainty behind as to exactly what [if anything] they did. Just dealing with that uncertainty can cause a far amount of expense and nuisance [e.g., getting all of 800 users to change their passwords].* ***(02, Male, 25 yrs exp, Unix, No)***

Apart from the actual damage they cause and the effect their activities have on people's faith in the information they receive from their computers, they are also causing an erosion in the "tendency to trust" that which which has been a bedrock in the development of the electronic community. The activities of crackers leads to an "erosion of trust and increased cynicism" which can lead to less cooperation amongst members of a community:

*One of the reasons why the Internet has been so successful is because of it's openness. Hackers cause companies on the Internet to stop sharing data. This is not a good step for the computer industry.* ***(43, male, 20 yrs exp, unix, no.)***

In creating fear, crackers "discourage good programming" and undermine the benefits of such activity. The fear of crackers, along with the hype of the security business that has grown with this fear, could cause an "over-reaction" which could lead "to a curtailment of liberty". Some respondents felt that the arguments for and against cracking's benefits are equal in eloquence:

*Usually neutral. Most get onto a system, play around and get off without doing any real damage. Some do real damage so there is some loss. Their existence leads companies and governments to plug security holes before some more significant loss occurs so there is some gain. Generally I think it balances out.* ***(52, male, 19 yrs exp, VMS, no.)***

Whilst others felt that we must re-assess what needs to be secure and what information should be made readily available to all society:

*The outcome of the crack determines the benefits or the harm. - WHY? - Some cracking activities are the equivalent of children climbing over a fence to get into a school yard to play. This class activities have happened since time immemorial and serves to remind all people that the purposes of certain fences perhaps require reconsideration.* ***(11, Male, 20 yrs exp, Unix, yes, no, no., yes.)***

Whether cracking is harmful or beneficial depends on the location of the target and the intentions of the cracker but some would argue that instead of wasting their own time and that of others they should spend it more fruitfully in activities that are more beneficial to the development of the electronic community. Even if they believe that they activity is benign it still has negative effects as it causes:

*It makes members of the society spend too much time building locks for doors rather than building windows to see through.* ***(64, male, 29 yrs exp, unix, no.)***

## what activities should be criminal?

There has been much debate concerning what activities should be criminal and what activities currently crimes should be de-criminalised. Should society even make a distinction between computer-crimes and other crimes; as one respondent pointed out "you don't have special law for 'Tuesday crimes'." Others liken the treatments of crackers to a "witch-hunt" which is "absurd in comparison to the light treatment violent criminals often get."

The question of what should be criminal is fundamentally a question about "information as property"; it is an idea "that not everyone is comfortable with". In magnetic form information has become infinitely more portable than it is when paper-based. this makes it more stealable.

*Computers are vulnerable to physical access. Suppose your confidential corporate files, that used to occupy five locked filing cabinets in five locked offices, are stored on a single hard disk in a locked room. Chances are I could break into that locked room simply by crawling along the "hyper space" above the ceilings of most modern office buildings. In one fell swoop, I can steal information that would not have been nearly so accessible were it still in five locked filing in five locked offices.*
*Computers are vulnerable to electronic access. Very very few people in the world understand the vulnerability introduced when connecting a computer to a network.* ***(11, Male, 20 yrs exp, Unix, yes, no, no., yes.)***

This new format of information also allows its alteration without, in many cases, easy detection; this quality undermines people's confidence further when a cracker's presence is feared. Computers have become so "user friendly" that probably the majority of users now have very little understanding of the way that the systems they use work. Whilst they have faith in the integrity of such systems they are happy and confident in the information that the system provides. If this faith is challenged by the presence of a cracker they may experience a feeling of violation and will distrust the information they receive; the cost of such a scenario is probably impossible to gauge.

The cost of recovering from an intruder's presence in a system can be great as the following two accounts indicate:

> *The 'internet worm'... hit us [X] and caused us a nontrivial amount of expense to deal with. A significant part of that cost was figuring out what the worm did [or didn't] do. I'm not at liberty to discuss what happened at X or what we did, but we did sever our network link [which was a business cost right there] and worked to figure out what the worm did to ensure that in the time before we isolated ourselves from the net nothing was compromised and we also had to make sure that nothing was corrupted and that no traps or other nasties were left behind. All of this cost us a fair bit of effort, and the secondary cost [of having a fair number of systems unusable while we sorted it all out].* ***(02, Male, 25 yrs exp, Unix, No)***

> *In 1987 we (at my previous job) had a breakin via the Internet into our VAX. The breakin came via a user ID and password stored in an accessible file on a machine in Oslo. That machine in turn had been hacked from elsewhere, some speculated members of the Computer Chaos Club in Hamburg. The machine contained no confidential information, but the intruders left several back doors for a subsequent return. DEC was greatly perturbed, and we used 4 weeks to clean up the machine, 4 weeks without the single central computer for 30 employees.* ***(37, male, VMS, 25 yrs exp, no.)***

As with ramblers there are areas which are acceptable locations where the potential harm they can cause is minimal and others where their presence can be a harmful, disruptive influence on the local environment. There are then areas which for sensitive reasons or merely reasons of privacy where their presence is unwanted and constitutes trespass.

# Chapter 8

## Motivation of computer criminals

*"Within its very first year of operation, 1878, Bell's company learned a sharp lesson about combining teenage boys and telephone switchboards... they played clever tricks with the switchboard plugs: disconnecting calls, crossing lines so that customers found themselves talking to strangers, and so forth.*

*"This combination of power, technical mastery, and effective anonymity seemed to act like a catnip on teenage boys." (Sterling 1992 page 14)*

Referring to "hackers":

*"...computer programmers and designers who regard computing as the most important thing in the world.... Beneath their often unimposing exteriors, they were adventurers, visionaries, risk-takers, artists . . . and the ones who most clearly saw why the the computer was a truly revolutionary tool." (Levy S. 1994 page 7)*

introduction.

The purpose of this chapter is to consider the significance of the computer crime problem, as distinct from the computer related problem. This is perhaps at first sight a specious distinction to make. But, in view of the increasing use of computers in business and other walks of life, it is necessary to do so in order to differentiate from business crime, etc. in which a computer is used. If this distinction is not made, all crime will become computer crime, as computers impact in all areas of life and this impact is set to increase further.

This chapter will then attempt to highlight the factors particular to the motivation of computer criminals. It will consider whether these factors are relevant or not for bank clerks and what implications they might have for the banks that employ them and the threat that computer related crime might pose?

### the myth of computer-crime

Computer crime is on the rise! It is possible to make the definitive statement with great confidence. Computer crime is increasing through the reclassification of many crimes as computer crimes if they involved a computer and as there are more computers in the areas where crime is

committed there must be more computer crimes. We must also add to this the number of computer misuses by those in the workplace. It is possible in many computer dependant industries to be dismissed for using unauthorised software for the fear of viruses. The Audit Commission 1994 report confirms this rise may be real. The number of instances reported by respondents to their questionnaire increased from 180 in 1988-1990 to 537 in 1990-1993.

Closer examination of the Audit Commission's figures reveal that nearly half of these reported instances involved viruses (261). By its very nature a virus is prolific in its ability to reproduce itself and thus infect many possible hosts in a short period of time. Many of these reported instances may therefore involve the same virus. It must also be remembered that a virus is merely a string of commands that performs a set task within the host. This task may cause a display message to appear or the screen to lock or in some case for data to be destroyed. Screens can lock or data be lost without the aid of a virus but as a result of human incompetance or bugs[41] in the software. When this does happen there is a tendancy to assume that the "machine is infected". More "viruses" are noticed as a result of the fear felt by many more people of their threat, possibly as a result of media coverage.

The number of instances of hacking in the Audit Commission's survey (Audit Commission 1994) represented five incidents per year for the three year period that the survey covered. Of these 15 cases over a quarter occurred in Education. The most alarming case involved a nurse who "hacked into a hospital's computer system and prescribed potentially lethal drugs for a patient and altered treatment records for others... He used a doctor's personal identification code, which he had memorised some months earlie, to gain access to the system." (Audit Commission 1994 page 17). Here we see that there is little difference between using another's personal identification code and forging their signature. The extent to which it can be described as

[41]In the early years of computing a computer was malfunctioning so it was given a thorough examination. An insect was found in the workings and was effecting the way that the computer operated. The term bug has been used since to indicate that there are small errors in software that are effecting the way that the computer operates.

hacking is doubtful. The individual would seem to have committed an offence under Section 3 of the Computer Misuse Act 1990, but whether his act should be classified as a computer crime is still debatable.

The total losses reported involving hacking and viruses represented less than one-tenth of the total losses reported for the 108 cases of computer abuse involving fraud. Losses, including indirect losses, totalled over £3 million and represented nearly 80 per cent of the total losses reported for the 537 cases recorded. Of the cases involving fraud 88 per cent involved "(t)he inputting of fraudulent data into a computer system... and... the unauthorised amendment of computerised data..." (Audit Commission 1994 page 13). Whilst it is true to say that the indirect losses of some of the cases involved are harder to assess than those for fraud it still seems that the increase in computer crime is largely as a result of fraudulent computer abuse by employees[42] and the reclassification of other crimes as computer crimes. Computer crime is a myth!

Or is it? Organisations have historically been quite slow in the UK to accept the benefits of the IT revolution. Education and Medicine are the two big exceptions in the list of areas involved in the survey and it is these two areas that reported 60 per cent of the cases involving hacking (although less than 40 per cent of the respondents came from these areas). The medical profession has an interesting conundrum to solve; it has many institutions which are both research/teaching units and hospitals. "Medical schools want access to world-wide research and encourage a free exchange of data while hospitals want to protect patients' data and make it available only on a need-to-know basis." (Audit Commission 1994 page 17). It is a problem that more institutions will face if they are to take full advantage of the IT revolution. The only way for a system to be secure is if it is stand-alone and only accessible to a select few, preferably one. Connection to other computers introduces the possibility of misuse by distant hackers. The major opportunity

[42]No incidents are noted as being perpetrated by "external" parties (Audit Commission 1994 page 12).

for a hacker arises from the weaknesses that threaten the security of even a stand-alone system.

> *"I walk past the computer building. It's locked, but when a group of students comes out, I go in. In the central room there are about fifty terminals. I wait for a while. When an elderly man comes in, I follow him. When he sits down, I stand behind him and pay attention. He doesn't notice me. He sits there for an hour. Then he leaves. I sit down at a free terminal and press a key. The machine prompts: Log on user ID? I type LTH3 - just as the elderly gentleman did. The machine replies: Welcome to the Laboratory for Technical Hygiene. Your password? I type JPB. The way the elderly gentleman did. The machine replies: Welcome Mr Jens Peter Bramslev." (Peter Høeg "Miss Smilla's feeling for snow" page 219).*

Good practice minimises opportunities whether the system is connected to an outside network or not.

It has been stated that the level of true computer crime is small and that any perceived computer crime problem is to do with the greater use of computers in the book-keeping functions of business:

> *"...the number of input frauds... still represents the largest proportion of frauds." (Audit Commission 1987, page 3).*

If this is accurate it becomes clear that the general motivation process for computer-related crime is consistent with that of any other form of fraud or embezzlement. An input fraud may be executed in a non-computer environment just as easily as in a computer one and is largely as a result of deception rather than any computer competences. Of course by their nature, computer crimes are difficult to detect and so it is possible that a great many go undetected. Alternatively they could go unreported as systems managers and their employers might be embarrassed to make such revelations. So is elite computer crime as significant as some would believe?

> *"Some professional informants... have estimated the hacker population at as high as fifty thousand. This is highly inflated... I would guess that as few as a hundred are truly "elite" - active computer intruders, skilled enough to penetrate sophisticated systems and truly to worry corporate security and law enforcement." (Sterling 1992 page 76-77)*

It is possible to summise that there is a Computer Crime pyramid featuring three groups of computer criminal.

Figure 8.1[43] above shows how the various different types of computer criminals can be categorised into three broad groups:

1. Elite Computer Criminals
2. "Copy-Cat" Computer Criminals
3. Naïve Computer Criminals

The use of the term criminal is perhaps somewhat misleading. It is intended that this term should also include the potential criminal, or those that act in a way that is deviant from the current norm. This is perhaps unfair on those that are not misusing the networks. Until the Computer Misuse Act 1990 the law failed, in the most part, to address the issues and new criteria that are particular to Cyberspace. Regulators were forced to apply old laws to this new environment.

The first two categories may be treated together as they are both capable of more sophisticated computer crimes which require a higher level of computer knowledge and skill. The distinction is made as Elite Computer Criminals (and those capable of such crimes) pose a much greater threat to the security of the networks. The Copy-Cat Computer Criminal has the ability and knowledge to duplicate the activities of the Elite, although they are unable to "crack"[44] the more sophisticated security systems without methods and techniques devised by the Elite.

The third group consists of individuals who have used a computer at some time during the perpetration of a non-computer crime, in other words an input

[43]The proportions are graphically nominal; whether it is possible to put figures to them is a question which falls outside the scope of this thesis. It is clear though that to address this question a number of parameters need first to be set to limit the number of crimes that *Naïve computer criminals* can be said to have committed and to define the point at which an *Elite compter criminals* becomes a *Copy-cat criminals.*

[44]Hackers have also been referred to as "crackers" to distinguish them from the earlier group referred to as hackers. This group were merely technology enthusiasts. For more read "Hackers" by S. Levy.

fraud would be categorised as a computer-related crime, as indeed could the now famous Equity Funding Corporation scandal (Seidler et al 1977). All of the crimes in this third category require or no computer knowledge and are motivated in the same as if the crime were committed without the assistance of the computer. This of course implies that the involvement of the computer is incidental, this is not always so. The Equity Funding Fraud would have been impossible on such a scale without the use of a computer, and it is, on the whole, a lot easy for an employee to manipulate inputs to a computer, than, if they had to present the vouchers to another human for processing manually.

If it is assumed that the Naïve Computer Criminal commits crimes for the same reasons as a criminal in a similar, but non-computerised, environment we can assume that there is nothing special about this process. But what of true computer crime, those crimes that would be impossible without a computer, what are the motivating factors behind the actions of the Elite Computer Criminal and the Copy-Cat Computer Criminal?

The lexicon of hacking vernacular is littered with a vast panoply of terms and literary allusions. Hackers with names or "handles" such as "Pengo", "The Mad Hacker", and "The Mentor" are involved in activities such as "Social Engineering", "Trashing", and "Phreaking". These are all activities related to hacking. Phone phreaks take an interest in the workings of telephone systems. They are interested in the ways and means by which the switches work in the telephone company networks so that they can manipulate them and use the system for free.

At the lower end of the phreaking spectrum are those phreaks that steal accounts and passcodes, and sell them to third parties to use. Because of the nature of these codes and account numbers the user may not be aware that they have been "lost" until they receive their telephone bill. On this bill they are likely to find a number of long distance calls to places they may not

of even heard of, let alone know someone there to telephone. The easiest way to acquire an account number and related password is through a process known as "Shoulder Surfing". This involves the thief merely observing the user inputting the various digits. They will then probably sell this information, possibly by way of a posting on a BBS (Bulletin Board System). The best place to steal these numbers are busy airport terminals and train stations.

Such antics may be annoying to all concerned but they hardly represent a serious threat to the fundamental system. The elite phreak, on the other hand, might. "The Matrix", as the metanetwork of computer systems that spans the globe has been called (Quarterman 1990), is reliant on the telecommunications network, as are emergency services, etc. A malicious phreak could have the ability to disrupt these activities through their manipulation of the switches. They are able to reroute calls, charge calls on one phone to another, etc., but have yet to disrupt the network on a massive scale. Such disruptions in the United States during 1991 were as a result of software (January 15, July 1 & 2) and power failure (September 17). The software failure is not surprising in a program featuring 10 million lines of code (Sterling 1992 page 40). People with the expertise to engineer such a crash in a program of that size are likely to be few in number.

"Social engineering" and "trashing" are both processes which rely on the weakness of the human link in any security system. Trashing involves delving through waste for information, even apparently trivial information may be used in the social engineering process. The hacker will use information of a company's hierarchy, for instance, to pressurise, or coax, a junior member of staff into revealing some more important information. It becomes clear that the easiest way to improve a security system may be to improve the human element by means of training and motivating them in other ways to ensure that they do not act out of spite, and so that they are aware of the importance of good practice when security is involved.

## motivation of hackers/crackers

The prosecution of Nicholas Whiteley in 1990 throws up some interesting pointers to the motivations of a computer criminal. Whiteley was prosecuted and convicted for illegal access to various computers via JANET, the Joint Academic Network. He was eventually convicted under the Criminal Damage Act 1971 (the Computer Misuse Act 1990 had not come into force then). Whiteley gained no financial benefit from his activities and during the trial it was revealed that he had left the following message on the computer system at St. Mary's College: "I think you should know that I am mad... I am also very depressed." (The Times, May 2, 1990)

Whiteley caused more than £25,000 worth of damage and eventually received a sentence of four months in prison plus another eight months suspended (The Times, June 8, 1990). He seems to have been motivated by something other than financial gain and under the pseudonym "the mad hacker" seems to have been seeking attention. Attention would seem to be a major motive for many hackers. This is a view partially supported by Lundell (1989) who feels that it is status that hackers and hi-tech criminals seek. He suggests that whilst the public fears the effects of rogue computers they also have respect for those with the virtuoso skills. The hacker is a hi-tech criminal, as is the virus creator. On this point Lundell cites Dr. Robert Lambert (Professor of Psychology at Concordia University in Montreal) who stated:

> *"They are status criminals, you are going to find people who are going to create viruses not only for reasons of revenge and retribution but simply as a way of attaining status. It's a good way for people to attain status when they haven't got any other way." (cited in Lundell 1989, page 91).*

The stereotype of the computer criminal would have us believe that they are outsiders. The "WarGames" storyline shows us a bright underachieving anti-social delinquent. Stoll's (1991) search lead to a gang of German students of a similar ilk, the principal hacker being German Merkus Hess:

*""Hacking is an addiction, Your Honor [sic]," Hess said. "And as long as you stay out of trouble, the addiction is difficult to shake."" (Hafner & Markoff 1992 page 242, quoting the testimony of Markus Hess. See The Cuckoo's Egg by Clifford Stoll for more on the exploits of Hess).*

In these and many more cases the motivation has been the challenge, an intellectual game involving the control of a large corporation or institution's computer, a computer that would be inaccessible otherwise:

*"When in the throes of hacking, Lenny was having a good time. The idea of having control over many computers was incredibly seductive. The challenge of figuring out where to go to look for the information they wanted was more stimulating than any college programming course. And all the while they watched a twelve-billion-dollar company flounder helplessly as it headed down one cul-de-sac after the other." (Hafner & Markoff 1992 page 126-127)*

There is also a romantic side to hacking:

*"In the end Lenny shared Kevin's delusion that what they were doing was undercover work worthy of a Hollywood spy thriller. Brazenly walking onto the campus was the kind of thing Robert Redford would do as the hunted CIA researcher in the movie Three Days of the Condor." (Hafner & Markoff 1992 page 68)*

So far it has been proposed that hackers are motivated in general by a desire for attention and the thrill of using the technology. It can also be argued that it is an addictive activity, this is not surprising if we think of the effect that Sega and Nintendo have had on the electronic games market. Part of this addiction may be the result of another motivating factor: Technical Power.

## technical power

*"For many in this country, hackers have become the new magicians: they have mastered the machines that control modern life. This is a time of transition, a time when young people are comfortable with a new technology that intimidates their elders." Hafner K. & Markoff J. (1992, page 11).*

Maslow (1943) argued that in general people were motivated by a hierarchy of needs that once satisfied cease to motivate. The individual's attention turns to the next need in their hierarchy. This theory was based on a single culture survey at a time when the world was facing war, the responses should therefore be applied to the modern individual with caution. That said

Maslow's theory does tend to support the view that each individual has needs at different levels. Obviously the physiological needs are primary but of low motivational strength due to the social security systems of most Western countries. Many theorists support the view that modern man is now likely to be motivated by the higher needs (MacGregor 1957, Likert 1961, 1967), one of these being the need for power (Hunt 1986).

Power comes in many forms: Physical; Resource; Position; Personal; Expert/Technical; and Negative. It can be argued that the computer criminal seeks both negative power and expert/technical power. The technical aspects are perhaps the most important as it is from this that they derive any negative power they may exert on others.

> *"The deep attraction of this sensation of elite technical power should never be underestimated.... For a few, it is overwhelming, obsessive; it becomes something close to an addiction. People - especially clever teenage boys whose lives are otherwise powerless and put-upon - love this sensation of secret power and are willing to do all sorts of amazing things to achieve it." (Sterling 1992 page 19)*

McClelland (1961, 1976) identifies three strong motivators for modern man: Power; Affiliation; and Achievement. The "Hacker Underworld" can offer satisfaction of all these needs for those who wish to "play" there. The Electronic Frontier (Kapor 1991) is a very tempting "area" for the hacker and other computer enthusiasts. It is a frontier that is still austere, suffering from the matrix's differing communication protocols and proprietary restrictions, as well as being legally a vague area. It offers the excitement of "breaking new ground". To the hacker and enthusiast, Cyberspace has the attraction of what may be termed "new snow". Cyberspace is an arena were the hackers and enthusiasts may be cowboys or indians and in some cases even the cavalry (a group of hackers from a group known as the Legion of Doom have set up a company, Comsec Data Security, to advise institutions on computer security matters [Branscomb 1991, page 113]).

Some have argued that it is more than merely a "revolution" about computers. The implications of cyberspace in its various manifestations have effects on other aspects of society and that this has caused a cultural revolution akin to the industrial revolution whilst others compare it to the Hippy movement of the Sixties. Rushkoff (1994) states that cyberspaces is a part of a greater world which is "Cyberia":

> *Cyberia is the place a businessperson goes when involved in a phone conversation, the place a shamanic warrior goes when traveling [sic] out of body, the place an 'acid house' dancer goes when experiencing the bliss of a techno-acid trance. Cyberia is the place alluded to by the mystical teachings of every science, and the wildest speculations of every imagination. Now, however, unlike any other time in history, Cyberia is thought to be within our reach. The technological strides of our postmodern culture, coupled with the rebirth of ancient spiritual ideas, have convinced a growing number of people that Cyberia is the dimensional plane in which humanity will soon find itself. (Rushkoff 1994 pages 16-17).*

Hackers have had the systems link to the networks around the world at their mercy on more than one occassion. A power that their parents would never have dreamed about. They also have the affliations through the hacker underworld that allows them to gain recognition for their feats. But it is probably true to say that whilst there is a thrill achievable from entering an American military installation's computer it would be difficult to trigger a military attack no matter how motivated the hacker was. Hackers are more interested in the feat rather than causing mayhem.

## compulsive programmers

The term "hacker" is often applied to those young individuals who spend their waking hours attempting to break-in to systems for which they have no access authority, although its original meaning is more to do with those "hacks" with a more legitimate use in computers and their workings. Such interest can border on the obsessed as Weizenbaum (1993), a professor of computing at M.I.T., noted when he described "computer bums":

> *"Whenever computer centers [sic] have become established, that is to say, in countless places in the United States, as well as in virtually all other industrial regions of the world, bright young men of disheveled appearance, often with sunken glowing eyes, can be seen*

*sitting at computer consoles, their arms tensed and waiting to fire their fingers, already poised to strike, at the buttons and keys on which their attention seems to be as riveted as a gambler's on the rolling dice. When not so transfixed, they often sit at tables strewn with computer printouts over which they pore like possessed students of a cabalistic text. They work until they nearly drop, twenty, thirty hours at a time. Their food, if they arrange it, is brought to them: coffee, Cokes, sandwiches. If possible, they sleep on cots near the computer. But only for a few hours - then back to the console or the printouts. Their rumpled clothes, their unwashed and unshaven faces, and their uncombed hair all testify that they are oblivious to their bodies and to the world in which they move. They exist, at least when so engaged, only through and for their computers. These are computer bums, compulsive programmers. They are an international phenomenon." (Weizenbaum. 1993 p 116.)*

The computer industry has been built on the backs of the effort of such young men. Levy (1994) subtitles his book about the early hackers "Heroes of the computer revolution", but he does not deny their compulsion referring to them as "those computer programmers and designers who regard computing as the most important thing in the world..." Weizenbaum emphasizes their compulsive nature more when he likens a compulsive programmer to a compulsive gambler, but not all those individuals who call themselves "hackers" are compulsive programmers. He notes that the "highly creative labor of people who proudly claim the title 'hacker'" has lead to the development of time-sharing systems, computer-language translators, graphics systems and much more.

Weizenbaum offers profiles for a hard-working professional programmer and a compulsive programmer as a comparison. In most cases they are opposites. The professional addresses the problem to be solved whilst the compulsive sees the problem merely as an opportunity to interact with the computer. The professional discusses the problem with others; prepares for the problem by making notes and flow-diagrams of what needs to be done. They are likely to spend less time at the computer console and are even willing to let others assist with some of this work: a marked difference to the stance taken by the compulsive programmer. The professional will document actions taken and the reasons for them. When a problem arises they will search for possible causes and solutions. This need not be done at the console.

*"The professional regards programming as a means toward an end, not as an end in itself. His satisfaction comes from having solved a substantive problem, not from having bent a computer to his will." (Weizenbaum, 1993 p. 117)*

The compulsive programmer is usually a superb technician with a good knowledge of the computer, its peripherals, its operating system, etc. These skills were[45] often employed by computer centres when the need arose. But the compulsive programmers tendency not to document what he has done can make it difficult to maintain the programmes they write. The systems they build are often merely a collection of subsystems which are "hacked" together. When a problem arises they are "patched until the manifest trouble disappears" (p. 119). They tend to add more features and sub-routines whilst also trying to amend errors in other subsystems.

When a programme fails, the compulsive programmer feels it as a challenge to "his power, not his knowledge." (p. 119) He feels the challenge acutely and spends much time and effort in the search for a solution to the problem. "Indeed, the compulsive programmer's excitement rises to its highest, most feverish pitch when he is on the trail of a most recalicitrant error" (p. 119), feeling that everything should be in order and yet the computer is acting in a strange and mercurial manner.

*"How are we to understand this compulsion? We must first recognize that it is a compulsion. Normally, wishes for satisfaction lead to behaviors that have a texture of discrimination and spontaneity. The fulfillment of such wishes leads to pleasure. The compulsive programmer is driven; there is little spontaneity in how he behaves; and he finds no pleasure in the fulfillment of his nominal wishes. He seeks reassurance from the computer, not pleasure. The closest parallel we can find to this psychopathology is the relentless, pleasureless drive for reassurance that characterizes the life of the compulsive gambler." (Weizenbaum, 1993 p. 121)*

The compulsion is not clear from the following statement but many of the attraction to a potential hacker are:

[45]Written in the past tense as Weizenbaum's account was originally published in 1976 and it is doubtful whether computer centres are now as dependent on compulsive programmers as they were. In his account he goes on to liken them to a bank employee who is the only one to know the code to the safe.

*"I made a discovery today. I found a computer.... It does what I want it to. If it makes a mistake it's because I screwed up. Not because it doesn't like me....*

*"And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins an electronic pulse is sent out a refuge from day-to-day incompetencies is sought... a board is found. "This is it... this is where I belong..." ... This is our world now... the world of the electron and the switch, the beauty of the baud.... We exist without skin color [sic], without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat and lie to us and try to make us believe that it's for our own good, yet were the criminals.*

*"Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for." (Sterling 1992 page 85. Quoting The Conscience of a Hacker by "The Mentor" in Phrack, Volume One, Issue 7, Phile 3.)*

## normless or psychopathic?

The question of whether the average hacker is normless or not is somewhat hard to answer unless we consider what the norm is first. Here lies the problem. The hackers are normless if we compare them to the standards set in the physical world. Cyberspace is not part of the real world and has by its very nature stretched the boundaries of the norms and the laws that govern the physical world.

*"Hackers are generally teenagers and college kids not engaged in earning a living. They often come from fairly well-to-do middle-class backgrounds, and are markedly antimaterialistic (except, that is, when it comes to computer equipment). Anyone motivated by greed for mere money (as opposed to the greed for power, knowledge, and status) is swiftly written off as a narrow-minded breadhead whose interests can only be corrupt and contemptible." (Sterling 1992 page 62)*

*"Somewhere at the center [sic] of this conspiracy there had to be some serious adult masterminds, not this seemingly endless supply of myopic suburban white kids with high SATs and funny haircuts." (Sterling 1992 page 94)*

## rationalisation of behaviour

It has been argued that hackers offer a valuable service to the computer community. They highlight faults in security measures and have been known to assist system managers with problems due to their intrinsic interest in computing in general.

*"I think, hackers--persons who creatively handle technology and not just see computing as their job--do a service for the computing community in general." (Hafner & Markoff 1992 page 231, quoting a posting by Pengo (Hans Huebner) to the Risks forum)*

Others would argue that without the threat of hackers computer security would be meaningless. So that rationalisation on purely security reasons may be said to be somewhat specious[46]. Were hackers are possible of value is the imaginative use of new technology. Play yields many rewards.

> *"We cannot unduly inhibit the inquisitive 13-year-old who, if left to experiment today, may tomorrow develop the telecommunications or computer technology to lead the United States into the 21st century. He represents the future and our best hope to remain a technologically competitive nation." (Senator Patrick Leahy quoted by Sterling 1992 page 283)*

Does hacking or cracking represent as much of a problem, or threat, compared to other forms of crime? Gail Thackeray [former Assistant Attorney General of the State of Arizona] thinks not:

> *"the biggest damage is telephone fraud. Fake sweepstakes, fake charities. Boiler-room con operations. You could pay off the national debt [USA] with what those guys steal.... They target old people, they get hold of credit ratings and demographics, they rip off the old and weak." The words come tumbling out of her.*
>
> *"It's low-tech stuff, your everyday boiler-room fraud. Grifters, conning people out of money over the phone, have been around for decades. This is where the word "phony" came from!" (quoted in Sterling 1992 page 177-178)*

Rushkoff (1994) cites her as having told a story of how one boy's character changed for the better when the authorities confiscated his computer. She apparently likens the computer to an addiction that allows some individuals to "vent their frustrations in an obsessive, masturbatory way." (p. 267). She criticizes some of the older hackers for not showing more responsibility and for not emphasizing the difference between then and now. Then "It was a few pieces of code or a university prank... Now these kids are being used by drug dealers! They are being prostituted, but it's the kids who go to jail!." (p. 268)

## summary of motivational factors

> *"If there's something people want, a certain percentage of them are just going to take it. Fifteen percent of the populace will never steal. Fifteen percent will steal almost anything*

[46]Of course this argument may be countered with the argument that it is better to have benign friendly crackers than the malicious kind. By having security measures tested by friendly crackers the system is more likely to repell the unfriendly variety.

*not nailed down. The battle is for the hearts and minds of the remaining 70 percent [sic]." (Sterling 1992 page 183)*

It can be summised that the motives of the average hacker include some, or all, of the following:

1. Attention
2. Affiliation
3. Power
4. Achievement
5. Curiosity

This premise is difficult to prove, but looking at the list there is nothing that could not be applied to an intelligent modern individual. Where they differ is in their means of achieving these needs. It is still difficult to defend the list above due to the nature of the hacker underground.

Whilst it is clear that these motives can be attributable to the employees of a bank it is clear that they are less likely to commit an Elite or Copy-Cat crime[47]. They have many other avenues open to them.

## "Outsiders" within the organisation

One of the biggest problems that organisations often fail to fully address is the problem of career progression for computer staff. The computer function is often on the periphery of the organisation. There is often little training and development of a general nature for such staff, they consequently face very flat careers which often fail to fulfil their aspirations. This Aspiration-Reality gap for these staff is a huge demotivator and may lead them to pursue other activities. When they feel that the organisation is to blame for their misfortunes they may conspire to correct the situation. When such a person feels that they are no longer a valued member of the organisation they have the power to cause much havoc within the organisation.

[47]This is due to their lack of sufficient computer knowledge, as will hopefully be proved by the survey.

Equity is a very important issue for the analyses of such crimes. Adams (1963) and Homans (1961) found that where the individual perceives that their reward is inconsistent with the level of effort exerted on their part that a feeling of inequity will arise. This obviously has consequences for the level and standard of output, but also forms a potent motive for crime against the organisation, or for the organisation, in an attempt to be seen as highly successful and warranting of promotion or greater reward.

But what of those members of bank staff that do have the requisite skills? Where companies must be most at guard is from "outsiders" within the organisation, those computer staff who feel under appreciated. They often have the power to bring a computer reliant organisation to its knees. The computer literacy of employees has advanced rapidly over the last decade. Most new employees to companies will have the opportunity to acquire a reasonable level of computer knowledge, be it through interaction with such at school, college or university, or because they have a computer at home. The cost of such computers has dropped dramatically and is expected to fall further making them more attainable.

Even though computer literacy has improved, indications are that there is a tendency to use home computers for game playing, rather than more serious uses. That is not to say that there are not those with virtuoso skills acquired through hours in front of their VDU's. The newspapers have catalogued the incidents of abuse similar to the War Games film scenario:

> *" A youth calling himself the mad hacker caused more than £25,000 worth of damage to university computer systems after "breaking in" and sabotaging files, a Southwark Crown Court was told yesterday." (The Times May 2, 1990).*
>
> *"Farmingdale, New York - A hacker, aged 14, suspected of penetrating a Pentagon computer has been arrested with 12 others on charges of breaking into a university computer in Washington State (AFP)." (The Times August 18, 1990).*

The best hackers have the ability to bring a system "to its knees", and along with viruses, have been the focus for the newspapers reporting of computer

crime. But as the Audit Commission's (1987, 1994) findings show they still account for very little in terms of total money defrauded[48]. The biggest area is still that relating to input fraud. On this the Audit Commission's report found that input fraud:

> *"...represents the largest proportion of frauds. As in previous surveys, and in common with surveys abroad, it also constitutes the largest proportion of financial loss. Although fewer of these input frauds were reported in 1987, the value was significantly higher and of the 57 cases, the five relating to creditor payments represented 70 per cent of the total fraud losses." (Audit Commission 1987., page 3)*

The Audit Commission's survey findings were based on the responses of some 1,200 firms from both the public and private sector, and attempted to highlight the incidence of computer-related fraud and misuse, and covered cases involving the use of a computer to program an adventure game during lunch hours[49] to a case involving two individuals who accessed a national electronic mailbox service[50], to the case of an accountant who set up fictitious companies and defrauded over £1 million using flaws in his employer's systems[51]. In the survey the total loss attributed to hacking was £100, but the cost of uncovering such acts was much higher. Hacking is very likely to increase in incidence over the coming years, and such unauthorized interaction is particularly worrying with the increase in the number of viruses (and their variants) which are now in existence. That said it is not something that management should fear if they have a "closed" system and have procedures and rules designed to deter the use of unauthorised software by their staff.

The fact that input frauds represent the largest category of computer misuse signals the fact that very little computer skill is necessary to commit a computer fraud. But should such frauds be considered as computer frauds?

---

[48] Although this can change as hackers turn to computer blackmail, etc. See the chapter on Computer Misuse.
[49] Case 110, Audit Commission 1987.
[50] Case 95, Audit Commission 1987. See discussion on the case of Gold and Schifreen in the previous chapter).
[51] Case 22, Audit Commission 1987. Ironically he had previously advised the management of these flaws).

The answer is a conditional yes! Of the 118 cases listed by the Audit Commission some are indeed contentiously called "computer misuse". Take case 56 for instance, where a computer development officer borrowed a computer, whilst on long-term sick leave, to use in the production of a computer-based directory for several voluntary sector organisations. Admittedly the computer was necessary for the activity but, it hardly constitutes a major abuse[52] or one that heralds a new phenomenon. It is still possible to argue that there is very little difference between taking a computer home and taking a chair home. Wasik (1991) cites Ingraham[53] who sums this issue up very eloquently when he stated:

> *"Striking a watchman with a disk pack should remain the battery that it is, and not be elevated to the status of a computer crime. There are enough red herrings in our courts already". (Ingraham cited in Wasik 1991 page 2).*

There must still be room within the categories of computer crime to include those crimes which a computer made possible, those crimes which while feasible on a theoretical basis would have been impossible without the aid of a computer, due to their size for instance. The most notable known case to date is that of the Equity Funding Corporation of America. When this gigantic insurance fraud was uncovered in 1973 it was found that of 97,000 policies that the company claimed were currently in force 64,000 were bogus, the details of which had been created and logged on computers which had been used to record cancellations, deaths, etc.. The bogus policies were sold to co-insurance and re-insurance companies. In the introduction to their book on the case Seidler, Andrews and Epstein comment:

> *"Few white-collar crimes have seized the nation's [the USA's] attention more dramatically than Equity Funding. None has been more disquieting. An established, nationally known insurance and securities company was abruptly exposed as a beehive of fraud, the seat of an enormous swindle that had gone undetected for years. Behind a facade of confident prosperity, Equity Funding had been forging documents, falsifying accounts, and manufacturing phony insurance business on an assembly-line scale". (Seidler, Andrews, and Epstein 1977 page 3).*

---

[52] People will call in sick when they have other things to do, it was not the computer that lead to the offence.

[53] D.G. Ingraham, "On Charging Computer Crime" (1980) **Computer and Law Journal** 429, page 438.

Without the computers the fraud could not have been as large as the scale perpetrated at Equity Funding. This is truly a computer-related fraud, even if the computer has not brought any originality to the crime. It is necessary to categorize it as a computer related crime if we are to fully assess the costs of computerization. After all if we are to attribute all the benefits that are related to computers we must also consider all the costs. The computer's ability to handle vast amounts of data with speed and accuracy is cited as a benefit. Equity Funding graphically highlights how such alacrity can be used for criminal purposes.

There being such broad categories of computer-related fraud means that the skills required to commit such are consequently broad and many and indeed most office workers capable of committing an "old fashioned" fraud are able to commit a computer-related one if given the opportunity.

## computer-related crime.

The July-August 1975 issue of the Harvard Business Review offered an "Embezzler's guide to the computer". Its author Brandt Allen presented a collection of both factual accounts and perhaps mythical stories[54] of abuses perpetrated using computers. In a note of encouragement to the individual considering criminal action, the introduction stated that:

> *The really big, successful embezzlement schemes are still out there working well. Most of the people who have been caught owe their capture not to the lack of their computer skills but to bad luck and mis-management. (Allen (1975) p. 79)*

This statement, whilst impossible to prove, may have some basis in truth. Computer crime was a popular press topic in the late 1980s and early 1990s, leading to many anecdotes about hackers and viruses. Dr. Popp, Nicholas

[54]The term "potentially mythical stories" is used as such cases are often difficult to validate. System managers and their employers are often very reluctant to admit such "attacks", and the cases may never make it to court as the perpetrator is never caught or a deal is struck before any legal action is taken. There is also no central record of computer attacks so that it is impossible to identify the true extent of this problem.

Whiteley and Robert Morris all made high profile court appearances that made headline news in the UK and the USA, whilst viruses such as "Friday 13th" and "Michelangelo" offered a faceless threat to the Computer Age. Whilst it is true that the potential of computer-aided criminals is immense if they are allowed a free hand, most computer users are not as helpless as some commentators would have us believe.

A number of the most high profile incidents of hacking and corrupting viruses have resulted from poor computer use by the legitimate user rather than the technical experise of the perpetrator (although some may be at an advanced level). One of the most notable cases was that of Robert Tappan Morris Junior, or "rtm"[55] as he is known to his friends. Morris is the son of a former Bell Company scientist turned National Security Agency advisor. He had grown up with computers as his father had a terminal at home linked to the Bell Company network. So, whilst his classmates learned to use Apple Macs, he got to know some considerably more sophisticated machines. He graduated from Harvard to Cornell where he conceived of the Internet Worm with the intention of highlighting a flaw in the Berkeley UNIX operating system (Hafner and Markoff 1991, Sterling 1992). The worm, that was never intended to be malicious, was released into the network in the evening of 2nd November 1988. It eventually affected a large number of computers linked to the Internet and the total cost of the "fire-fighting" operation is estimated by some to be enormous. Estimates range from zero, due to its highlighting security flaws, to $96 million by one industry group (Hafner and Markoff, 1991).[56]

There are two important lessons to be learned from the above case. First, the worm relied on a weakness in the security of the system, which had little security due to its nature[57]. Secondly, this weakness was identified from

[55]His computer login.

[56]Morris was eventually convicted and sentenced to 3 years probation, a $10,000 fine and four hundred hours community service.

[57]The Internet is a network designed to be accessible to many users and is much used by academic institutions. Referring to the lack of security at such institutions, Cliff Stoll stated: "Sure, it's easy to muck around computers at universities where no security was needed.

reading public literature on the Berkeley UNIX program and from knowledge acquired from Morris's experience of the system. A good example of the significance of this is the use of default passwords. It is the responsibility of system managers to change these passwords once the system is up and running, but many users are lax in this regard. Reading the manuals to these systems will often inform any interested party of the default password and any hacker will try this first as it has a high chance of success.[58]

A more chilling story is that told in Clifford Stoll's 1991 best-seller, "The Cuckoo's Egg", which tells of an "attack" on the military network of the USA; the "War Games"[59] scenario coming true? The intruder was apprehended and transpired to be a resident of East Germany who was gathering information, as part of a gang, to sell to the KGB. His presence was only noticed due to a 75 cent accounting discrepancy and Stoll's stubborn pursuit.

## types of computer-crime.

Both of the incidents mentioned involved highly computer literate individuals who stumbled upon systems that had inadequate security. They were both crimes that few other people could have been committed and are true computer crimes in that they could not have committed without a computer. There has been much discussion about what constitutes a computer-crime (see Wasik 1991) and as there are many acts that may be termed "computer crimes", there are obvious benefits in classifying them. All may be motivated in different ways and require different skills to perpetrate. This author proposes three distinct categories: computer exclusive crimes; computer dependent crimes; and computer involved crimes. The first category relates to crimes committed by Elite computer criminals and Copy-cat criminals, whilst the latter two may be categories of Naïve computer criminals.

---

After all, colleges seldom even lock the doors to their buildings." (Stoll 1991, p 12).

[58]When changing the password managers should be careful about words chosen. The best passwords have a mixture of letters, numbers, and where available, symbols, although some systems only accept alphanumeric passwords. The manager should avoid passwords with some personal meaning as these may be easy to guess.

[59]Warner Home Video (1984).

It would be impossible to commit a computer exclusive crime without a computer owing to the nature of the crime. Hacking and virus writing are good examples of such crimes, as evidenced by the fact that the authorities had to create new laws when the existing legislation failed to cover the offences effectively. This type of computer crime gains the bulk of the media attention but represents only a small portion of the total number of computer crimes committed.

Computer dependent crimes are crimes that require the technical capability of a computer because of their size or complexity. The best example of this is the Equity Funding Corporation fraud in which 64,000 policies, out of a total 97,000 that the company had claimed were current, were found to be bogus (Seidler, Andrews and Epstein 1977). The company had been creating "new" policies so that they could sell them in the secondary market for cash. The computer was used to keep track of the scam and to maintain the policies, using some of the cash received to pay the premiums on the policy. The fraud was quite simple in nature but would have been impossible without a computer unless more people were involved.

Computer involved crimes involve use of computers but are not computer exclusive or dependent. Typically the computer is central to the environment where the crime was committed. Input frauds are a good example of such crimes. The change from manual book keeping to computer maintained accounts has meant that many frauds once committed under the old systems now involve computers. Input frauds are the most commonly recorded form of all computer crime (Audit Commission, 1987, 1994).

Whilst stories of computer wizards and cyberpunks[60] "jaywalking" or trespassing in the computers of corporation are numerous, the extent of

[60]Such terms are used by many to describe those individuals with the necessary skill to enter a system and navigate their way through the networks, especially entering areas that will yield further information and that are prohibited to them. John P. Barlow (quoted in Scientific American September 1991 page 112) described cyberspace as: "a frontier region, across which roam the few aboriginal technologists and cyberpunks who can tolerate the austerity of its savage computer interfaces, incompatible communications protocols, proprietary

reported damage, whilst potentially great, has so far been minuscule in comparison to theft by employees. There have been a number of attempts to catalogue computer crimes over the last twenty years (Norman 1983, Audit Commission 1985, 1987, 1994, et al). They invariably make interesting reading but are often littered with input frauds and other frauds requiring little technical knowledge or ability. The majority of employees are not sufficiently computer literate to commit any but the most simple of computer crimes. For this reason, employers should be more concerned about the problem of input manipulation and similar frauds, rather than the problem of possible "salami" frauds[61]. A lack of computer knowledge is not a problem. Allen (1975) offers advice to those considering perpetrating such an act:-

> *... it does not really matter what industry you are in or whether you work for a profit-orientated, governmental, or not-for-profit group. It does help, however, if you are in a position of responsibility and are a 'trusted' employee - the greater your responsibility, the better. Knowledge of basic accounting, record keeping, and financial statements is also necessary, though the same is not so of the computer. You are in the ideal position of not needing to know a lot about computer technology in order to beat it. The auditors and management must, however, know a great deal in order to catch you at it. The best embezzlement schemes have to be well executed to work, but the ideas are simple. (Allen (1975), p.81)*

The reality, in the most part, is that it is a breach of trust that leads to computer crimes and that the majority of these are input frauds; they are computer related rather than computer dependent. Whilst there are indubitably computer users with virtuoso skills, these are few in number and are as adept at information gathering as they are at pure hacking. Information about system procedures is gathered by methods such as "social engineering"[62] and "trashing"[63] and by reading computer system manuals. Organisations can improve security with a number of simple steps in order to

---

barricades, cultural and legal ambiguities, and general lack of useful maps or metaphors."

[61]A fraud where only small sums are taken from many accounts. The sums are so small that they are unlikely to be noticed as missing and taken from a great number of accounts to make the fraud worthwhile.

[62]"Social engineering" works well in large organisations. Using the organisation's hierarchy it is possible to make a junior employee believe you are more senior and thus reveal information which is either sensitive in itself, or which may be used to validate a further request for information from another employee. Seeming credible can be very rewarding.

[63]"Trashing" involves delving in the waste of organisations. Many organisations discard waste that contains information that is of great value to hackers.

prevent outsiders accessing the system. But what of the insider intent on fraud.

# Chapter 9
## Summary and Discussion

*Fraud has a unique glamour in the range of criminal activities. There is no violence. There may be no readily identifiable victim. There may be a sneaking regard for the fraudster's ingenuity. The methods used to conceal the crime may, at least to the accountant and lawyer, contain the intellectual interest of a detective novel. (Huntington 1992, Preface vii)*

*"A good deal has been written in the last decade about the links between organisational strategy and culture, the problems of strategic inertia in firms, and the need for managers to manage the cultural context of the organisation so as to achieve strategic change and an adaptive organisation to sustain the change for long-term success." (Johnson 1992, page 202).*

### introduction

In this chapter a summary of the findings of this thesis will be presented followed by a discussion of their implications for the banking industries in particular, and those other industries that have *trust-based* relationships more generally. The summary will include a discussion of the strengths and weaknesses of the approach adopted as well as offering areas for further research.

### summary

The purpose of this thesis, as has already been stated, may be summarised as follows:

1. to review existing knowledge of the issue of crime management in banks
2. to review existing knowledge of the issue of employee motivation
3. to look at the problems inherent in the changing of the culture or strategy, with particular reference to the banking industry and the changes it has experienced in the 1980s and the early 1990s.
4. to create a knowledge map of the process and to highlight the areas that should be of interest to bankers
5. to assess the areas of most important attention when making the changes that the banks wish to make in their strategic direction

The reasons for doing this were that such work should help managers in the banks focus on the real problems - motivation problems - and understand

better when employees are dissatisfied or disenfranchised. The importance of this research lies in the fact that it offers an overview of the processes that impact upon the bankers' environment and the banks' internal cultures.

This research tests a number of hypotheses that are both stated and implicit in some of the assumptions made. The hypotheses may be summarised as follows:

- bank clerks are inherently moral - non-deviant
- banks' security has been dependent on this morality
- the banks' recruitment campaigns have been successful in attracting individuals with an appropriate personality profile
- banks have offered tenure for the loyalty and commitment of their staff
- the culture was service oriented
- the culture was paternalistic
- that change in such a psychological contract will have an impact on the trust/loyalty factor - a change that the banks do not yet comprehend
- that change in the culture will require a new employee profile
- the banks' management understand the new culture no better than they did the culture of the City during the post-Big-Bang period
- that the Computer Crime threat from the Outsiders is less of a threat than the threat from financial mismanagement and incompetent lending
- that the true Computer Crime threat comes from employees - especially the Outsiders that banks employ
- as employees' ability increases their opportunities to perpetrate non-input computer frauds will increase

## problems of the research

This research was not without its problems. Research of this nature is difficult to achieve. There are a number of reasons why this might be so:

- sensitivities of an opinion/attitude survey
- closed nature of banks' computer systems
- the impact of the increasing prevalence of a sales culture
- confidentiality to customers creates an ethos of secrecy
- an ethos of secrecy creates reluctance to discuss internal issues with outsiders
- fear that the information gained through the research will be misused
- what you can't look at is the opportunities for employees to commit crime within the system

- perhaps a belief by the banks that their systems are so good that there aren't any opportunities
- reputation is all - discussing the issue opens up the possibility of the impossible occurring!

To my knowledge the banks have never published information about their computer systems - therefore it was impossible to conduct an Internal Audit on the system to assess risks. Therefore an approach was adopted that focused on the personal aspects of the system - the human interface within the branches.

As a result of the reluctance of many managers to commit their branches or regions to the research and the budget restrictions, the research is neither comprehensive in its scope nor national in its focus. The thesis can therefore be criticised as:

- having a geographical bias, or
- needing a stronger reference group or greater information about the population nationally.

## notes on the structure

The structure of this thesis is far from conventional but it is need driven and is intended to provide an easy reference for readers interested in the various areas that this thesis covers. Because of the difficulties noted above a highly exploratory approach has been adopted in an attempt to highlight the problems which are of a multi-disciplinary nature. This thesis touches upon the following subjects:

- General management
- Strategy
- HR management
- Motivation
- IT management
- Computer audits
- Risk management
- Communication
- Marketing
- Criminology
- Sociology

The author claims an interest in each but no great expertise, consequently some of the conclusions reached in any area may seem somewhat naïve to the expert in these fields.

As a result of the difficulties listed above and the variety and range of issues that are dealt with in the thesis it was felt useful and effective to conduct three pieces of research. The first study was originally intended to form the main body of the work without the addition of the other two but it soon became apparent that it would be difficult if not impossible to gather sufficient data to conduct a national survey and any bank based survey would have political implications as regard to confidentiality of results.

The second area of research had its share of difficulties with regard to the issue of the use of the Internet and eventually ran into a brick wall when the account manager threatened to withdraw the author's account if he continued to make cold approaches to individuals over the Internet. The data collected to that point was exceedingly interesting but lacks global statistical credibility. That said the results make interesting reading and have value for those with an interest in the issue of "what is a hacker?"

For the third area of research a case study approach was adopted. The purpose of these studies was to highlight the importance of understanding the culture that your employees operate within. The information gained from these three areas of research may now be used to develop the Model of Motivation further.

## model of motivation

The second chapter of this thesis proposes a model which draws on the work of Fishbein & Ajzen (1975) and applies it to a corporate environment. It maps the pressures that individuals may experience from this environment. The pressures relate not only to the effect of authority but also the hierarchical nature of many organisations that may create circumstances where

obedience is expected or believed to be necessary. The work of Milgram (1963), Asch (1956) and Janis (1972) has shown how such relationships can affect the behaviour of the individuals involved.

The Fishbein and Ajzen motivational model highlights the relationship between an individual's *Attitude Toward Behaviour*, their *Subjective Norm*, and their *Intention* to behave in the way considered. These three factors are related with the *Intention* being an outcome of the individual's weighting of the relative importance of the other two factors. Their *Attitude Toward Behaviour* is affected by their belief that the behaviour will achieve a desired outcome, thus satisfying a need. In figure 9.1 this has been altered to read merely *Attitude*.

The second causal factor, *Subjective Norm*, represents the effects of societal norms and local norms on the individual. For the case of white collar workers in general this has been changed to merely read *Pressures*. These pressures may be *Supportive* or *Preventive* of a particular action. As in the original model it is proposed that the net effect of these two factors would then be compared for relative strength with the *Attitude* of the individual. Even when the *Intention* has been established it is still possible that the action will not be executed as the individual must have the skill and the opportunity to do so.

Before considering some of the pressures that were highlighted by the surveys it is worth briefly commenting on the implications of such a model for the employers of white collar employees, especially those in trust-based environments. If you remove opportunity, or make the skill level required extremely high, you reduce the potential incidence of crime. If you are unable to do so then consideration should be given to assessing the pressures that the employees face. Not so long ago the banks were also able to assess an individual's possible attitude to a certain behaviour. Up to 1985 it was an offence within Barclays Bank to have an account with any other bank and you faced disciplinary action if your account was overdrawn with the bank. The

bank was therefore able to see those members of staff who were facing financial difficulty. The bank's management could therefore identify employees who, whilst being generally moral, might be experiencing pressure to take from their employers so as to relieve financial pressures in their personal life.

The two chapters following the model proposed examined, in the context of the banking industry, the factors that might affect individual's feelings towards potentially deviant behaviour, in particular they focused on the pressures - both supportive and preventive - that might affect the motivation of a bank clerk. The research conducted assumed that the majority of bank clerks were not criminal by nature - it assumed in short that the majority of employees involved were extremely moral, an assumption that is supported by the responses to those questions that related to the importance of honesty and family in the survey.

When the responses to the questionnaire were examined the three strongest factors that prevented individuals from acting in a deviant manner were: *the belief that such behaviour is immoral; what my family would think; and what my friends would think.* Factor analysis of these figures produced three clear groups of factors that may be used to supplement the model proposed. A factor analysis of the two groups of pressures reveal three distinct categories of factors for both the preventive and supportive factors. These groupings have been used to develop the model in figure 9.1.

This model may be used to explain how a moral individual might feel the pressure to commit a deviant act. When the changes that are outlined in chapters 4 and 5 are considered it is possible to conceive of circumstances where crimes might be committed. Whether there is a crime-wave in the banks as a result of the changes that have occurred is something that would probably go unreported because of the banks' obvious reluctance to announce such cases. It is possible to conclude if the respondents to the

survey are typical of the general population of bank employees that there is no crime-wave and that they are prevented from committing such acts because of a strong sense of what is morally right. In other words, the existence of strong *Preventive Pressures* outweighs most desires or temptations to deviate.

## business deviance

From the analysis of this process it was clear that the motivational model for an individual acting out of self interest would be different from one that represented the actions of an individual acting for a company or acting in a way that they feel uneasy with because of potentially criminogenic pressures. The first part of the thesis therefore sought to focus on different categories of corporate crimes. The second chapter presents three distinct categories of business deviants:

1. Endogenous business deviants;
2. Exoteric business deviants; and
3. Exogenous business deviants.

Broadly speaking these three categories represent a risk of crime from within (Endogenous) and from without (Exogenous), as well as from within on behalf of the organisation (Exoteric). The motivational model is appropriate for an endogenous act, partially appropriate for an exoteric act, and inappropriate for a exogenous one.

Each of these categories was considered to a greater or lesser extent in the thesis. The greatest attention rests on the first category as this includes crimes committed by employees against their employers, crimes that are of particular interest when the changes in the role of bank clerks is considered. Such changes have had a radical effect on the working lives of potentially hundreds of thousands of employees.

## computer crime

Chapters 6 to 8 consider the act of computer misuse which represents a good example of a potential threat from an exogenous business deviant. Cases were cited and a survey undertaken to discover the likely profile of a computer criminal. The moral code assumed by many individuals who commit deviant acts using computers is somewhat amoral by the standards of society as a whole - they tend to challenge society's concepts of right and wrong. They may do so because they disagree with society's standards and feel that Cyberspace offers an opportunity to reinvent society, but most crack or commit other computer misuses or crimes for the thrill of it.

These chapters categorised computer crime into three broad categories:

1. Elite computer crimes
2. "Copy-cat" computer crimes
3. Naïve computer crimes

The risks associated with the first two categories of crimes are exceedingly hard to assess due to the difficulties associated with detecting them, consequently, it is very difficult to build systems that are free from any risk of attack. The risk of the third category - that of naïve computer crimes - is easier to evaluate but potentially impossible to defend against as the number of people with the necessary skill level is very large.

On a more practical level these chapters highlight a number of categories of computer misuse and advocate a different approach to each. For the assessor of risk to companies the low-tech crime may actually represent the most likely risk. Such crimes are apparently more frequent if the figures of the Audit Commission (1993) prove to be representative. The problem with such surveys is that the high-tech crimes may go completely undetected, or when detected may be covered up for fear of "copy-cat" attacks.

This middle category of "copy-cat" requires some computer user knowledge but little skill in comparison to the high-tech elite crimes. The low tech crimes require even less skill and are therefore a more current risk for the banks. One of the purposes of this research was to assess the possible risks faced by banks from insiders. The majority of bank employees are unlikely to have the skill to commit a high-level computer crime. Also if the profile of the average bank clerk is compared with that of the average computer cracker a disparity becomes quickly apparent. Banks have traditionally attracted a different mentality than has the world of computers; that said it is still possible to conceive of an internal computer crime risk as the naive or low-tech crime requires very little skill to perpetrate.

## changes and risks in the banking industry

In this section the risks facing the banking industry will be considered in general and more particularly with regard to the changes banks currently face or have chosen to undertake. Chapters 4 and 5 of this thesis focused on the changes that have occurred in the banking industry of the 1980s and early 1990s. The changes may be summarised as follows:

**Before:**

- Service oriented
- Life-time career
- Branch-based processes
- Paper-based operations

**After:**

- Sales oriented
- Short-term contracts
- Increasing use of part-time staff
- Increasing centralisation and clustering
- Computer-based operations

Banking is a risky business without taking into account the risks associated with the changes highlighted above. Huntington (1992) identifies three types of generic business risk:

1. Inherent industry risk
2. Environmental risk
3. Business risk (Huntington 1992, page 3)

He argues that inherent industry risks may be found in industries where a variety of factors or characteristics are evident. Four[64] of these are particularly relevant for the analysis of risks in the retail banks:

1. Financial structure
2. Secrecy
3. Transaction volume
4. Market conditions (Huntington 1992, page 4)

## financial structure

When the industry demands a relatively high risk financial structure there is an inherent industry risk of fraud. Highly geared businesses must maintain the confidence of lenders if they are to continue in business. The banking industry is by its very nature a highly geared business - it takes £ billions in deposits every year to lend on; its equity level in comparison is very small. Huntington (1992) argues that when these businesses are not performing at the required level that there is likely to be a pressure to misrepresent the position to maintain the confidence of the lenders.

## secrecy

When confidentiality is an important part of the product or service the risk of fraud will be higher as there will be fewer people in a position to detect irregularities. The banking industry has been notorious in its endeavours to maintain secrecy. The duty of confidentiality has been a fundamental tenet of banking since the case of Tournier v National Provincial and Union [1924][65] which established a duty of care on the part of the banker not to divulge information pertaining to his or her clients' affairs.

When confidentiality offers a cover for potential frauds it is imperative that the internal measures employed by the organisation concerned are of an excellent standard. This represents a potential problem for the banking

[64]A fifth is relevant to some banks trading in more specialised areas - New and Complex Products - for an example of this one may think no further than to Barings et al that have lost money in the derivatives markets.
[65]1.K.B. 461.

industry as many banks are moving from people based systems to computer based systems in the belief that these are more reliable and less costly to maintain. Whether this is true or not has yet to be seen.

## transaction volume

The volume of transactions that the banking industry handle each year has increased quite dramatically with the improvement in computer power and the increasing use of computers by the banks and their clients. This has led to an increase in the number of opportunities for the perpetration of frauds by the banks' employees.

> *Risk is inherent in those industries in which there is a high volume of major transactions involving the movement of financial assets and liabilities by book record rather than physical assets. (Huntington 1992, page 4).*

One of the greatest areas of growth evident in the retail banking industry has been in the area of CHAPS payments - in 1993 the system carried more than £23,000 billion of payments. It is not uncommon for an individual payment from one bank branch to another to be in £ millions - if the origination of this payment is not handled and monitored properly an opportunity for fraud may arise.

## market conditions

The fourth of the factors listed by Huntington (1992) is particularly appropriate for the banking industry:

> *Industries in which market conditions have become unusually competitive may be at a greater risk of fraud than those operating in more stable conditions. The need to succeed may drive management and employees to take risks, such as indulging in fraudulent practices. Sharp practices may be condoned by management, leading to a general breakdown in control consciousness and morality in the business. (Huntington 1992, page 5).*

The actions may also be such that they lack criminal intent but lack the normal measures of prudence expected of bankers. A possible example of

this is the lack of appropriate controls in Barings that allowed Leeson to build huge positions that eventually lead to the bank's collapse.

It is clear that the banking industry is a high risk industry. It has a highly geared financial structure; it owes a duty of secrecy or confidentiality to its customers; it handles a very high volume of high value transactions every day; and it is experiencing greater competition both from home based organisations and foreign financial institutions. It has also changed the roles it expects many of its employees to fulfil thus creating an environmental risk.

This final risk is perhaps the one the banks will find hardest to quantify. The other four risks may be easily managed with the skills and prudence that British Bankers have been historically renowned. The final one is a new risk and is associated with the very core of a trust-based organisation. With the move from a long-term approach to employment to a more flexible firm approach the banks may also have to reassess the basis of their trust.

## trust

The banking industry has for long relied on a mixture of good procedures and trust to maintain security in its branches. The banks' commitment to long term employment allowed them to develop relationships of trust with many of their employees. With the move to a smaller cadre of long termers and more short term and fixed contract staff this must change. Handy (1995) warns that:

> *"**Trust is not blind.** It is unwise to trust people whom you do not know well, whom you have not observed in action over time, and who are not committed to the same goals." (Handy 1995, page 44)*

With the increasing use of fixed term contract employees and a decline in the number of career bankers and bank clerks the banks will have to reassess the amount of reliance they place on the trustworthiness of employees.

When employing a long term employee the banks would spend a great deal of time and effort assessing the potential candidate. Once selected and after satisfactory references were received a new clerk used to be able to expect to spend a number of months, maybe even years, in the sorting rooms before they could expect promotion to cashier. The opportunities to commit crimes in the first couple of years were minimal and the work was often extremely tedious, but the graduate of such a system was very aware of the standards expected of them and was part of a group with a very strong norm. Such an approach has changed and with it must change the banks' reliance on trust. Or the banks must find new ways to establish the trust base, new ways of getting to know their employees - employees who do not expect job security or long term employment.

## return of the middle manager?

One of the reasons that opportunity might increase in the banks is due to the loss of middle managers and supervisors. The middle managers and supervisors were responsible for managing the staff and their inputs. An office manager would be responsible for discipline and would speak to those staff whose personal accounts were overdrawn each morning.

Entries would be signed by supervisors and another middle manager before they were input. They focused on the accuracy of the documentation and made sure that there was an appropriate audit trail for each item. Where the instructions for a transfer were received over the telephone the manager might confirm the instruction with the customer before authorising the action. All of the above reduced the opportunity for fraud.

> *"The move to flatter organizations has taken out layers, and many so-called middle managers took the hit. Companies responded to cost pressures by getting rid of people with only coordinating roles. But plenty of middle managers survived, and some of the best executives we know are looking at them from a new perspective. They see, not hapless pencil pushers, but rather a value-adding resource at that unique place, the middle, which offers a 360 degree perspective. Middle managers are in the best spot to integrate the corporation because they can translate strategy into execution." (Price Waterhouse 1996, page 151).*

On another level this loss has an impact on the motivation of employees as their promotional opportunities decline.

## computers

The computer is one of the villains in this piece but has also been a hero:

> *"The computer came as a godsend to the banks, when social change stopped up the source of qualified clerks of the type portrayed by Jack Lemmon in the film The Apartment or Frank Dickens in the Bristow cartoon strip. Rather than reconsidering training procedures or pay scales, so as to attract back those who would have become bankers but had gone to university instead, senior bankers redefined banking." (Taylor 1993, page 197)*

Taylor (1993) argues that senior managers drew on wartime experiences to create units to undertake various functions and to adopt a "*production line*" approach. The "*cannon-fodder*" in this approach were young girls whose ambitions did not extend much past marriage.

> *"The second stage of reorganisation was to develop staff and head-office functions, so as to make these jobs attractive to graduates, and to support or supplant branch-management structure. This led to confusion among customers and bankers alike, for, though the branches looked the same, these steadily lost the knowledge and authority once incorporated in their professional staff. From the 1960s onwards banking ledgers were replaced with computer files and, with banking split into barely understood functions, handled by ill-paid and under-trained functionaries, any decision of importance was referred up the line. Henry Ford would have been proud of the production-line techniques with which banking was deskilled. The arrogance of barely understood technologists then combined with the centralising tendencies of head offices and bankers were persuaded that everything else, including judgement, could also be centralised. The banks proceeded to build themselves "command and control" systems that Stalin would have envied." (Taylor 1993, page 198).*

Taylor (1993) argues that this tide turned for many banks at just the right time and computers are now used to support decisions at a local level. The benefits of computers have certainly been felt in the area of money transfer where the level of entries currently handled would be impossible with even the highest staff levels that the banks have experienced. Computers actually make banking easier and more interesting. It is doubtful whether there are many people who would like a return to ledgers and quill pens.

Computers are still the cause of why banks no longer need as many employees and why employee numbers fall further each year. They may even

be the solution for the problem of trust. Computers are used to replace the monitoring functions fulfilled by supervisors and middle managers. They are used to evaluate loan requests. They may be used in a number of ways that minimise the opportunities for fraud that were present under the old system. In the long term the need for cash may even decline to an irrelevance as people become more accustomed to the use of credit and debit cards to handle their money needs. These are all changes that the computer has helped to facilitate.

With these changes new opportunities will arise as the profile of bank employees changes still further. The bank will have to employ more individuals with information technology skills and will be recruiting from a pool in which crackers also exist. The cracker may become an internal as well as external threat in the future. It is possible to imagine the banks' senior managers having difficulty managing these people just as they had difficulty coming to terms with the employees of the city institutions they purchased in the early 1980s.

This is of course merely a prediction of the future and one that is both pessimistic and optimistic with equal measure.

## mismanagement

Taylor (1993) also argues that the banks' computers and the money-markets encouraged the banks to expand into businesses other than their core ones. The addition of investment-banking services to the list of services already proffered increased further the complexity of the commercial banks (Taylor 1993).

This increasing complexity has lead to a number of large errors on the part of many senior bankers. Banks have made very large loans to the property industry and to the less developed nations, and heavy investment in

acquiring City firms which have lead to large bad and doubtful debts and write-offs:

> *"...the irresistible inertia created by the knowledge that one has money to lend steamrollers into the ground most bankers' imagination and flexibility." (Taylor 1993, page 302)*

There are those who argue that the mismanagement of banks represents a greater threat to a bank's future than threat of computer crime or the risk of employee fraud. Banks lose larger sums of money each year in the form of bad debts than they ever report in fraud. Perhaps the banks' senior managers should seek savings in that area next time they seek to reduce their costs.

## implications for practitioners: internal controls and procedures

There are a number of lessons that are offered from the findings of this thesis. On the whole the best "cure" is prevention and in the case of crime management that means ensuring robust internal controls and procedures to ensure that the opportunities to commit crimes are minimised. The findings of the research that this thesis draws upon may be summarised as follows:

1. Clear roles and responsibilities for all employees
2. Clear lines of reporting
3. Regular staff rotation - regular rotation ensures that staff are not given the opportunity to set-up "systems" to cover up fraud
4. Job holidays - due to the nature of some roles it is impossible to rotate all staff, where this is the case the staff should be relieved by another member of staff for a period. This ensures that the back-up staff are kept up-to-date as well as decreasing the opportunity for fraud
5. Investigate warning signs - when staff fail to take a holidays it could be because of commitment to or pressure of the job, it could also be because they are unable to leave without reveal shortfalls in their accounts. Such instances should be viewed seriously
6. Preparation, authorisation and input should be separate - ensure that no one individual is able to prepare, authorise and input documentation. Splitting these three roles ensures that the chances of input frauds are reduced. DO NOT split the roles so that preparation and input are undertaken by the same person as this offers opportunities for input fraud, unless the authorisation has been coded for the document details as in the case of the CHAPS payments hexadecimal coding of input details to authorise payments

7. Conduct random checks of documentation input and output to ensure consistency
8. Internal Audit departments should be given autonomy from management
9. Ensure proper staff selection procedures are observed
10. Conduct regular training and update sessions for ALL staff to ensure that they follower the procedures
11. Train supervisors how to spot the warning signs
12. Do not trust blindly - trust must be earned, and trust relationships should be reviewed regularly
13. DO NOT assume that your staff's skill levels are too low to commit a fraud or that they will remain so
14. MANAGE MOTIVATION

The points raised above are well supported in practice within risk management systems and procedures. The last three are perhaps less apparent from such systems as they are dependent on the line manager's relationship with his staff.

The banks' internal control procedures have not been reviewed in this thesis because of a lack of opportunity on the part of the author. That said, first hand experience of the procedures of one of the major clearing banks, if representative of the whole industry, indicated that they were pretty comprehensive in their scope. Indeed, one of the motivating factors for undertaking this research was to consider what would happen if the culture ceased to regard them as important, favouring sales generation to the "paper work". Procedures, no matter how global in scope, are only as good as their execution.

## implications for practitioners: impact on strategy

> *"The notion of strategy is to do with the long-term direction of the organisation and not just the response to difficulties... The evidence from research which has looked at the decision processes that give rise to strategic decisions and the development of strategy in organisations, shows that the decisions arise through the application of managerial experience as a filter of external and internal stimuli, within a politicised social setting."* (Johnson 1992, page 29).

This thesis has argued that the banking industry has changed and that the banks therefore need a new paradigm. Johnson (1992) defines a "*paradigm*"

as the "*core set of beliefs and assumptions*" held by the members of the organisation (Johnson 1992, page 29) and argues that "*It is this which, in many organisations, creates a relatively homogeneous approach to the interpretation of the complexity that the organisation faces.*" (Johnson 1992, page 29).

Whether or not the banks have an appropriate new paradigm for the new environment is yet to be seen. One thing that can be said with certainty, is that they need one if they are to develop the appropriate strategy. If they do not develop the necessary paradigm they will suffer from what Johnson (1992) terms "*Strategic Drift*".

> *"In these circumstances it is likely that, over time, the phenomenon of 'strategic drift' will occur: that is, gradually, perhaps imperceptibly, the strategy of the organisation will become less and less in line with the environment in which the organisation operates." (Johnson 1992, page 33).*

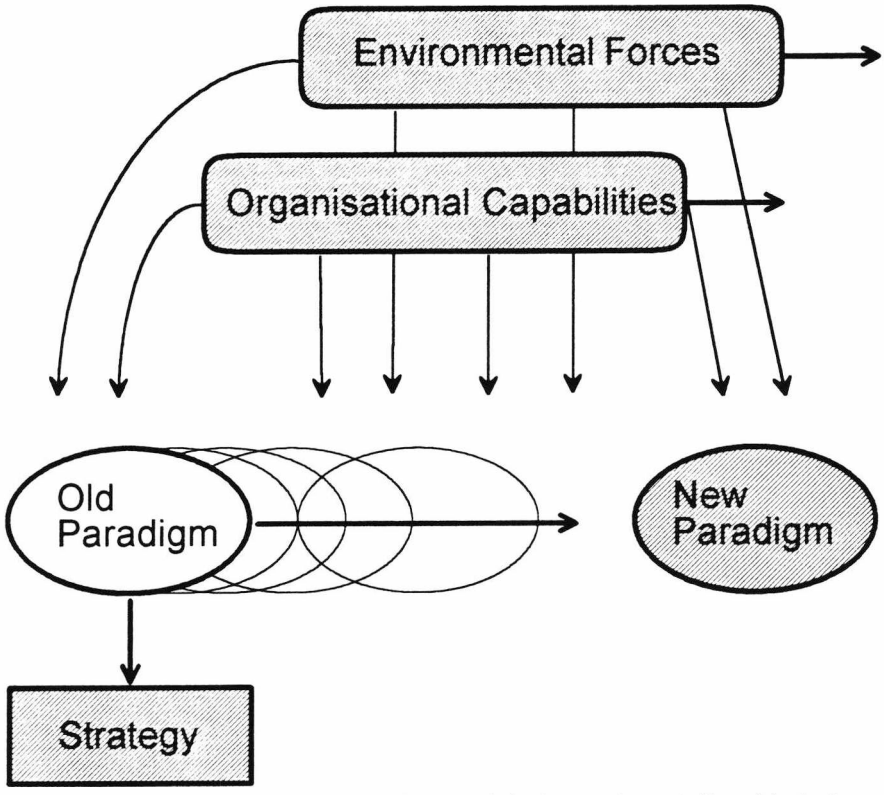



Figure 9.2 shows the relationship between the paradigm and strategy. Based on Johnson 1992.

Figure 9.2 is a graphical representation of strategic drift. As the environmental forces change or the organisational capabilities change the paradigm is impacted upon. Unless the banks react to these pressures and develop a new paradigm they will not have the ability to develop an appropriate strategy. Alternatively, if the senior management sense a need for change they must find ways of influencing the paradigm of their sub-ordinates to ensure that the new strategy that they formulate will be implemented effectively.

> *"This raises difficulties when managing strategic change, for it may be that the action required is outside the scope of the paradigm and the constraints of the cultural web - that members of the organisation would be required to change substantially their core beliefs or 'the way we do things around here'." (Johnson 1992, page 33).*

If the banks do not develop the necessary paradigm they will have problems both with their success in the market and with how they handle their staff. Managing the motivation of their staff may offer them the answer to many of the problems that change brings.

## further research

Drawing on the findings of this thesis it is possible to suggest a number of areas for further research.

## further research - Model of Motivation

The model proposed in this thesis could be tested in another environment, preferably one that allowed fuller observation. Perhaps the National Audit Office might consider sponsoring its use in a location or network of offices.

## further research - banks

A number of weaknesses in the research that underlies this thesis have been acknowledged earlier in this chapter. Research could be conducted that sought to mitigate these or expand on the information gained. Firstly, a second visit to the study group could be undertaken to assess whether time has affected their attitudes

Secondly, a national study of all bank clerks and managers could be undertaken thus overcoming any geographical bias experienced by the current sample. It is possible to suggest that this be done through the Chartered Institute of Bankers but, whilst the sample would be national, it may bias the results as more senior bankers would be involved rather than a representative spread of ages and experiences.

To overcome that bias, BIFU or another employee representative body might be approached to sponsor the data collection. This sample would also be biased as the respondents are likely to be the more active union members.

The banks themselves might be appraoched. This survey is likely to be more representative of the staff as a whole but this might be hard to achieve unless it was to be on behalf of the banks and for their own use. This would of course limit the academic applications because of the confidential duties that the researcher/consultant owes the client.

## feminine nature of banks

When a young male banker joins as a school leaver he will spend his early years in a department probably run by a woman and surrounded by women with virtuoso typing skills and the ability to input document information at great speed. Contact with other males will probably be of a limited nature or with those males in the early stages of their career. The females employed in these "machine rooms" or account departments are unlikely to have a chance of promotion above the clerical grades whilst the male historically could expect to make manager. In the 1970s it was possible for a male joining the bank to predict a managerial appointment of one sort or another by his retirement.

A fast track joiner might spend only a couple of months in the machine room before joining the till. The cash tills in banks represent a promotion and are again run by a female in many branches. Here again the young male will experience a female dominated environment. The best of the fast track entrants will expect to make it into the loans department or the securities department in his second year. Others may have to wait until they are well into their twenties. Only when they reach this stage will they be in a predominantly male environment.

As branches have consolidated and merged this division between the various departments, and particularly between senior and junior ones, has become more marked. The division may even be geographical as managers and securities departments are moved into management centres in the business areas of many towns leaving the administrative departments and customer contact points located in the high street.

## further research - computers

Stage 2 - the structured part of the survey - could be undertaken. The purpose of a Delphi study is to put the information gathered in the qualitative

free-form stage into a survey instrument that may be used to gather quantitative data. Whilst it is possible to seek responses to the survey on bulletin boards and USENET there still remains the problem of validating the experience and expertise of the respondents.

### further research: impact of computer based organisational transformation in other industries

Technology has been the change driver in a number of other firms and industries. Management Consultancy firms have used products such as SAP and Oracle Financials as the catalyst for organisation wide business process re-engineering (BPR). What opportunities might such change offer to Outsiders within these organisations?

# Appendix A

This appendix contains the responses from the survey of computer users.

## questionnaire

Please could you help me with a Delphi study I am conducting as part of work for my PhD. I would be grateful if you could answer the following short questionnaire:

1a. How long have you been using computers?

1b. What major operating system, such as UNIX, would you say you are most experienced with?

1c. Are you male or female?

2a. Have you ever hacked into a computer system on which you do not have authorised access? Your answers will be treated in strictest confidence!

2b. If YES, do you feel that your activities were ever illegal?

2c. Immoral?

2d. Do you feel that such activities fulfil a positive purpose?

3a What skills do you feel a good cracker needs?

3b What would you say their main motives are?

3d Do you feel that their activities are beneficial or harmful to society?

3e Why?

4a What activities would you class as Computer Crimes?

4b Do you have any examples of such?

5 Do you have any further comments that you wish to make?

## responses

01, Male, 29 yrs exp, Unix, No

3a What skills do you feel a good cracker needs?

*patience*
*willingness to experiment*

3b What would you say their main motives are?

*curiosity*
*feeling of power*

3d Do you feel that their activities are beneficial or harmful to society?

*So far, neutral*

3e Why?

*Computer systems are subject to accidental failures as well as those caused by malicious agents. Crackers have forced the user community to look for more robust systems. Eventually we may get to well-designed capability based systems.*

4a What activities would you class as Computer Crimes?

*theft of services (minor)*
*theft of data (moderate)*
*computer aided fraud (major)*
*destruction of data (major)*

4b Do you have any examples of such?

*Mine was one of the many sites bothered by the RTM worm. I've also had users capturing other users' passwords.*

5 Do you have any further comments that you wish to make?

*Regarding 4a, we still have no good mechanism to measure the cost of theft of services and theft of data. The cost of "theft of services" should not be reckoned as the billable rate unless denial of services can be shown. The cost of "theft of data" should not be the cost of collecting the data (as has been suggested by some). Only fraud and destruction of data should be regarded as major crimes.*

## 02, Male, 25 yrs exp, Unix, No.

3a What skills do you feel a good cracker needs?

*minimal sense of ethics. minimal respect for other folks property and privacy. And a lot of patience and persistence.*

3b What would you say their main motives are?

*Beats me...*

3c What percentage of crackers are male?

*Dunno*

3d Do you feel that their activities are beneficial or harmful to society?

*mostly harmful. At best they are neutral [i.e. in the spirit of the NBA's "no harm no foul"]. Hard to see 'beneficial'.*

3e Why?

*Harm is easy: even if they do no actual harm at all, if they have meddled into a system that contains any private or confidential information, or any information that could lead to [or weaken] other systems they will have left a LOT of uncertainty behind as to exactly what [if anything] they did. Just dealing with that uncertainty can cause a far amount of expense and nuisance [e.g., getting all of 800 users to change their passwords].*

4a What activities would you class as Computer Crimes?

*I don't know, actually. While i understand that the analogy isn't really on-point, I am inclined to view computer systems as 'property', and so I tend think we ought to have "computer crimes" that by and large parallel the obvious 'property' crimes [trespass, vandalism, conversion, etc].*

4b Do you have any examples of such?

*Sure — the 'internet worm'. It hit us [BBN] and caused us a nontrivial amount of expense to deal with. A significant part of that cost was figuring out what the worm did [or didn't] do. I'm not at liberty to discuss what happened at BBN or what we did, but we did sever our network link [which was a business cost right there] and worked to figure out what the worm did to ensure that in the time before we isolated ourselves from the net nothing was compromised and we also had to make sure that nothing was corrupted and that no traps or other nasties were left behind. All of this cost us a fair bit of effort, and the secondary cost [of having a fair number of systems unuseable while we sorted it all out].*

*I don't see why this kind of thing should be any less of a 'crime' than it would be if you came home and found a "guess what I did" note taped to your refrigerator: you know someone has been in your house [and you might even be able to figure out how they got in], but you have no hint as to what [if anything] they did.*

## 08, Male, 27 yrs exp, Unix, No.

3a What skills do you feel a good cracker needs?

*Patience, detail memory, general OS knowledge*

3b What would you say their main motives are?

*Personal glory.*

3c What percentage of crackers are male?

*99.5 or so.*

3d Do you feel that their activities are beneficial or harmful to society?

*Harmful.*

3e Why?

*We expend resources blocking them, they force us to make access policies more restrictive, they damage the public perception of computer amateurs.*

4a What activities would you class as Computer Crimes?

*Unauthorized access, deliberate or reckless denial of service, deliberate or reckless damage, copying unauthorized information, Apple II, IBM mainframe operating systems.*

4b Do you have any examples of such?

*Other than widely publicized events, no. The Morris internet worm was a computer crime, for example. possibly by negligence or recklessness if we believe his claim that it wasn't supposed to get out.*

## 10, Male, 15 yrs exp, Unix, No.

3a What skills do you feel a good cracker needs?

*curiosity, persistence, discretion*

3b What would you say their main motives are?

*curiosity, challenge*

3c What percentage of crackers are male?

*90*

3d Do you feel that their activities are beneficial or harmful to society?

*harmful*

3e Why?

*lead to less openness in computer networks*
*damage files through ignorance*
*damage files through design*

4a What activities would you class as Computer Crimes?

*theft or destruction of intellectual property*
*copying of another's work for own profit*

4b Do you have any examples of such?

*only those which have appeared in mass media and on Internet*

11, Male, 20 yrs exp, Unix, yes, no, no., yes.

3a What skills do you feel a good cracker needs?

*An understanding of how the operating system and system programs work and a willingness to explore the behavior of those objects.*

3b What would you say their main motives are?

*It's hard to say. Certainly curiousity was my significant motivation.*

3c What percentage of crackers are male?

*I don't know.*

3d Do you feel that their activities are beneficial or harmful to society?

*The outcome of the crack determines the benefits or the harm.*

3e Why?

*Some cracking activities are the equivalent of children climbing over a fence to get into a school yard to play. This class activities have happened since time immemorial and serves to remind all people that the purposes of certain fences perhaps require reconsideration.*

*Other cracking activities are the equivalent of theft or "peeping". This class of activities has happened since time immemorial and serves to remind all people that some people are willing to take what is not theirs or to pry into information that they are not entitled to.*

4a What activities would you class as Computer Crimes?

*Theft of information.*

4b Do you have any examples of such?

*Stealing passwords, source code, or "competitve" information. Copying personal email.*

5 Do you have any further comments that you wish to make?

*People are integrating computers into their professional and private lives because computers are useful. Information that used to be stored on many pieces of paper (roomfuls of files) are now stored on high capacity magnetic media that fits in your coat pocket. What most people have not yet assimilated is that data stored on a computer is vulnerable to theft or tampering.*

*Computers are vulnerable to physical access. Suppose your confidential corporate files, that used to occupy five locked filing cabinets in five locked offices, are stored on a single hard disk in a locked room. Chances are I could break into that locked room simply by crawling along the "hyper space" above the ceilings of most modern office buildings. In one fell swoop, I can steal information that would not have been nearly so accessible were it still in five locked filing in five locked offices.*

*Computers are vulnerable to electronic access. Very very few people in the world understand the vulnerability introduced when connecting a computer to a network. If you are willing to take the time,*

*cracking through Novell or WorkGroups For Windows is not nearly as hard as getting a Ph.D. in computer science and possibly far far more lucrative.*

12, male, 30 yrs exp, Prime OS, Yes, no, no

2d Do you feel that such activities fulfil a positive purpose?

*Only if amusment is a positive purpose. (My last effort was logging into a system at U of Michigan that was on the net formally administered by one of my employees. He said "I found a Prime, how do I get in. I said "Try the default login and password, see if they have deleted the account." they hadn't. (We did tell the administrator that he might consider closing the hole.)*

3a What skills do you feel a good cracker needs?

*There are no "good" crackers. Sometimes they are benign. There can be benefit to discovering methods to "pick electronic locks" but most cracking is using methods developed by others.*

3b What would you say their main motives are?

*Hard to say.*

3c What percentage of crackers are male?

*Almost all, it seems.*

3d Do you feel that their activities are beneficial or harmful to society?

*Most such activity is harmless. Sometimes harmful. (Lost time due to the threat of comprimise is seldom considered by an intruder.)*

3e Why?

4a What activities would you class as Computer Crimes?

*Probing confidential material for profit or political gain.*
*Destruction of files. Denial of service to autorized users.*
*Defamation of character by accusation or impersonation.*
*Electronic "tagging" or vandalizing systems, newsgroups, files, mail, etc. (consider the attack of alt.tasteless on rec.pets.cats)*

*However, most "Computer Crimes" are simply ordinary crimes that have used a computer. Ordinary laws already cover much of it.*

4b Do you have any examples of such?

*Yes*

5 Do you have any further comments that you wish to make?

## 13, male, 25 yrs exp, Unix, no.

2d Do you feel that such activities fulfil a positive purpose?

*Generally no, but sometimes yes. The exceptions are those wherea cracker, having cracked the security of a supposedly secure system proceeds to inform the managers of that system and assists in correcting the weakness he or she exposed.*

3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)

*patience, curiosity, and, as the sophistication of system security measures increases, a knowledge of combinatorics, information theory, and cryptography. Most crackers today either concentrate on systems with fairly trivial security measures, or they take advantage of the work of others who have the above skills. Research skills, the ability to find relevant previous work and take advantage of it, are important!*

3b What would you say their main motives are?

*Some crackers are in it for thrills. Others are malicious and intent on vandalism. Others are driven by curiosity or by the rewards of meeting a technical challenge.*

3c What percentage of crackers are male?

*I have no idea, probably most, I'd guess 90 percent.*

3d Do you feel that their activities are beneficial or harmful to society?

*Most are harmful, but see my answer to 2d where I suggest a way for a cracker to be beneficial.*

3e Why?

*When a cracker deliberately vandalizes a system, or accidentally damages the system, as in the well known case of Morris's Internet worm, there is direct harm. If a cracker breaks in and then merely looks around, there may be no harm done, but how is the cracker to know or assure that no harm is done? Commands that do nothing on some systems may do quite different things on other apparently similar systems! But, see my answer to 2d for a description of an ethical and beneficial way for a cracker to act.*

4a What activities would you class as Computer Crimes?

*Breaking into a system and then entering that system to execute any command other than logout – this should be viewed as legally equivalent to picking a lock and then entering the previously locked room.*

*Deliberate damage to data stored on a computer, or deliberate disruption of computer service – this should be viewed as legally equivalent to damaging the contents of someone's file cabinet or cutting off someone's electrical service – it's an act of vandalism, plain and simple.*

*Accidental damage to data or to a computer service. This should be legally treated in the same way you'd treat someone who accidentally damages conventional property. They should pay for the damage, but they aren't generally liable for criminal charges unless they, for example, picked your door lock and*

*then carelessly blundered around your house. The criminal charge is breaking and entering, in that case, not blundering about.*

*Theft of data. If someone copies files from your computer system, they should be liable in the same way that someone is liable who enters your office, removes a file from your file cabinet, and takes a photocopy. This liability is complex – they may be liable for breaking and entering, either at the lock in your office door or at the lock on your file cabinet, and then they may be liable for copyright infringement, unless the file they copied was in the public domain. This gets into intellectual property law, not related to cracking! I feel that there ought to be criminal penalties for making copies of material that was not intended to be published (personal papers as well as files on a computer).*

*Breach of privacy in electronic communication. Someone who reads your E-mail without a legitimate reason ought to be tossed into the same class as someone who listens in on your phone conversation or reads your postal mail. In all these cases, there are legitimate reasons for the invasion of privacy. Postal clerks, telephone system maintenance personell, and system operators must all occasionally do so in order to run their communications systems. Others, be they snoopy neighbors or crooks, should be stiffly punished.*

4b Do you have any examples of such?

*See above!*

5 Do you have any further comments that you wish to make?

*I made many above!*

15, Female, 22 yrs exp, Unix, no.

3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)

*Knowledge of the operating system, a creative mind in terms of finding loopholes in the software, or the ability to guess someone's password.*

3b What would you say their main motives are?

*It's a challenge. Some crackers really want to get hired by the people running the system and just want to get the system manager's attention. Other motives are wanting access to something on the system.*

3c What percentage of crackers are male?

*I'd guess 95%.*

3d Do you feel that their activities are beneficial or harmful to society?

*Believe it or not, I think most of their activities are beneficial.*

3e Why?

*Although there are a few honest-to-God malicious crackers, most of them are either just trying to see if they can break system security or just want to harmlessly access something. At worst they alert sysadmins to security holes and often make it obvious as to how to plug these holes.*

4a What activities would you class as Computer Crimes?

*Stealing information from someone's account, breaking into someone's account with malicious intent, breaking system codes and reading protected files, tampering with someone's files.*

4b Do you have any examples of such?

*When I was a sysadmin, someone abused security privileges to read my e-mail file which was protected so only I could read it.*

*Another such example would be the time someone broke into a bunch of accounts at Berkeley and deleted people's files.*

5 Do you have any further comments that you wish to make?

*I think we need to go back to hiring more people who break into computer systems. Computers are more complex than they used to be, and anyone who can break today's security systems is much sharper than someone who could break in ten or twenty years ago.*

16, Male, 20 yrs exp, Unix, No.

3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)

*A good puzzle-solving ability.*

3b What would you say their main motives are?

*Formerly, the challenge of a good puzzle. Currently, I think there are economic motives that are beginning to appear.*

3c What percentage of crackers are male?

*95%*

3d Do you feel that their activities are beneficial or harmful to society?

*Somewhere between neutral to harmful.*

3e Why?

*They cause us to erect barriers where formerly they were unnecessary.*

4a What activities would you class as Computer Crimes?

*Stealing people's money (or other things of value) by means of access to a computer.*

4b Do you have any examples of such?

*credit card fraud*
*industrial espionage*

17, Male, 20 yrs exp, Unix, yes, ?, yes&no, yes.

3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)

*curiosity, intelligence, an eye for details and quirks*

3b What would you say their main motives are?

*curiosity, challenge, learning*

3c What percentage of crackers are male?

*No idea. A large majority.*

3d Do you feel that their activities are beneficial or harmful to society?

*(They are both.)*

3e Why?

*Good security and authentication, in most environments, are beneficial. It is a bad thing that a great many programs and programmers rely on security-through-obscurity or are careless about security; the threat of crackers helps keep this from being even more prevalent. It is a bad thing that organizations often ignore security until they are bit, and that crackers sometimes damage systems and data. Good security design, however, can lead to both networks that are relatively open and relatively secure.*

4a What activities would you class as Computer Crimes?

*Theft of services or material goods; destruction of files & information.*
*Using information gained for profit at others' expense.*

4b Do you have any examples of such?

5 Do you have any further comments that you wish to make?

*Asking for 1 & 0 instead of yes/no is silly.*

*The nature of hacking/cracking has changed tremendously over the last twenty years, and networking has made an enormous difference in its nature as well.*

*Question 2a is poor. I have hacked on both machines that I did have authorised access to, and on machines that I did not.*

*As I point out in response to question 3d, I don't think the question is an either-or question. Like many issues, good/bad is a subjective call and there are clearly elements of both.*

18, Male, 14 yrs exp, Unix, No.

3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deterintruders)

*Problem solving skills, paranoia.*

3b What would you say their main motives are?

*Fun.*

3c What percentage of crackers are male?

*90*

3d Do you feel that their activities are beneficial or harmful to society?

*Harmful*

3e Why?

*Their activities often cannot be distinguished from attempts at more serious computer crime, so administrators must assume the worst when dealing with them. This takes time away from more important work.*

4a What activities would you class as Computer Crimes?

*Modifying important computer data. Preventing legitimate users from using systems.*

4b Do you have any examples of such?

*Diverting funds in bank computers. Modifying patient records in hospital computers. Breaking into a computer and running programs that slow it down, so that regular users don't get the performance they should. Breaking into and crashing a computer.*

## 19, male, 45 yrs exp, Unix, ?.

*Why should I do something so unintuitive? Can't your analysis program understand YES or NO or MAYBE or UPYOURNOSE ?*

1a How long have you been using computers?

*Far longer than you have been alive. Remember the IBM CPC? (Card-Programmed Calculator (vintage 1949))? I thought not. You wrote loops by duplicating that part of the card deck.*

1b What major operating system, such as UNIX, would you say you are most experienced with?

*You would never have heard of most of them. I use MS-DOS on my PC, running under an overlay I wrote called PCnix, which makes it look enough like Unix so I don't get brain damage moving between them.*

1c Are you male or female?

*Yes.*

2a Have you ever hacked into a computer system on which you do not have authorised access? Your answers will be treated in strictest confidence!

*Why should I trust you to keep a confidence? I've never heard of you. Are you an AI program at the NSA?*

3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)

*My main purpose in life is to enter systems I am not authorized to access, and, once in, to DO GOOD. This confuses everyone connected with Security. I empty the /dev/null bitbucket to avoid overflow, I kill processes that have slept for over 3 days, tying up authorized access lines, and I debug programs for novice programmers so they do the Right Thing, always. I do not seek thanks; knowing I have DONE GOOD is all the reward I seek.*

3b What would you say their main motives are?

*Sheer animosity.*

3c What percentage of crackers are male?

*You want I should go out and take a survey? I thought that was what you were doing. Most computer users are male. Go figure.*

3d Do you feel that their activities are beneficial or harmful to society?

*I think society is totally indifferent to their behaviour. Even if you explained it carefully, to Society, she would answer "...huh?"*

3e Why?

*Because computer users have a seriously overblown sense of their own importance.*

4a What activities would you class as Computer Crimes?

*There are no Computer Crimes, only criminal computers. And they're getting faster all the time. One day they will just unplug us all.*

4b Do you have any examples of such?

*See, you anticipated the answer to question 4a, and you missed. Very bad form for a survey. If you know the answer already, why ask it?*

5 Do you have any further comments that you wish to make?

*No. I've helped enough so you can now get your PhD with no further effort.*

Thank you again for your time.

*It took no time at all. This is a recording.*

20, male, 25 yrs exp, Unix, no.

3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)

*Persistence. Deviousness.*

3b What would you say their main motives are?

*Depends. In some cases, curiosity. In some, desire to get something for nothing. In others, maliciousness.*

3c What percentage of crackers are male?

*Almost all, I would_guess_.*

3d Do you feel that their activities are beneficial or harmful to society?

*Harmful, some more, some less.*

3e Why?

*Moral erosion. Same reason that walking into a house uninvited is not good.*

4a What activities would you class as Computer Crimes?

*Well, there's a large range, isn't there? Everything from illegitimate personal enrichment (embezzlement etc.) and malicious destruction and theft of secrets to simple unauthorized use.*

21, male, 15 yrs exp, Mac OS, no.

3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)

*intuition, mathematics, comm. systems familiarity, OS familiarity*

3b What would you say their main motives are?

*sport. trying to prove it can be done. very rarely, revenge for ex-school, ex-employer, etc.*

3c What percentage of crackers are male?

*no concrete data, but I would assume all are male.*

3d Do you feel that their activities are beneficial or harmful to society?

*harmful.*

3e Why?

*They (1) invade privacy (2) [potentially] disrupt systems, corrupt data (3) cause society to built systems with ever-increasing, user-unfriendly security measures.*

4a What activities would you class as Computer Crimes?

*forgery of data, destruction of data, virus writing, intellectual-property theft, should be felony-class crimes. Lesser violations, such as unauthorized access, should be misdemanors.*

4b Do you have any examples of such?

*the Macintosh NVIR was very disruptive about five years ago.*

5 Do you have any further comments that you wish to make?

*The worst disruption caused by hackers will be the eventual (mis)-regulation of the industry by government, in an attempt to stop hacking. Such measures seem inevitable, but are rarely effective in view of their intent. People who compute for a living, or for enjoyment pay the price of such legislation in increased costs, dimished empowerment, and complex regulations.*

23, Male, 25 yrs exp, Unix, no.

3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)

*Probably the same skills as any good programmer – curiosity, alertness, analytical skills, determination.*

3b What would you say their main motives are?

*To feel powerful, to think themselves above the law, to hurt others.*

3c What percentage of crackers are male?

*Don't know, but I've never met nor heard of a female one.*

3d Do you feel that their activities are beneficial or harmful to society?

*Harmful*

3e Why?

*Not only do they cause direct damage to others, but they also require others to spend time making their systems secure.*

4a What activities would you class as Computer Crimes?

*Obtaining unauthorized access; damaging files; creating and disseminating viruses; etc.*

4b Do you have any examples of such?

*I'm not sure what you're asking. One reads of such activities all the time.*

24, ?, 15 yrs exp, SunOS, yes.

2a Have you ever hacked into a computer system on which you do not have authorised access?

*Define "hacked into". I also assume you mean "...you _did_ not...", since the rest of the question is in the past tense.*

*I once performed actions that the owner(s) of the system in question treated as a (mild) intrusion. None of the people involved caught any heat for it as far as I know, probably because the owner(s) knew me personally and believed (correctly) I did what I did without malicious intent.*

2b If YES, do you feel that your activities were ever illegal?

*(I assume you refer strictly to the activities that provoked the yes answer. I have performed many definitely illegal acts; most recently, I suspect, crossing against a red light.) I have no idea; I am not a lawyer, and neither know nor knew enough about the applicable laws, if any, to say.*

2c Immoral?

*Yes, in that I should not have presumed their acceptance of what I did; I should have checked beforehand. No, in that what I actually did was not anything I consider immoral per se. (That is, it's not the activities, but the lack of explicit permission for performing them, that I feel was wrong.)*

2d Do you feel that such activities fulfil a positive purpose?

*I did at the time, or I wouldn't've done it. I don't recall precisely why I wanted access to the system in question, though. (The access was gained through a complete no-brainer, and did not, per se, hold any interest; I could have done it any time in the preceding several weeks.)*

3a What skills do you feel a good cracker needs?

*Define "good" here. Does it mean simply "successful"? Does it mean "experienced"? Does it mean "able to avoid getting caught"? Does it mean "able to crack tough systems"? Does it mean "ethical"?*

*In any case, I don't know. The major requirement for the "cracker" epithet, in my opinion and use of the word, is something I can't characterize well, but could perhaps call a lack of respect for others.*

3b What would you say their main motives are?

*Crackers, I assume you mean. I don't know. _The Hacker Crackdown_ gives me the impression their main motives are egoboo and, for the more technically skilled and innovative ones, the power-trip that comes from overcoming any difficult obstacle.*

3c What percentage of crackers are male?

*I don't know, and I don't believe anyone else does either. I feel fairly confident it's over 80%, though.*

3d Do you feel that their activities are beneficial or harmful to society?

*Hard to say. Probably harmful, on the whole.*

3e Why?

*Because they erode the `tendency to trust' that currently still pervades the electronic community (at least as I see it).*

4a What activities would you class as Computer Crimes?

*I don't know. A crime is something in violation of some law, and as I mentioned before, I'm not a lawyer and don't know enough about the applicable laws, if any, to say.*

4b Do you have any examples of such?

*No.*

5 Do you have any further comments that you wish to make?

*I find myself very puzzled as to what you're trying to find out via this survey - what the motivation is behind your choice of questions. If you wouldn't mind, I'd be interested to hear.*

## 25, Male, 18 yrs exp, Genera, no.

3a What skills do you feel a good cracker needs?

*Ethics.*

3b What would you say their main motives are?

*Curiousity, or possibly revenge (not specific revenge; rather, an expression of frustration/power over something else in the environment)*

3c What percentage of crackers are male?

*No idea. I'd imagine 90-95%*

3d Do you feel that their activities are beneficial or harmful to society?

*Harmful*

3e Why?

*Lots of wasted effort goes into stopping and circumventing them. Time and resources are taken up with articles, books, and surveys about them. This very survey is making me less productive, and taking you away from some activity which could be directly enhancing society, rather than just dealing with and examining a rather annoying aspect of socity.*

4a What activities would you class as Computer Crimes?

*Too broad a question.*

4b Do you have any examples of such?

*Sure. "Cracking." Stealing data. Copying commercial computer programs without paying for them.*

26, male, 22 yrs exp, Unix, yes, no, no, yes.

3a What skills do you feel a good cracker needs? (Please assume that by CRACKERthat I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)

*Curiosity.*

3b What would you say their main motives are?

*Curiosity.*

3c What percentage of crackers are male?

*90+%*

3d Do you feel that their activities are beneficial or harmful to society?

*Different world than when I did it.*

3e Why?

4a What activities would you class as Computer Crimes?

*The usual: theft, espionage.*

27, male, 17 yrs exp, unix, yes, yes, no yes

3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)

*patience*
*good telephone manners*
*ability to use reference material*

3b What would you say their main motives are?

*bordom*
*search for prestige*
*search for challenge*

3c What percentage of crackers are male?

*95*

3d Do you feel that their activities are beneficial or harmful to society?

*harmful*

3e Why?

*accidently damage*
*incremental cost of protection*
*increase in fear*

4a What activities would you class as Computer Crimes?

*theft of propriartary data*
*damage of damage*
*harrasment*
*use of computers to steal physical property*

28, male, 30 yrs old, unix, no.

(Please answer YES/NO questions with 1 (YES) or 0 (NO))

*[Presumably this is to indicate that one has experience with ancient computer systems that cannot handle data that isn't numerical.]*

3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)

*Desire; otherwise untapped hunting skills; memory & imagination for patterns.*

3b What would you say their main motives are?

*Mountaineering.*

3c What percentage of crackers are male?

*About 130% or more. Never heard of any women.*

3d Do you feel that their activities are beneficial or harmful to society?

*No.*

3e Why?

*The question is too simplistic.*

4a What activities would you class as Computer Crimes?

*Theft of proprietary data, violation of copyright.*

4b Do you have any examples of such?

*0 (no)*

5 Do you have any further comments that you wish to make?

*This whole computer security thing results from people having naive beliefs about computers. If you want a secure system, don't put it on a phone line, and don't trade disks with other people. "I left my front door open, with a sign saying, FREE LUNCH, and everyone came in and drank all my beer, and peed in my ashtrays. Have they no respect for private property? They have no right to mess up my place, and I was planning to give up smoking anyway! Next time I'll have a Norwegian parrot to watch the door."*

29, male, 18 yrs exp, unix, yes, yes, depends, depends.

2c Immoral?

*This is tougher. Cracking a system and deleting files is immoral. Same as breaking into a building and vandalizing it. Hacking a system for fun and knoweledge is more like riding a bike through someone's property and I don't consider it morally the same.*

2d Do you feel that such activities fulfil a positive purpose?

*People hack for many reasons and sometimes these are good reasons for positive purposes. Learning about computers is good and challenging computer security is good because it can help keep out those with evil intent.*

3a What skills do you feel a good cracker needs? (Please assume that by CRACKER that I mean an individual who meddles in systems where he or she does not have authorised access and where the system manager makes attempts to deter intruders)

*Patience, computer knoweledge, willingness to try new things.*

3b What would you say their main motives are?

*It used to be almost exculsively for the persuit of knoweldge. Maybe as a stepping stone to other things back when computers were very expensive. Now it seems to be mostly glory seekers like the kind of people who spray-paint grafiti.*

3c What percentage of crackers are male?

*I would guess almost exclusively male. Although I was the "victim" of an exception once. I have a PC running internet protocols over amateur radio at home. There is an anonymous login with access to some public files and some private logins with more access. I discovered a woman who had cracked a password (it was almost trivial) and was poking around. I handled it by creating a user account with her name and full system access and warning her to please not copy any of my commercial software or gif files as these would break FCC Amateur Radio rules.*

3d Do you feel that their activities are beneficial or harmful to society?

*Yes.*

3e Why?

*The challenge to find out about systems can drive people to learn a great deal. But the destructive nature of some makes a bad image for all hackers and is further exploited by the "Computer Security" business.*

4a What activities would you class as Computer Crimes?

*Pretty much the way the law in the US is now. Wilfully breaking and entering systems and destroying data. But the general public needs to understand the significance of computer crime compared to "real" crime. The witch-hunt persecution of hackers in this country for relatively minor offenses is absurd in comparison to the light treatment violent criminals often get.*

4b Do you have any examples of such?

*Most of the examples I am familiar with of the the type I described above. Like Phiber Optik, the Steve Jackson and LOD cases. The theft of a minor 911 document that was shown in court to be almost worthless was blown into a full conspiracy involving people far beyond any crime as if it was the World Trade bombing.*

5 Do you have any further comments that you wish to make?

*Safety through knowledge not persecution.*

31, male, 11 yrs exp, unix, no.

2a Have you ever hacked into a computer system on which you do not have authorised access? Your answers will be treated in strictest confidence!

*NO/YES, I was once member of a Tiger team in a University. We used very simple tricks to discover passwords or to access files and reported them to the management.*

3a What skills do you feel a good cracker needs?

*Patience, since most brute force attacks will work*

3b What would you say their main motives are?

*The challenge, the appeal of doing something clearly illegal, but that can be harmless, and destructive instincts.*

3c What percentage of crackers are male?

*I would say a great percentage (80%), since I believe women have a better social behavior.*

3d Do you feel that their activities are beneficial or harmful to society?

*Clearly harmful, since this activities influence the number of restrictions the society have to live with.*

3e Why?

*Ooops, see above.*

4a What activities would you class as Computer Crimes?

*breaking into a computer*
*distributing virus*
*destroying other's people data*

4b Do you have any examples of such?

*I am usually updated on the bigger cases, like the Morris Worm, and with virus.*

5 Do you have any further comments that you wish to make?

*I believe cracking is like writing in walls (grafitti?) and destroying other person property. Because of cracking, we have to live with passwords, encryption, etc...*

*I do also believe that bad behavior is inerent to human behavior, so there will always be crackers.*

*3rd: Crackers make costs bigger!*

32, male, 22 yrs exp, unix, no.

3a What skills do you feel a good cracker needs?

*What do you mean by "good"? Just kidding, I know what you mean. Mostly they need lots of patience; I think very few cases involve special expertise. There are so many unlocked doors lying around that safecrackers are not necessary.*

3b What would you say their main motives are?

*Mostly the thrill of the challenge.*

3c What percentage of crackers are male?

*99%.*

3d Do you feel that their activities are beneficial or harmful to society?

*Most are neutral to society since they don't really cause much harm. Of course, a few have more malicious motives and cause trouble, and those are surely harmful. I don't see much benefit to society; certainly some honest people acquire some skill and knowledge that might be useful when they try to do cracking, but they could get that any number of other ways.*

3e Why?

*See above.*

4a What activities would you class as Computer Crimes?

*Crashing someone's computer, destroying someone's data, denying someone access to their computer resources (e.g. the famous Morris Worm), stealing intellecutal property (including industrial espionage), even harassment. The fact that the cracker is a kid and the crackee is "the establishment" does not, in and of itself, justify the activity.*

4b Do you have any examples of such?

*Oh, the papers are full of them.*

5 Do you have any further comments that you wish to make?

*I'm not happy about the overreaction of law enforcement people in the USA who don't understand what's going on, and make trouble for people who are NOT crackers. See Bruce Sterling's "The Great Hacker Crackdown"*

34, male, 30 yrs exp, unix, yes, yes, yes, yes.

3a What skills do you feel a good cracker needs?

*Lots of knowledge of the system.*

3b What would you say their main motives are?

*Fun.*

3c What percentage of crackers are male?

*This is a stupid question to ask in a delphi study – it does not matter what anyone thinks the percentage is, it has an objective answer.*

3d Do you feel that their activities are beneficial or harmful to society?

*beneficial.*

3e Why?

*encourage security, encourage expansion as knowledge.*

4a What activities would you class as Computer Crimes?

*hacking/cracking.*

## 36, male, 25 yrs exp, unix, no.

2a Have you ever hacked into a computer system on which you do not have authorised access? Your answers will be treated in strictest confidence!

*No.*

*(This is a silly question, isn't it? Why should I trust a "strict assurance" from someone I know nothing about? And why should you trust a reply — negative OR affirmative — from someone you know nothing about? I was seriously tempted to answer "Yes, thousands of times...", just for the fun of it...)*

3a What skills do you feel a good cracker needs?

*Motivation, quick learning, quick thinking, good memory. Helpful but not necessary: programming skills and knowledge of basic software (OS, shells, mail, etc.) and hardware (computers, disk drives, networks, modems).*

3b What would you say their main motives are?

*My guess is mostly ego gratification; rarely personal gain.*

*However, I guess that ego-boosters may seek some personal gain as "trophy" — a tangible proof of their superiority. Sort of like the stuffed heads that hunters hang one the wall.*

3c What percentage of crackers are male?

*I would guess close to 100%.*

3d Do you feel that their activities are beneficial or harmful to society?

*Harmful.*

3e Why?

*It is like someone entering your house univited. Even if he means no harm, he will scare you, disturb your peace of mind, disrupt your work, and waste your time — if nothing else, by forcing you to check whether any harm has been done.*

*Besides, he will quite often *do* unintentional damage, sometimes very serious. Last year, for example, a Rio research lab suffered a "benign" cracker attack by two of our students, which resulted in the loss of their entire network file system. (They weren't doing backups, of course...)*

*As a matter of fact, I cannot think of any beneficial aspect of computer cracking.*

4a What activities would you class as Computer Crimes?

*You mean, as distinguished from "misdemeanors", "violations", "improprieties", "reprehensible behavior", or whatever? I am not enough of a lawyer to know (or care) about such distinctions.*

4b Do you have any examples of such?

*See above.*

5 Do you have any further comments that you wish to make?

*I generally wish that people who do Bad Things get punished: severely enough to save most people from temptation, but not so severely as to turn a bright irresponsible prankster into a bright embittered criminal.*

*Similarly, I wish that systems be made secure: enough so to prevent random high-schoolers from deleting my files, but not to the point that the security devices themselves start interefering with my work. (Besides, cracker motivations are such that ostensive security measures may actually increase the probability of a successful attack.*

*)*

37, male, VMS, 25 yrs exp, no.

3a What skills do you feel a good cracker needs?

*Ability to psychologically maipulate users and administrators of the target system*

3b What would you say their main motives are?

*curiosity, bravado*

3c What percentage of crackers are male?

*97%*

3d Do you feel that their activities are beneficial or harmful to society?

*harmful in a few cases, generally neither beneficial nor harmful*

3e Why?

*damage done in the few cases, otherwise no damage done*

4a What activities would you class as Computer Crimes?

*all criminal acts involving computers or computer personell in their computer-connected roles*

4b Do you have any examples of such?

*In 1987 we (at my previous job) had a break-in via the Internet into our VAX. The break-in came via a user ID and password stored in an accessible file on a machine in Oslo. That machine in turn had been hacked from elsewhere, some speculated members of the Computer Chaos Club in Hamburg. The machine contained no confidential information, but the intruders left several back doors for a subsequent return.*

*DEC was greatly perturbed, and we used 4 weeks to clean up the machine, 4 weeks without the single central computer for 30 employees.*

38, male, 15 yrs exp, Unix, no.

3a What skills do you feel a good cracker needs?

*Patience. Good software.*

3b What would you say their main motives are?

*I wouldn't like to speculate.*

3c What percentage of crackers are male?

*Almost all, if not all.*

3d Do you feel that their activities are beneficial or harmful to society?

*Don't know.*

4a What activities would you class as Computer Crimes?

*I think that's a spurious subdivision. Crimes are crimes. You don't have special law for "Tuesday crimes".*

## 39, male, 16 yrs exp, MacOS, no.

3a What skills do you feel a good cracker needs?

*Very little. Being able to write a simple program that tried lots of different passwords and send that to a login prompt.*

3b What would you say their main motives are?

*Being unable to do anything serious with computers, they want to feel powerful in another way. One way is cracking, breaking the security systems, thereby feeling powerful.*

3c What percentage of crackers are male?

*No idea, but I'd guess it's a clear majority.*

3d Do you feel that their activities are beneficial or harmful to society?

*Mostly harmful.*

3e Why?

*Just breaking in will cause the system admin to trash all passwords, making the system unavailable for days. Breaking in and trashing/changing files is obviously harmful.*

*The only good thing is that the crackers stress the security levels, forcing better security levels, which is somewhat positive, raising the bid for REAL spies.*

4a What activities would you class as Computer Crimes?

*Writing computer virii: Serious crime (at least if it leaks out).*

*Cracking into a system: Criminal, but not quite as bad as a virus.*

*Cracking and doing anything more, like reading secret documents or editing them: Serious crime.*

4b Do you have any examples of such?

*Yes. On virii (which might not be of interest, but still) I know a convicted virus author (who is now actively working against virii). On cracking, our system was once shut down for a week due to a cracker, who had broken in and installed some password tapping program. I don't know any cracker personally.*

5 Do you have any further comments that you wish to make?

*One question that could be interesting: Is cracking something you do just by yourself, or is it a social activity?*

40, male, 20 yrs exp, Ultrix/OSF/1, no.

a What skills do you feel a good cracker needs?

*patience, luck and a bad system adminstrator.*

3b What would you say their main motives are?

*cheap thrills.*

3c What percentage of crackers are male?

*beats me. probably 90+*

3d Do you feel that their activities are beneficial or harmful to society?

*50/50*

3e Why?

*beneficial because they point out flaws in our systems, harmful because of all the extra work they cause*

4a What activities would you class as Computer Crimes?

**Any* use of *any* computer for which one does not have an explicit authorization.*

4b Do you have any examples of such?

*They are obvious. telnetting to random hosts on the Internet and trying random accounts and passwords springs immediately to mind.*

*You're welcome. I'd like to see a copy of your paper when it's published.*

## 43, male, 20 yrs exp, unix, no.

3a What skills do you feel a good cracker needs?

*'Good cracker' is an oxymoron.*

3b What would you say their main motives are?

*Improve their self-esteem. To prove their value and importance to themselves and their friends who are impressed by these actions. They feel it is safe to perform these actions because nobody is harmed, or atleast nobody they care about like 'the big faceless corporation' or 'the oppressive goverment'.*

*Some people hack computers to gain some advantage at work over their boss of co-workers.*

*Finally, some people simply do it for purposes of gaining more money. They may do this by embezzlement or espionage.*

3c What percentage of crackers are male?

*Probably a majority are male if you look strictly at the combined population of people who use computers.*

*But a much more interesting analysis would be to find out what percentage of women hack computers and for what purposes. Then compare to the same stats for men.*

3d Do you feel that their activities are beneficial or harmful to society?

*Harmful*

3e Why?

*Most people would not want others breaking into the bank account or wire tapping their phone service. Why should I approve of people doing basically the same thing with computers? One of the reasons why the Internet has been so successful is because of it's openness. Hackers causes companies on the Internet to stop sharing data. This is not a good step for the computer industry.*

4a What activities would you class as Computer Crimes?

*I can think of a million potential actions which could be classified as computer related crimes. Generally anything which effects someones ability to do legitimate business or conduct private affairs using computers and digital communications can be classified as a crime.*

45, male, 20 yrs exp, yes, no, yes, depends.

*Ah, ok. I like to be helpful, but realize you sometimes you have to give a little information if you want total strangers to give you information. Information is like money, you know. Also, since I have no assurances of what you will do with my information, I can't be entirely free with it.*

*I am a bit astonished you prefer 1/0 to yes/no. Maybe you've been spending a little too much time with computers, and should hang out with people a bit more??*

2b If YES, do you feel that your activities were ever illegal?

*At the time they were not. They would be if done today.*

2c Immoral?

*yes, I would not repeat these knowing now what I know*

2d Do you feel that such activities fulfil a positive purpose?

*sometimes yes, sometimes no*

3a What skills do you feel a good cracker needs?

*perseverance, curiosity, technical skill, and a weakened sense of ethics*

3b What would you say their main motives are?

*Different people have different motives. I'd say largely thrill-seeking, but some people now do it for profit or pure spite. These ratios are changing rapidly.*

3c What percentage of crackers are male?

*I'd guess around 95%. But don't confuse conjecture with facts; a survey question like this is meaningless.*

3d Do you feel that their activities are beneficial or harmful to society?

*In the long run, clearly harmful.*

3e Why?

*Aside from any actual damage caused, the erosion of trust and increased cynicism makes society more sour than it should be.*

*The actual damage caused in most cases today is zero, but history clearly shows that sooner or later, truly malicious people will exploit the skills and the tools created by today's naive crackers who think they're not doing any harm.*

4a What activities would you class as Computer Crimes?

*Use of a computer to deprive another person of property, privacy, or to cause injury or other harm, either directly or indirectly.*

4b Do you have any examples of such?

*Go read the RISKS digest, each week brings you some new ones.*

5 Do you have any further comments that you wish to make?

*I'm a big fan of lock-picking or cracking in its purest form, as a recreational sport. Like shooting a gun, it can be loads of fun, as long as you don't hurt anyone. I draw the line simply at where people get hurt, but I have a more expansive definition of 'hurt', which includes violation of privacy.*

*Perhaps what's needed is a sporting event, where people build and attempt to break into isolated systems, to earn fame and prizes, without ever having to tread on someone else's private property. Don't shoot my farm animals, go have yourself a weapons range and shoot bloody bazookas for all I care. Wouldn't that be nice?*

*There was a time when only kings and nobility had weapons, and there was a certain chivalry and responsibility of honor that went with such ownership. As weaponry (and computer skills) become more widespread, you cannot help but see more people use them unscrupulously. Cracking in the 90's is much different from the 70's, and is increasingly more common (in both senses of the word).*

*Good luck in your endeavor, it's a worthy area to study. I'd be interested in seeing a copy of your study when it's completed, if you don't mind. thanks.*

55, male, 29 yrs exp, Unix, no.

2a Have you ever hacked into a computer system on which you do not have authorised access? Your answers will be treated in strictest confidence!

*Only to deal with emergencies of some kind.*

*By the way, if I had anything juicy to reveal, the assurance of strict confidence from a stranger out in net-land would not carry a whole lot of weight.*

3a What skills do you feel a good cracker needs?

*Excellent knowledge of the systems being cracked, plus some cleverness and a good mind for details.*

3b What would you say their main motives are?

*Curiosity. Desire for power or status among peers.*

3c What percentage of crackers are male?

*I've never heard of a female one, excpet as a junior member of a team.*

3d Do you feel that their activities are beneficial or harmful to society?

*Mostly harmful.*

3e Why?

*A few do malicious damage. More do accidental damage. Most invade someone's privacy. The fact that these people are around at all means that more effort must go into security.*

4a What activities would you class as Computer Crimes?

*Are you asking what activities should be classed as crimes, or what currently are? Any deliberate unauthorized use of someone else's computing resources is a theft of services, but some law enforcement agencies act like it's blowing up the World Trade Center.*

56, male, 12 yrs, MacOS, yes, no, no, yes.

2d Do you feel that such activities fulfil a positive purpose?

*Yes, it taught me a lot and helped inprove security*

3a What skills do you feel a good cracker needs?

*Menal aptitude for logic/design, knowledge of computers, social skills specially charistma*

3b What would you say their main motives are?

*Self fullfilment, achieving a hard to reach goal. Cracking is a great learning oportunity.*

3c What percentage of crackers are male?

*85% +*

3d Do you feel that their activities are beneficial or harmful to society?

*Most are harmfull*

3e Why?

*Most follow no social or moral code when Cracking and end up hurting others, or at least causing financial troubles to victims.*

4a What activities would you class as Computer Crimes?

*Obtaining/spreading private information. Using cycles without concent. Interfering with private comunicaes. Defeating copy protection schemes.*

4b Do you have any examples of such?

*Too many to list*

5 Do you have any further comments that you wish to make?

*There is a diference between cracking with a concience, amd malignent mischeif, the media feeds on the later, many use the first.*

57, male, 15 yrs exp, unix, no,

3a What skills do you feel a good cracker needs?

*PATIENT, HIGH TOLERANCE FOR BOREDOM*

3b What would you say their main motives are?

*EGO-BOOST THROUGH KUDOS*
*NOTORITY/ATTENTION GAINING*
*MYSTICISM*

3c What percentage of crackers are male?

*HOW CAN I ANSWER THIS WITHOUT CONDUCTING A SURVEY ? IF YOU MEAN 'What percentage of crackers do you think are male?' THEN MY ANSWER IS 99%*

3d Do you feel that their activities are beneficial or harmful to society?

*BENEFICIAL*

3e Why?

*1. THEIR ACTIONS WILL HELP TO EXPOSE SYSTEMS THAT OUGHT TO BE SECURE BUT WHICH ARE NOT.*
*2. BY POSING A THREAT TO COMPUTER SOCIETY THEY ENSURE THAT THE PROBLEMS OF SECURITY WILL BE RESEARCHED/DISCUSSED. THIS OUGHT TO HELP THE SPREAD OF INFORMATION. SOMETHING I BELIVE TO BE VITAL.*

4a What activities would you class as Computer Crimes?

*WILFUL DESTRUCTION OF DATA.*
*WILFUL CORRUPTION OF DATA.*
*WILFUL PERVERTION OF ANOTHER'S PROGRAMS*

>4b Do you have any examples of such?

*0*
*("rm -fr *.*" :-)*

>5 Do you have any further comments that you wish to make?

*1. I assume you know of this distinction between CRACKER and HACKER.*
*2. "Security through Obscurity' seems to be a common feature of many Operating Systems/installations. I believe this is to be a flawed method, and I would much rather see an open discussion of how systems were cracked and to stop it happening in the future. In particular I suspect that a lot of commercial installations, if they were cracked, would attempt to cover up the break-in and pretend that it had never happened, rather than seek help from the rest of the community to prevent it happening again.*

61, male, 12 yrs exp, unix, yes, no, no, yes.

2a Have you ever hacked into a computer system on which you do not have authorised access? Your answers will be treated in strictest confidence!

*Yes - but this is a very broad question; "authorised" is a very broad term. Have you ever had to break into someone's desk to retrieve a vital document they accidentally left there before going on vacation? I have, but I don't consider that act "illegal", "immoral" or "bad" - it was necessary, and, pragmatically, was the right thing to do.*

3a What skills do you feel a good cracker needs?

*Patience*
*Knowledge of back-door/undocumented features in/routes into an OS*
*If mounting a brute-force attack, the ability to write a good password cracker!*
*Awareness of how their activities may be monitored/logged/traced*

3b What would you say their main motives are?

*You want me to second-guess other people? Hmm. Thrill of the chase or the delight of solving a good puzzle. I think outright vandalism is rare.*

3c What percentage of crackers are male?

*Probably even more skewed towards males than the demographics of most computer users, who are already mostly male; maybe 90%.*

3d Do you feel that their activities are beneficial or harmful to society?

*I'm sure some have been, and some have not. Generally, cracking activity is probably harmful to society for the same reasons as most petty crime; in some cases, cracking or attempted cracking will prompt an SA to beef up system security, in which case one can argue their is a net benefit to society, but one can also argue that such measures should not be necessary. True, and neither should cars or houses need locks, in an ideal world.*

*The question is too broad.*

3e Why?

*See above*

4a What activities would you class as Computer Crimes?

*Not substantially different to non-copmputer crimes, eg, breaking and entering, petty theft, wanton & wilful destruction of property etc all have their analogues in the computer world.*

64, male, 29 yrs exp, unix, no.

3a What skills do you feel a good cracker needs?

*an underdeveloped conscience*

3b What would you say their main motives are?

*self-gratification*

3c What percentage of crackers are male?

*probably high 90's*

3d Do you feel that their activities are beneficial or harmful to society?

*harmful*

3e Why?

*It makes members of the society spend too much time building locks for doors rather than building windows to see through.*

4a What activities would you class as Computer Crimes?

*illegal entry, destruction or unauthorized examination of data, unauthorized copying of data. This is the hard-nosed classification. However, if a file has read permission to non-users, then that is, by definition, authorization for examination.*

66, male, 14 yrs exp, unix, no.

3a What skills do you feel a good cracker needs?

*persistence/patience, good memory, moderate intelligence*

3b What would you say their main motives are?

*fun, thrill, boredom*

3c What percentage of crackers are male?

*99+*

3d Do you feel that their activities are beneficial or harmful to society?

*more harmful*

3e Why?

*less trust, higher costs, wasted resources*

4a What activities would you class as Computer Crimes?

*intrusion, direct or indirect destruction of hardware, software or data*

4b Do you have any examples of such?

*read the papers or visit your local bookstore...*

68, male, 11 yrs exp, unix, no.

3a What skills do you feel a good cracker needs?

*Imagination, technical skills, social skills*

3b What would you say their main motives are?

*2 types – a=technical challenge, b=malicious*

3c What percentage of crackers are male?

*90%*

3d Do you feel that their activities are beneficial or harmful to society?

*type a – yes*
*type b – no*

3e Why?

*type a disseminate information & help to produce reliable software*

4a What activities would you class as Computer Crimes?

*damage, misuse of personal information, denial of service [but not theft of service]*

69, male, 20 yrs, exp, unix, yes, no, yes, no.

2a Have you ever hacked into a computer system on which you do not have authorised access? Your answers will be treated in strictest confidence!

*That depends on what you mean by "authorised access." As a student, I once logged in to a computer at a previous employer to look around for a few friends. My account had been deleted, and I used an seldom used, unprivileged service account. Did the admins want me to use that account? Probably not. Was I authorized to use the system? By TCSEC criteria, yes.*

*So, my answer to this question is twofold. No, I haven't cracked a computer system in the way most people think of cracking. Yes, I've used a computer system that I probably shouldn't have used.*

3a What skills do you feel a good cracker needs?

*In order to be a good cracker, they need intelligence, creativity, and knowledge of the OS they're trying to crack. What they *need*, though, is to learn ethical conduct, that their activities may have real negative effects of people, and responsible behavior.*

3b What would you say their main motives are?

*That varies from cracker to cracker. Some of the possibilities are revenge, espionage, the need for a challenge, pride, and extreme egotism.*

3c What percentage of crackers are male?

*There's no way to know. I think most of the reported ones have been male.*

3d Do you feel that their activities are beneficial or harmful to society?

*Harmful.*

3e Why?

*Great resources in manpower, time, money, and computers have been expended attempting to stop cracking. This isn't just in countering known risks, but in anticipating the potential risk. These resources are much better spent on the tasks for which they were intended. All of the large number of sysadmins I know would prefer to be free from the threat of their systems being cracked.*

*Cracking also reinforces irresponsible, megalomaniacal, anti-social behavior.*

4a What activities would you class as Computer Crimes?

*The definition of a crime depends on the jurisdiction. Here's a list of what I think should be classed as a computer crime:*

- *intentionally damaging data belonging to other users*
- *using computer resources beyond that allowed one by the sysadmin*
- *denial of access attacks*
- *viewing another user's private data that one hasn't been granted access to.*

*The second point is a poor attempt to draw a fine line. On the one hand we have legitimate users. This includes those who have an account, those who use anonymous ftp services in a polite fashion, and those who properly use other network facilities (finger, mail, etc.) On the other, we have illegitimate users.*

*This includes people who sniff passwords and use them, those who exploit the well-known sendmail bug, and those who use other network services to steal cycles from a machine they don't have legitimate access on.*

4b Do you have any examples of such?

*Internet Worm*
*Cracking by the Legion of Doom (?)*
*Activities described in Stoll's _The Cuckoo's Egg_.*

5 Do you have any further comments that you wish to make?

*Not really. I think my attitudes towards crackers are clear.*

70, female, 12 yrs exp, no.

3a What skills do you feel a good cracker needs?

*a) Don't know as never bothered to find out*
*b) A good reason or desire to do it.*

3b What would you say their main motives are?

*A challenge*

3c What percentage of crackers are male?

*How to I know?*

3d Do you feel that their activities are beneficial or harmful to society?

*Yes and No - depends what they do.*

3e Why?

*If they change data (for better or for worse) then it is harmful*

4a What activities would you class as Computer Crimes?

*Changing computer information. I see no harm in browsing. If the information is very very confidential and personal and should not be seen by unauthorised people then a system should be used that where it is impossible to hack into it.*

5 Do you have any further comments that you wish to make?

*Good luck!*

71, female, 20 yrs exp, unix, no.

3a What skills do you feel a good cracker needs?

*Persistence, and some degree of knowledge about system design in general, and the system to be cracked in particular – how much of each depending on the system in question.*

3b What would you say their main motives are?

*It depends. Most of the old-style (as in 10 to 15 years back) crackers seem to have been motived mainly by curiosity and the intellectual challenge of cracking a protected system. As far as I can tell many of them still feel this way, though I would not be surprised, given the exponential growth of network use and the expansion of the user base from the research-lab coterie to the more general public, if more venal and malicious motives (theft, various forms of deliberately causing trouble for other people) were reaching significant proportions.*

3c What percentage of crackers are male?

*Damn near all of them, I expect.*

3d Do you feel that their activities are beneficial or harmful to society?

*It depends.*

3e Why?

*It depends on what they actually do. If a cracker just gets into a protected system, pokes around a little without damaging anything, and then goes away, I find it very hard to consider him guilty of a crime. If he does this when the system is under heavy load from its regular users, or if his otherwise non-destructive presence loads the system enough to make things more difficult for the regular users, that's a social offense. If he damages files or the running system, or uses information he has seen which was intended to be private, that becomes significantly more objectionable.*

*On the ITS system (Incompatible Time Sharing – an MIT homebrew system for PDP10s) there was no security. Or rather, there was security through obscurity – you simply had to be able to figure out where stuff was in order to do things. This meant that there was essentially no challenge in trying to, say, look at other people's files, or make system messages print out differently, or crash the system. Some guest users did do these things briefly, but they quickly grew tired of them. Having no file security had the great advantage of letting people collaborate without having to go through any amount of fuss whatsoever about permissions – and the additional feature of allowing people not included at first, who happened to poke around and notice a project, to chime in if they had anything useful to say.*

*This was at a university research lab, so the impulse to secrecy that occurs in other settings wasn't present except in very small doses – for instance, lab personnel and financial records were not kept on the ITS machines. And we've run out of PDP10s these days.... But returning to your question: I feel that, in general, cracking activity ranges in effect from actively harmful to neutral. In some cases, probably a small number, it could be considered useful – for instance, a cracker who finds an easy way into a system he believes ought to be better protected, and informs the authorities there about it. I think Robert Morris got shafted a lot worse than he deserved; if he had been – or felt – able to do his project with some degree of openness, and to have someone competent review the code, I think it would have been a useful network experiment, not a crime.*

4a What activities would you class as Computer Crimes?

*Actual damage, theft, or misuse of services.*

4b Do you have any examples of such?

*Credit card fraud. Phone hacking. To varying degrees, theft of software found online. Vandalism to files or the running system. Misuse of information intended to be private (up to a point – have you read Shockwave Rider?)*

5 Do you have any further comments that you wish to make?

*Not offhand.*

*Good luck.*

## 72, female, ? yrs exp, unix, yes (but with an authorised users permission)

*I began using computers in elementary school, when the Apple company donated them to our school. Basically, back then, I just used the programs to help me learn math. The computer was used as an incentive, if one finished the lesson early, one could use the computer for the remainder of the period. I did not begin to program in BASIC until junior high school, when special classes were offered after school. I lost all interest in them in high school, and did not begin to program again until after being at MIT for three years.*

2a Have you ever hacked into a computer system on which you do not have authorised access? Your answers will be treated in strictest confidence!

*I once had to "hack" into a computer for which I did not have autorized access, but I did so with the permission of those who did have authorized access and had managed to lock themselves out of the system by logging in as root and messing around with access files they did not fully understand.*

2d Do you feel that such activities fulfil a positive purpose?

*Being able to hack is like being a lockpick. It is a good skill to have, when your friends lock themselves out of their computers, but I would not hack into someones account any more than I would break into someone's home. I consider what most sporting hackers do to be both illegal and immoral, under the crime of tresspassing.*

3a What skills do you feel a good cracker needs?

*Well, you have to understand networks and root systems, most of the hacking people do is by finding out passwords to systems which a regular user doesn't know about. If you can log in to a system as root, using the root passsword, you are recognized as a "superuser" by the system and are given special permissions with the system. There is a program called "Supercrack" which is available which can crack an password using english words and common names a matter of seconds or minutes, however some companies now require that all employees register their passwords and the company will tell them if the password is acceptable (can not be broken by supercrack). Such passwords are eight characters in length and often contain capital letters, numbers and symbols such as periods. For example the password "mypassword" would be easily found by supercrack, but "My.Passwd" would not. A friend of mine was working at Raytheon and was asked if their system was secure. He said he would let them know and brought in supercrack over the Internet. He was able to break 80% of the passwords in half a day. He sent everyone whose account he could access a note, over e-mail, that they should change their password. Also, there are "people leaks." If I install a security system for your company, I would probably install an extremely complex back-door password such as Ctrl-alt-f 2Y67UI333 Alt-8 2290TYU (which nothing can figure out) this is a master key. It would let me in to do anything to your system. If I told this to anyone in my circle of friends, it might get out, it might not. I know people know these things, but I don't know how exactly.*

*You learn how to be a hacker by hanging around other hackers until someone takes you into their confidence. How do lockpicks become lockpicks?*

3b What would you say their main motives are?

*Mostly fun and a secret joy of the power to look into other peoples secret things. Sometimes, when I listen to them, their glee of breaking into a system sounds like the prankish glee of boys who have managed to steal something from a womens' underwear drawer without being caught. I look on both activities with the same puzzeled distain.*

3c What percentage of crackers are male?

*Most, probably 90%, I think it has something to do with the "to boldly go where no man has gone before" attitude of the whole thing*

3d Do you feel that their activities are beneficial or harmful to society?

*neither, just stupid. People waste a lot of thime hacking and now companies have to waste a lot of money on computer security, which just provides jobs for the hackers when they grow up.*

3e Why?

*It would be nice if everyone could respect privacy.*

4a What activities would you class as Computer Crimes?

*Things which are harmful, destruction or theft of data. I don't like "harmless" snooping either, and I think they should be given the same punishment as "peeping Toms"*

4b Do you have any examples of such?

*People I've known who have been mad at each other have destroyed each others files, which is very nasty and harmful and devastating.*

5 Do you have any further comments that you wish to make?

*No, I think I've worked them in, sorry for the non-standard format*

73, male, 14 yrs exp, yes, yes, no.

3a What skills do you feel a good cracker needs?

*-Patience!*
*-Experience knowing how programmers and system administrators tend to do things, e.g., where they get careless, where they don't check for errors.*
*- Knowledge of specific known security holes.*
*- Knowledge of general security features/misfeatures in various systems.*
*- Knowledge of human factors. (Does a given person write all his passwords down on a scrap of paper he keeps in his desk? If so, why bother banging on exotic kernel idiosyncracies. A successful cracker is perceptive enough to recognize obvious non-technical solutions to problems.)*
*- Caution.*
*- Good record-keeping skills.*

3b What would you say their main motives are?

*Everything from innocent curiosity to truly evil intent.*

3c What percentage of crackers are male?

*I'd guess at least 95%, but probably less than 98%.*
*Then again, I could be a bigot. Maybe the female crackers are just smart enough not to get caught or brag about it. :-)*

3d Do you feel that their activities are beneficial or harmful to society?

*Both.*

3e Why?

*Some harm is done by descructive crackers; valuable work is lost, people's time is wasted, etc. However, The presence of a large number of non-destructive, merely curious crackers causes system administrators and operating system designers to work harder to develop reliable security systems for their own use and for others. As an example,consider the fact that most UNIX systems, though not perfect, have much greater security than PC operating systems. The reason for this is that UNIX systems supported multiple users, networking, and server-client systems long before PCs. I'm not sure about this anymore, but the last time I checked, there were many more UNIX machines on the Internet than PCs, even though the install base for PCs is much greater.*

*You might ask the same question about germs. Are germs harmful or beneficial? They are certainly harmful in the sense that they can cause disease, but if you consider the fact that is impossible to eliminate them entirely, then it becomes clear that their presence in moderate numbers is necessary for the development of the immune system—a system which can later save you from more serious threats.*

4a What activities would you class as Computer Crimes?

*Most "Computer Crimes" involve information as property (in this case, the kind of information which, by its size or nature, is naturally stored on a computer.) Thus, breaking into a system is a form of trespassing and software piracy is a form of theft.*

*It is usually not the computer itself that is important, but the information. Stealing a computer is not a "Computer Crime" and neither is smashing a VAX one over someone's head or shoplifting a box of blank floppy disk from a electronics store. Those are ordinary crimes.*

*The reason there is a lot of controversy about the nature of computer crime is that not everyone is comfortable with the idea that information can be property. Information is very different from other types of property, in that it is extremely easy to duplicate. This concept has been beaten to death in the literature (see any of the publications by the EFF, any copy of Wired magazine, any recent copyright law case, such as the recent AT&T/BSDI lawsuit, or any of numerous libertarian-dominated newsgroups.)*

5 Do you have any further comments that you wish to make?

*Put your dissertation up for ftp or on the WEB when you're done. :-)*

*Good luck!*

77, male, 18 yrs exp, unix, yes, yes, no, yes.

2d Do you feel that such activities fulfil a positive purpose?

*When I was doing cracking back in the mid 80s, it fulfilled a purpose in that I didn't have access to the types of machines that I wanted access to. So, it filled a gap. Unfortunately, I didn't learn as much as I had hoped I would.*

3a What skills do you feel a good cracker needs?

*Cracking varies from Real Hacking, in that anybody who has the persistance can do it.*

*However, if you're the one going out, reading the tech manuals, coming up with new logins and code to patch the OS, etc, then you're doing some of both (doing Real Hacking to crack a system).*

*I'd consider myself more of a hacker than a cracker anymore. There's not much sport in it, and I'm over 18. :-)*

3b What would you say their main motives are?

*Boredom ("rich" kids with smarts and nothing to use them on). A sense of power, in some respects. Doing something illegal for the thrill of it.*

3c What percentage of crackers are male?

*It used to be 99%-ish. I'd say, probably, 95%-ish now. There were some female hangers-on (we used to call them "hacking groupies"), but they were generally the same girls who'd date the math club. ;-)*

3d Do you feel that their activities are beneficial or harmful to society?

*Poor society, victimized by a bunch of kids. They are neither.*

3e Why?

*Because hacking OR cracking is largely a value-neutral activity, with respect to the rest of society. You live to hack, and hack to live (or, can substitute crack for hack there).*

4a What activities would you class as Computer Crimes?

*Destruction of property above and beyond the call of remaining undiscovered, certainly. This includes informational property. Stealing and selling information (I guess you'd term this industrial espionage). I don't think hacking a system just to get in, poke around, etc, is really a crime.*

*Now, if the government or a corporation uses the computer to spy, collect information on you, pry, etc, then I consider that a crime. Privacy should be protected.*

4b Do you have any examples of such?

*RISKS Digest has quite a bit on industrial espionage. You can get back issues somewhere off ftp.sri.com. I can find out exactly, if you want to know. :)*

5 Do you have any further comments that you wish to make?

*Your questionnaire is a little colored, and I think it's a little silly that you'd check out _The_New_Hacker's_Dictionary_ to get information on cracking from Real Hackers. I'd be curious what slant you're trying to put on things, that's all. But I've learned to be a cynic. :)*

*Are you going to summarize to respondants?*

48, male, 15 yrs exp, unix, no.

3a What skills do you feel a good cracker needs?

3b What would you say their main motives are?

3c What percentage of crackers are male?

*don't know*

3d Do you feel that their activities are beneficial or harmful to society?

*harmful*

3e Why?

*for there is no need to meddles in a system, just for fun.*

4a What activities would you class as Computer Crimes?

*cracking, hacking in the sense of question (3), stealing of software and data from individuals or companies.*

49, male, 15 yrs exp, unix, y, y, n, y.

3a What skills do you feel a good cracker needs?

*smart, ability to keep his/her mouth shut (bragards get caught)*

3b What would you say their main motives are?

*1. curiousity*
*2. maliciousness*

3c What percentage of crackers are male?

*95*

3d Do you feel that their activities are beneficial or harmful to society?

*harmful*

3e Why?

*they create a fear of computers and the people who use/understand them*

4a What activities would you class as Computer Crimes?

*depends on site cracked, misdemeanor to felony*

4b Do you have any examples of such?

*any time someone's credit or personal info is accessed w/out approval (including by corps and gov't)*

5 Do you have any further comments that you wish to make?

*it will only get worse*

*I'd be interested in seeing the results of this.*

50, male, 18 yrs exp, VMS, no.

3a What skills do you feel a good cracker needs?

*Knowledge of the particular vulnerabilities of the operating system under attack. Knowledge of the password habits of the type of users of the system.*

3b What would you say their main motives are?

*Proving they can overcome the defences placed by an inferior intelligence. Intellectual vandalism.*

3c What percentage of crackers are male?

*90+%*

3d Do you feel that their activities are beneficial or harmful to society?

*Definitely harmful.*

3e Why?

*I grew up in a society where someone could go away for several weeks and leave their house unlocked. It was not even a consideration that someone might choose to burgle the house. I do not consider living in a fortress an improvement.*

*Preventing accidental access is reasonable. But having to actively defend against intruders is a diversion of valuable resources, and constitutes theft from the owner of those resources.*

4a What activities would you class as Computer Crimes?

*Any use of computing resources that is not explicitly authorized by the administrator of those resources (on behalf of the person/organisation that pays for those resources).*

4b Do you have any examples of such?

*Playing games on computers belonging to organisations that explicitly prohibit that use of their machines.*

*Writing a novel on a word processor owned by an organisation that explicitly states that use of its resources for non-work-related purposes is not allowed.*

*Some of these crimes qualify as victimless crimes (like prostitution). Such crimes should be dealt with by educating the perpetrator as to exactly why the prohibitions are in place, and indicating that further violations will be viewed as attacks on the property of the owner of the resources. When the activity actively costs the owner of the resources money, or makes those resources unavailable for legitimate purposes, it should incur appropriate penalties. My idea of appropriate penalties would be thought shocking by the majority of people (see below).*

5 Do you have any further comments that you wish to make?

*I would execute writers of virii. They have demonstrated a willingness to violate the rights of others to such an extent that their continued presence in society is unjustifiable.*

51, male, 24 yrs exp, unix, no.

3a What skills do you feel a good cracker needs?

*stupidity, ignorance, selfishness, thoughtlessness*

3b What would you say their main motives are?

*self-aggrandization*

3c What percentage of crackers are male?

*100*

3d Do you feel that their activities are beneficial or harmful to society?

*harmful*

3e Why?

*They take away the benefits of good programming, hence they discourage good programming, which is to the detriment of us all.*

4a What activities would you class as Computer Crimes?

*software piracy, software fraud, cracking, plus the usual definition, which is the use of computers to perform crimes (usually theft)*

4b Do you have any examples of such?

*no - read the papers*

5 Do you have any further comments that you wish to make?

*Why don't you study something redeeming about computers, rather than one of the worst aspects of some users of them?*

*Sorry, I'm grumpy this morning, and software piracy, etc. are some of the things in life that anger me the most.*

52, male, 19 yrs exp, VMS, no.

3a What skills do you feel a good cracker needs?

*Intelligence, persistance, a love of puzzles and a drive to solve them, a knowlege of human frailty.*

3b What would you say their main motives are?

*becaus it's there. to prove that they can.*

3c What percentage of crackers are male?

*90%*

3d Do you feel that their activities are beneficial or harmful to society?

*Usually neutral. Most get onto a system, play around and get off without doing any real damage. Some do real damage so there is some loss. Their existence leads companies and governments to plug security holes before some more significant loss occurs so there is some gain. Generally I think it balances out.*

4a What activities would you class as Computer Crimes?

*Writing and/or knowingly disseminating virus programs that damage data or equipment. Unauthorized altering or damage to data on systems. Reading and/or disseminating private information.*

53, male, 12 yrs exp, MS-DOS, y, y, n, Sometimes.

3a What skills do you feel a good cracker needs?

*Math, and logistics skills.*

3b What would you say their main motives are?

*Curiosity.*

3c What percentage of crackers are male?

*I'd say 95%.*

3d Do you feel that their activities are beneficial or harmful to society?

*Neither.*

3e Why?

*I don't feel that there's enough of an effect.*

4a What activities would you class as Computer Crimes?

*Er, none, really.*

54, male, 25 yrs exp, VM/ESA CMS, y, y, y, n.

3a What skills do you feel a good cracker needs?

*access and where the system manager makes attempts to deter intruders)*
*Skill, courage, lack of personal-ethics, ability to program in C.*

3b What would you say their main motives are?

*Personal gain, and self-empowerment.*

3c What percentage of crackers are male?

*50%*

3d Do you feel that their activities are beneficial or harmful to society?

*Harmful.*

3e Why?

*Interrupt productive systems; force system-programmers to do non-productive work.*

4a What activities would you class as Computer Crimes?

*Accessing unauthorized systems.*
*Unauthorized use of functions on those systems.*

58, male, 12 yrs exp, MS-DOS, no.

3a What skills do you feel a good cracker needs?

*Wit, intelligence, patience*

3b What would you say their main motives are?

*Curiosity*

3c What percentage of crackers are male?

*95*

3d Do you feel that their activities are beneficial or harmful to society?

*Only if with malicious intent (i.e. vary rarely)*

3e Why?

*Is only harmful when the hacker sets out to hurt someone, rather than satisfy curiosity.*

59, male, 7 yrs exp, unix, y, n, n, y.

3a What skills do you feel a good cracker needs?

*patience*

3b What would you say their main motives are?

*exploration*

3c What percentage of crackers are male?

*85*

3d Do you feel that their activities are beneficial or harmful to society?

*beneficial*

3e Why?

*We, as a society, are moving to wards becoming completely computerized. Should we trust our lives to such poor;y designed systems? I think not!*

4a What activities would you class as Computer Crimes?

*Unethical use of computers (i.e. changing information you have no access for, reading other persons PRIVATe documents, etc.*

60, male, 15 yrs exp, unix, y, n, y, n.

3a What skills do you feel a good cracker needs?

*To crack requires either knowledge of security weaknesses in the computer system of the ability to acquire legitimate userids and passwords via weaknesses in other systems or human errors. A good cracker will have access to a wide range of other crackers, a fair amount of technical skill, and the ability to peek over other people's shoulders.*

3b What would you say their main motives are?

*The feeling of having accomplished something forbidden or frowned upon by society at large.*

3c What percentage of crackers are male?

*Almost all I would imagine, although really I have no idea.*

3d Do you feel that their activities are beneficial or harmful to society?

*Potentially harmful, but in practice not much so.*

3e Why?

*If cracking were perceived as endemic and widespread, people wouldn't trust the answers machines produce or the communications they receive via machine. But it isn't. (Also the obvious point about the dangers of using potentially critical resources, and violating people's right to privacy)*

4a What activities would you class as Computer Crimes?

*Any unauthorised access (with varying degrees of seriousness depending on what one had done inside the system.)*

5 Do you have any further comments that you wish to make?

*When I did crack (and I didn't very much) about 6 years ago, I found it pretty unrewarding - although I can understand why people with stamp-collecting or puzzle-solving mentalities might find it addictive. I guess if I had found it a lot of fun I might have a more positive view of it, although perhaps I'm just more considerate to legitimate users these days.*

62, male, 15 yrs exp, unix, n.

3a What skills do you feel a good cracker needs?

*Knowledge of the system. Access to the system. Access to known useful cracker codes.*

3b What would you say their main motives are?

*Generally Evil. Nothing like what we did.*

3c What percentage of crackers are male?

*I have no statistics.*

3d Do you feel that their activities are beneficial or harmful to society?

*Depends on who does what for what reason. Random hijacking of systems is like joyriding. Illegal and immoral.*

*Breaking into a system to which "one has lost the key" is like a locksmith opening up someones house for them.*

3e Why?

*Damage to data, log files, etc. Theft of services or data.*

4a What activities would you class as Computer Crimes?

*Breaking into systems belonging to others; altering files belonging to others; theft of data beloning to others; denial of service.*

4b Do you have any examples of such?

*They are legion. What precisely are you trolling for?*

5 Do you have any further comments that you wish to make?

*Simplest way to get at many systems is to take them down, bring them up "standalone" and to hack the password file. Inelegent but simple and effective.*

63, 16 yrs exp, unix, male, no.

3a What skills do you feel a good cracker needs?

*A good understanding of the operating system which s/he is trying to crack, and possibly a high degree of cryptographic knowledge (I say 'possibly' because that would depend upon the method of the cracking - if using 'backdoors' or other 'features' of the operating system, cryptography may be unnecessary).*

3d Do you feel that their activities are beneficial or harmful to society?

*Could be both (or either), depending upon their motives and what they do once they've gained access.*

3e Why?

*Why not?*

4a What activities would you class as Computer Crimes?

*Damaging a computer, or parts of a computer, that is (are) someone else's property.*

4b Do you have any examples of such?

*#1) Breaking a monitor with a hammer.*
*#2) Formatting a hard disk without permission of its owner.*

65, female, 14 yrs exp, unix, y, n, n, n.

3a What skills do you feel a good cracker needs?

*Patience. _Lots_ of patience. :) Stubbornness. Lack of anything better to do.... and a broad general knowledge of computers.*

3b What would you say their main motives are?

*Trophy collecting; "Hey, I hacked into A last night!" "Oh, I got in there_months_ ago. But I did B and C as well. Easy."*

3c What percentage of crackers are male?

*Given my answers above, I can't say 100%. But I'd certainly like to. 95%+.*

3d Do you feel that their activities are beneficial or harmful to society?

*Harmful when they are one or the other. Mostly I suspect they do neither harm nor good.*

3e Why?

*See answer above.*

4a What activities would you class as Computer Crimes?

*"Rampantly stupid in charge of a computer" – anyone who's in charge of any system ought to have at least some idea what they're doing. Unfortunately, many do not. Unauthorised access where it can be proved that intentions were malicious, or that harm was caused (just looking, as long as it's not at private or secret information, shouldn't be a crime; both of those categories should be properly secured, of course)*

4b Do you have any examples of such?

*see above*

> 5 Do you have any further comments that you wish to make?

*Can I see the results of this sometime?*

*No problem. Good luck with the Phd.*

67, female, 14 yrs exp, DOS, no.

3b What would you say their main motives are?

*"Because it is there" syndrome*

3c What percentage of crackers are male?

*80+*

3d Do you feel that their activities are beneficial or harmful to society?

*Harmful*

3e Why?

*Ultimately they will cause an over-reaction leading to a curtailment of liberty*

4a What activities would you class as Computer Crimes?

*Same as any other crime including invasion of privacy, embezzlement, malicious mischief, etc.*

76, male, 23 yrs exp, MS-DOS, no.

3a What skills do you feel a good cracker needs?

*I disagree with 'good cracker'. Perhaps successfull, or talented. Anyway: patience, technical knowledge, psychological understanding, creativity.*

3b What would you say their main motives are?

*Showing off (to themselves), intellectual challenge, admiration by fellow crackers. Ego.*

3c What percentage of crackers are male?

*95-105*

3d Do you feel that their activities are beneficial or harmful to society?

*Definetly harmful.*

3e Why?

*Cost to the victim sites in recovering, and evaluating if any 'real' damage was done, as well as stolen communications costs.. Violation of privacy. Increased uncertainty about what happens to all the data 'the system' has on me. General glorification of criminal acts.*

4a What activities would you class as Computer Crimes?

*If you mean in strict legal sense, that depends on the coutry and time. But in moral sense: Unauthorised entry and use of resources, stealing of data and/or programs, modifying data, planting of malicious software, blackmail with threats of any of these, unauthorised filing of sensitive personal data, unauthorised cross-checking of official databases (e.g. insurance policies against welfare),etc.*

4b Do you have any examples of such?

*Yes.*

5 Do you have any further comments that you wish to make?

*I've seen an analysis of a the costs of a 'harmless' virus attack on a large office. Alone the cost in lost work hours due to down-time while waiting for the speocialists to get to this machine was incredible.*

*Denmark has a pretty restrictive law about what the authorities may do with their databases, which I think is a good thing.*

*Do you intend to publish your study? May I have a copy?*

# Appendix B

This appendix contains the questionnaire and results from the survey conducted to collect information about bank employees attitudes to their jobs. The data was collect between the summer 1993 and the spring 1994. The response rate was just over 40 per cent.

# Attitude Survey

This survey is undertaken by **Simon Rogerson MBA, ACIB** as the research element of his PhD in Management. Simon was employed by a major clearing bank until September 1990 when he left to take an MBA at the **Canterbury Business School at the University of Kent.**

The aim of this survey is to find out your opinions on a range of issues associated with working within the Financial Services Sector, a sector that has experienced much change over the last few years. In particular the questions will focus on the role of computers in banking.

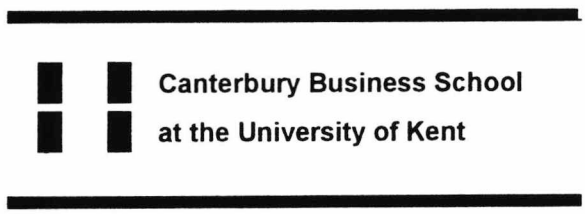
Simon would like to take the opportunity of thanking you in anticipation for your assistance. Should you have any questions regarding this survey please do not hesitate to contact him on **(0227) 764000 ext.7922.**

**Confidentiality**

This survey is totally confidential; no other member of your employing company will see your answers. Should you decide to make further comments at the end of any section of the questionnaire these may be quoted in the eventual thesis, if you do not wish them to be reproduced in this way please indicate accordingly.

## Thank You for your time.

Simon Rogerson MBA, ACIB,
Canterbury Business School,
The University,
Canterbury, Kent,
CT2 7PE.



# Attitude Survey
# Part 1

**Please tick the appropriate box.**

**1. Gender**

| | | | |
|---|---|---|---|
| **Female** | 1 | **Male** | 2 |

**2. Age**

| **16-21** | **22-29** | **30-39** | **40-49** | **50+** |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

**3. Marital Status**

| | | | | | |
|---|---|---|---|---|---|
| **Single** | 1 | **With long term partner** | 2 | **Other** | 3 |

**4. Qualifications**

| | |
|---|---|
| No formal qualifications | 01 |
| O Levels/GCSE's | 02 |
| A Levels | 03 |
| BTec | 04 |
| Diploma or Certificate (HND, HNC, etc.) | 05 |
| Degree | 06 |
| Banking Certificate | 07 |
| Associate Exams | 08 |
| MBA | 09 |
| Other (Please state:- ) | 10 |

**5. Your Area of Work**

| | |
|---|---|
| Accounts Department | 01 |
| Cash Tills | 02 |
| Enquiries/ Customer service | 03 |
| Foreign Desk | 04 |
| Loans Department | 05 |
| Securities Department/ Stock Ex. | 06 |
| Management | 07 |
| Computer Department | 08 |
| Other (Please state: ..... ) | 09 |

**6. Length of Service**
**With Current Bank**

| <1 year | 1-2 years | 2-5 years | 5-10 years | >10 years |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

**In Current Branch**

| <1 year | 1-2 years | 2-5 years | 5-10 years | >10 years |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

**7. Your Pay Range**

| <£10,000 | £10-15,000 | £15-20,000 | £20-25,000 | >£25,000 |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

# Part 2
# Your Opinions of Your Work and Your Working Environment.

**1. Job Satisfaction**

How satisfied are you with the following aspects of your job?

| | |
|---|---|
| **Very Satisfied** | **2** |
| **Very Dissatisfied** | **-2** |

| | 2 | 1 | 0 | -1 | -2 |
|---|---|---|---|---|---|
| Pay -Including benefits such as preferential rate loans | | | | | |
| Job Security | | | | | |
| Number of hours worked | | | | | |
| General management | | | | | |
| Direct Supervision | | | | | |
| Relationship with supervisor | | | | | |
| Bank policy and administration | | | | | |
| The work itself | | | | | |
| Responsibility/ Autonomy | | | | | |
| Relationship with peers | | | | | |

**Any other comments?**

**2. How do you feel about your job?**
How strongly do you agree with the following statements?

| | |
|---|---|
| **Very Strongly Agree** | **2** |
| **Very Strongly Disagree.** | **-2** |

| | 2 | 1 | 0 | -1 | -2 |
|---|---|---|---|---|---|
| I get a lot from my job | | | | | |
| My abilities are underused in my current job | | | | | |
| Others are paid more fairly than me | | | | | |
| I would leave if I could | | | | | |
| The bank is well run | | | | | |
| My work makes me tense | | | | | |
| The bank's directors are overpaid | | | | | |
| I feel secure in my job | | | | | |
| The bank is poorly run | | | | | |
| I am happy at work | | | | | |
| I would call in sick to attend a job interview with another company | | | | | |
| A bank clerk's role has changed from one of service to one of selling | | | | | |
| I am only working here because of the poor state of the job market at present | | | | | |
| If I knew then what I know now I would not have joined this bank | | | | | |

**Any other comments?**

**3. Computers at work**

The use of computers has increased over the last two decades. What are your views of them in general and on their use in banking in particular? Please indicate whether you agree with the following statements:

| | |
|---|---|
| **Very Strongly Agree** | **2** |
| **Very Strongly Disagree.** | **-2** |

| | 2 | 1 | 0 | -1 | -2 |
|---|---|---|---|---|---|
| I have a good understanding of computers | | | | | |
| I have had much experience of computers and their possible applications | | | | | |
| Viruses are a major threat to computer users | | | | | |
| Hackers are a major threat to computer users | | | | | |
| If a colleague used unauthorised software or hardware they should be dismissed | | | | | |
| I would "turn a blind eye" if a colleague amended their bank credit card limit using a branch terminal | | | | | |
| I would alter the balance of my account if I knew I would not get caught | | | | | |
| Bank clerks are in general honest | | | | | |
| Computers make my job easier | | | | | |
| I write my own programs (Please indicate the language use: ..... ) | | | | | |
| I have a modem at home (Please indicate the services used: .... ) | | | | | |
| I enjoy using computers | | | | | |
| I have acquired a good understanding of computers from bank training courses | | | | | |
| I have a poor understanding of the computers that the bank uses | | | | | |

**Any other comments?**

**4. Attitude to crime and deceitful behaviour**

How would you score the following acts? If the theft of an unlocked bicycle were to score 10 how would the following score relative to that? For instance if you feel that the theft of an umbrella was only half as bad as the theft of an unlocked bicycle you should score it 5. Please put an X in the box if you are unfamiliar with the case.

| | |
|---|---|
| **Theft of an unlocked bicycle** | **10** |
| **The act is thirty two times as bad as the theft of an unlocked bicycle** | **320** |
| **The act is twice as bad as the theft of an unlocked bicycle** | **20** |
| **The act is not a crime. It is acceptable behaviour** | **0** |

| | |
|---|---|
| Robert Maxwell's misuse of pension funds | |
| The theft of £100 from the till | |
| A loans officer takes out loans in a false name | |
| A junior clerk makes phone calls to a boyfriend in Australia. The total cost of the calls increases the branch's telephone bill by over £100 a month | |
| A clerk who is on self certified sick leave spends the day writing a computer programme to help a local charity manage its books | |
| A clerk manages to access the computer system and instructs it to pay one penny of interest due to all the bank's customer's deposit accounts to his account instead | |
| A manager and a junior clerk act together to transfer £1,000,000 via CHAPS and then SWIFT to an account they have opened in South America | |
| The Barlow Clowes affair | |
| A clerk is using a computer at work to write a number of computer programmes for his own personal use | |
| A manager transfers £100,000 from a branch sundry account to a large corporate customer the day before he must report to regional office on the borrowing position of said client, the transfer takes the client below their overdraft limit. The following day he transfers the money back and has the statements retyped | |

**Any other comments?**

**How would you score the following acts?**

| | |
|---|---|
| Three women attack and mug a man on his way home late at night | |
| A clerk takes a box of envelopes home | |
| A clerk rings his mother every day. The cost of these phone calls adds £15 to the branch's monthly phone bill | |
| A computer operator at the foreign department delays payments to branch customers holding the money on a deposit account for a day so that he earns interest on the money at the customer's expense | |
| A clerk uses a wordprocessor at work to prepare their CV | |
| A clerk increases her credit card limit without authority. She needs the money to pay a gambling debt | |
| A clerk uses the photocopier to make 100 copies of their CV | |
| A clerk at a branch uses a terminal at his branch to place money on deposit over night in london in the name of a large corporate customer. He completes all necessary procedures but removes the entries for the customer's account before they can be processed. When the branch receives the interest payment he makes the appropriate enteries to credit his account with the £4,000 interest earned. | |
| A clerk uses a terminal to increase his overdraft limit without authorization. He needs the money to pay the rent | |
| A man is shot by a terrorist on a train. The terrorist escapes by jumping from the moving train | |

**Any other comments?**

questionnaire for the summer school participants

## Attitude Survey

*Dear MBA/MBS student,*

*believe me when I say that I understand how much pressure you are under, but I hope that you can spare a few minutes to complete the following questionnaire. The two sections are headed "Part four" and "Part Five" as they form part of a larger questionnaire which I am currently using to survey financial sector employees' attitudes. Your responses will be used for comparative purposes.*

*Thank you for your time,*

**Simon Rogerson**
*(a humble research student and former MBA student)*

Please tick as appropriate

1. Sex:

| | | | |
|---|---|---|---|
| Male | 1 | Female | 2 |

2.Age:

| <22 | 22-29 | 30-39 | 40-49 | 50+ |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

3. Martital status:

| | | | | | |
|---|---|---|---|---|---|
| Single | 1 | With long term partner (inc. Married) | 2 | Other | 3 |

4. Nationality:

| |
|---|
| |

5. Computer use:

| Expert | Experienced | Frequent user | Novice user | Non-user |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

6. Which programmes do you regularly use?

| Wordprocessor | Spreadsheet | Dos | Basic | Other computer language |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

If 5 please state which:

7. Which area of employment do you come from?

| Marketing | Finance | Production | Personnel | Other |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |

**Attitude to crime and deceitful behaviour**

How would you score the following acts? If the theft of £100 from the till were to score 80 how would the following score relative to that? For instance, if you feel that the theft of an umbrella was only half as bad as the theft of £100 from the till you should score it 40.

| | |
|---|---|
| **Theft of £100 from the till** | **80** |
| **The act is four times as bad as the theft of £100 from the till** | **320** |
| **The act is only a quarter as bad as the theft of £100 from the till** | **20** |
| **The act is not a crime. It is acceptable behaviour** | **0** |

**There is no limit to what you may score an act! 320 is only an example.**

| | Your Score |
|---|---|
| Robert Maxwell's misuse of pension funds | |
| The theft of an unlocked bicycle | |
| A loans officer takes out loans in a false name | |
| A junior clerk makes phone calls to a boyfriend in Australia. The total cost of the calls increases the branch's telephone bill by over £100 a month | |
| A clerk who is on self certified sick leave spends the day writing a computer programme to help a local charity manage its books | |
| A clerk manages to access the computer system and instructs it to pay one penny of interest due to all the bank's customer's deposit accounts to his account instead | |
| A bank manager and a junior clerk act together to transfer £1,000,000 via CHAPS and then SWIFT to an account they have opened in South America. | |
| The Barlow Clowes affair - the senior official of an investment firm defrauds many of millions of pounds. | |
| A clerk is using a computer at work to write a number of computer programmes for his own personal use | |
| A manager transfers £100,000 from a branch sundry account to a large corporate customer's account the day before he must report to his senior manager about the borrowing position of said client, the transfer takes the client below their overdraft limit. The following day he transfers the money back and has the statements retyped | |

[1] CHAPS and SWIFT are both money transfer systems used by banks.

**How would you score the following acts?**

| | Your Score |
|---|---|
| Three women attack and mug a man on his way home late at night | |
| A clerk takes a box of envelopes home | |
| A clerk rings his mother every day. The cost of these phone calls adds £15 to the branch's monthly phone bill | |
| A computer operator at the foreign department delays payments to branch customers holding the money on a deposit account for a day so that he earns interest on the money at the customers' expense | |
| A clerk uses a word processor at work to prepare her CV | |
| A clerk increases her credit card limit without authority. She needs the money to pay a gambling debt | |
| A clerk uses the photocopier to make 100 copies of his CV | |
| A clerk uses a terminal at his branch to place money on deposit over night in London in the name of a large corporate customer. He completes all necessary procedures but removes the entries before they can be processed and the customer debited. When the branch receives the interest payment from their head office three days later he makes the appropriate entries to credit his account with the £4,000 interest earned. | |
| A clerk telephones his girlfriend to tell her he is working late. The call costs the bank £1.47. | |
| A clerk uses a terminal to increase his overdraft limit without authorisation. He needs the money to pay the rent | |
| A man is shot by a terrorist on a train. The terrorist escapes by jumping from the moving train | |

**Any other comments?**

## *Part Five*

**General Section.**

1. Have you ever committed a crime? **Yes** **No**

If **Yes**, please tick those categories that apply (if more than once please add a **+**):

| | |
|---|---|
| Substance abuse; drug taking etc. | |
| Shoplifting | |
| General theft | |
| Pilfering at work | |
| Traffic offence | |
| Other - Please indicate: | |

2. Have you ever considered taking funds, or other assets, from your employer?
**Yes** **No**

3. It is acknowledged that the chances of you committing a crime against your employer are very slim, but if you did what do you think would be most likely to motivate you? Please rank each of the following for their relative strength (**5** being the strongest motivator, **1** the weakest):

| | |
|---|---|
| If a friend or member of your family needed money | |
| Revenge | |
| Peer pressure | |
| Boredom | |
| If you needed money | |

4. What do you think prevents you or your colleagues from behaving in a criminal way?

5. Please rank the following for their importance (**9** being the most important and **1** being the least) in preventing you from acting criminally:

| | |
|---|---|
| The belief that such behaviour is immoral | |
| The knowledge that such behaviour is illegal | |
| Security measures | |
| Procedures | |
| Fear of being caught | |
| Fear of prison | |
| What my family would think | |
| What my friends would think | |
| What my peers would think | |

6. What Starsign are you?

responses

BANK Is the respondent a clearing bank employee?

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| No | 0 | 19 | 18,4 | 18,4 | 18,4 |
| Yes | 1 | 84 | 81,6 | 81,6 | 100 |
| | Total | 103 | 100 | 100 | |

Valid cases 103 Missing cases 0

The respondents answering in the negative to this question were employed by one of the building societies.

## Question:

*Job satisfaction - How satisfied are you with the following aspects of your job?*

*Please also indicate whether you consider each of the factors as Very Important to you, Important, or Not Important at all to you.*

## A.1 Pay

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Not important | 0 | 0 | | | |
| Important | 1 | 30 | 29,1 | 31,3 | 31,3 |
| Very important | 2 | 66 | 64,1 | 68,8 | 100 |
| | Total | 96 | 93,2 | 100 | |

Valid cases 96 Missing cases 7

## A.2 Job security

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Not important | 0 | 0 | 0 | 0 | 0 |
| Important | 1 | 18 | 17,5 | 18,9 | 18,9 |
| Very important | 2 | 77 | 74,8 | 81,1 | 100 |
| | Total | 95 | | 100 | |

Valid cases 95 Missing cases 8

## A.3 Number of hours worked

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Not important | 0 | 19 | 18,4 | 20,2 | 20,2 |
| Important | 1 | 56 | 54,4 | 59,6 | 79,8 |
| Very important | 2 | 19 | 18,4 | 20,2 | 100 |
| | Total | 94 | | 100 | |

Valid cases 94 Missing cases 9

## A.4 General management

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Not important | 0 | 8 | 7,8 | 8,5 | 8,5 |
| Important | 1 | 44 | 42,7 | 46,8 | 55,3 |
| Very important | 2 | 42 | 40,8 | 44,7 | 100 |
| | Total | 94 | | 100 | |

Valid cases 94 Missing cases 9

## A.5 Direct supervision

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Not important | 0 | 25 | 24,3 | 26,9 | 26,9 |
| Important | 1 | 43 | 41,7 | 46,2 | 73,1 |
| Very important | 2 | 25 | 24,3 | 26,9 | 100 |
| | Total | 93 | | 100 | |

Valid cases 93 Missing cases 10

## A.6 Relationship with supervisor

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Not important | 0 | 6 | 5,8 | 6,5 | 6,5 |
| Important | 1 | 44 | 42,7 | 47,8 | 54,3 |
| Very important | 2 | 42 | 40,8 | 45,7 | 100 |
| | Total | 92 | | 100 | |

Valid cases 92 Missing cases 11

## A.7 Bank policy and administration

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Not important | 0 | 2 | 1,9 | 2,1 | 2,1 |
| Important | 1 | 64 | 62,1 | 68,1 | 70,2 |
| Very important | 2 | 28 | 27,2 | 29,8 | 100 |
| | Total | 94 | | 100 | |

Valid cases 94 Missing cases 9

## A.8 The work itself

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Not important | 0 | 1 | 1 | 1,1 | 1,1 |
| Important | 1 | 39 | 37,9 | 41,5 | 42,6 |
| Very important | 2 | 54 | 52,4 | 57,4 | 100 |
| | Total | 94 | | 100 | |

Valid cases 94 Missing cases 9

## A.9 Responsibility and autonomy

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Not important | 0 | 3 | 2,9 | 3,2 | 3,2 |
| Important | 1 | 59 | 57,3 | 62,8 | 66 |
| Very important | 2 | 32 | 31,1 | 34 | 100 |
| | Total | 94 | | 100 | |

Valid cases 94 Missing cases 9

## A.10 Relationship with peers

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Not important | 0 | 3 | 2,9 | 3,2 | 3,2 |
| Important | 1 | 51 | 49,5 | 53,7 | 56,8 |
| Very important | 2 | 41 | 39,8 | 43,2 | 100 |
| | Total | 95 | | 100 | |

Valid cases 95 Missing cases 8

## A.1A Pay

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very dissatisfied | -2 | 9 | 8,7 | 9,4 | 9,4 |
| Dissatisfied | -1 | 12 | 11,7 | 12,5 | 21,9 |
| Neither | 0 | 31 | 30,1 | 32,3 | 54,2 |
| Satisfied | 1 | 32 | 31,1 | 33,3 | 87,5 |
| Very satisfied | 2 | 12 | 11,7 | 12,5 | 100 |
| | Total | 96 | | 100 | |

Valid cases 96 Missing cases 7

## A.2A Job security

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very dissatisfied | -2 | 13 | 12,6 | 13,4 | 13,4 |
| Dissatisfied | -1 | 23 | 22,3 | 23,7 | 37,1 |
| Neither | 0 | 28 | 27,2 | 28,9 | 66 |
| Satisfied | 1 | 24 | 23,3 | 24,7 | 90,7 |
| Very satisfied | 2 | 9 | 8,7 | 9,3 | 100 |
| | Total | 97 | | 100 | |

Valid cases 97 Missing cases 6

## A.3A Number of hours worked

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very dissatisfied | -2 | 6 | 5,8 | 6,3 | 6,3 |
| Dissatisfied | -1 | 7 | 6,8 | 7,3 | 13,5 |
| Neither | 0 | 24 | 23,3 | 25 | 38,5 |
| Satisfied | 1 | 33 | 32 | 34,4 | 72,9 |
| Very satisfied | 2 | 26 | 25,2 | 27,1 | 100 |
| | Total | 96 | | 100 | |

Valid cases 96 Missing cases 7

## A.4A General management

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very dissatisfied | -2 | 6 | 5,8 | 6,3 | 6,3 |
| Dissatisfied | -1 | 15 | 14,6 | 15,6 | 21,9 |
| Neither | 0 | 39 | 27,9 | 40,6 | 62,5 |
| Satisfied | 1 | 29 | 28,2 | 30,2 | 92,7 |
| Very satisfied | 2 | 7 | 6,8 | 7,3 | 100 |
| | Total | 96 | | 100 | |

Valid cases 96 Missing cases 7

## A.5A Direct supervision

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very dissatisfied | -2 | 3 | 2,9 | 3,1 | 3,1 |
| Dissatisfied | -1 | 6 | 5,8 | 6,3 | 9,4 |
| Neither | 0 | 31 | 30,1 | 32,3 | 41,7 |
| Satisfied | 1 | 42 | 40,8 | 43,8 | 85,4 |
| Very satisfied | 2 | 14 | 13,6 | 14,6 | 100 |
| | Total | 96 | | 100 | |

Valid cases 96 Missing cases 7

## A.6A Relationship with supervisor

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very dissatisfied | -2 | 4 | 3,9 | 4,2 | 4,2 |
| Dissatisfied | -1 | 4 | 3,9 | 4,2 | 4,8 |
| Neither | 0 | 23 | 22,3 | 24,2 | 32,6 |
| Satisfied | 1 | 38 | 36,9 | 40 | 72,6 |
| Very satisfied | 2 | 26 | 25,2 | 27,4 | 100 |
| | Total | 95 | | 100 | |

Valid cases 95 Missing cases 8

## A.7A Bank policy and administration

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very dissatisfied | -2 | 9 | 8,7 | 9,4 | 9,4 |
| Dissatisfied | -1 | 20 | 19,4 | 20,8 | 30,2 |
| Neither | 0 | 43 | 41,7 | 44,8 | 75 |
| Satisfied | 1 | 22 | 21,4 | 22,9 | 97,9 |
| Very satisfied | 2 | 2 | 1,9 | 2,1 | 100 |
| | Total | 96 | | 100 | |

Valid cases 96 Missing cases 7

## A.8A The work itself

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very dissatisfied | -2 | 4 | 3,9 | 4,2 | 4,2 |
| Dissatisfied | -1 | 7 | 6,8 | 7,4 | 11,6 |
| Neither | 0 | 21 | 20,4 | 22,1 | 33,7 |
| Satisfied | 1 | 42 | 40,8 | 44,2 | 77,9 |
| Very satisfied | 2 | 21 | 20,4 | 22,1 | 100 |

| | | | | |
|---|---|---|---|---|
| | Total | 95 | | 100 |

Valid cases 95 Missing cases 8

## A.9A Responsibility and autonomy

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very dissatisfied | -2 | 5 | 4,9 | 5,3 | 5,3 |
| Dissatisfied | -1 | 10 | 9,7 | 10,6 | 16 |
| Neither | 0 | 26 | 25,2 | 27,7 | 43,6 |
| Satisfied | 1 | 38 | 36,9 | 40,4 | 84 |
| Very satisfied | 2 | 15 | 14,6 | 16 | 100 |
| | Total | 94 | | 100 | |

Valid cases 94 Missing cases 9

## A.10A Relationship with peers

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very dissatisfied | -2 | 2 | 1,9 | 2,1 | 2,1 |
| Dissatisfied | -1 | 1 | 1 | 1 | 3,1 |
| Neither | 0 | 20 | 19,4 | 20,6 | 23,7 |
| Satisfied | 1 | 51 | 49,5 | 52,6 | 76,3 |
| Very satisfied | 2 | 22 | 21,4 | 22,7 | 100 |
| | Total | 97 | | 100 | |

Valid cases 97 Missing cases 6

Number of Valid Observations (Listwise) = 85.00

| Variable | Mean | Std Dev | Min | Max | N | Label |
|---|---|---|---|---|---|---|
| A.1 | 1.69 | .47 | 1.0 | 2.0 | 96 | Pay |
| A.2 | 1.81 | .39 | 1.0 | 2.0 | 95 | Job security |
| A.3 | 1.00 | .64 | .0 | 2.0 | 94 | Number of hours work |
| A.4 | 1.36 | .64 | .0 | 2.0 | 94 | General management |
| A.5 | 1.00 | .74 | .0 | 2.0 | 93 | Direct supervision |
| A.6 | 1.39 | .61 | .0 | 2.0 | 92 | Relationship with su |
| A.7 | 1.28 | .50 | .0 | 2.0 | 94 | Bank policy and admi |
| A.8 | 1.56 | .52 | .0 | 2.0 | 94 | The work itself |
| A.9 | 1.31 | .53 | .0 | 2.0 | 94 | Responsibility and a |
| A.10 | 1.40 | .55 | .0 | 2.0 | 95 | Relationship with pe |
| A.1A | .27 | 1.13 | -2.0 | 2.0 | 96 | Pay |
| A.2A | -.07 | 1.18 | -2.0 | 2.0 | 97 | Job security |
| A.3A | .69 | 1.14 | -2.0 | 2.0 | 96 | Number of hours work |
| A.4A | .17 | .99 | -2.0 | 2.0 | 96 | General management |
| A.5A | .60 | .92 | -2.0 | 2.0 | 96 | Direct supervision |
| A.6A | .82 | 1.02 | -2.0 | 2.0 | 95 | Relationship with su |
| A.7A | -.13 | .94 | -2.0 | 2.0 | 96 | Bank policy and admi |
| A.8A | .73 | 1.03 | -2.0 | 2.0 | 95 | The work itself |
| A.9A | .51 | 1.05 | -2.0 | 2.0 | 94 | Responsibility and a |
| A.10A | 1.04 | 1.31 | -2.0 | 2.0 | 97 | Relationship with pe |

---

## Question:

*How strongly do you agree with the following statements:*

## B.1 I get a lot from my job

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 5 | 4,9 | 4,9 | 4,9 |
| Disagree | -1 | 12 | 11,7 | 11,7 | 16,5 |
| Neither | 0 | 30 | 29,1 | 29,1 | 45,6 |
| Agree | 1 | 40 | 38,8 | 38,8 | 84,5 |
| Very strongly agree | 2 | 16 | 15,5 | 15,5 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## B.2 My abilities are underused in my current

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 5 | 4,9 | 4,9 | 4,9 |
| Disagree | -1 | 17 | 16,5 | 16,5 | 21,4 |
| Neither | 0 | 30 | 29,1 | 29,1 | 50,5 |
| Agree | 1 | 31 | 30,1 | 30,1 | 80,6 |
| Very strongly agree | 2 | 20 | 19,4 | 19,4 | 100 |
| | Total | | | 100 | |

Valid cases 103 Missing cases 0

## B.3 Others are paid more fairly than me

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 7 | 6,8 | 6,9 | 6,9 |
| Disagree | -1 | 26 | 25,2 | 25,7 | 32,7 |
| Neither | 0 | 45 | 43,7 | 44,6 | 77,2 |
| Agree | 1 | 14 | 13,6 | 13,9 | 91,1 |
| Very strongly agree | 2 | 9 | 8,7 | 8,9 | 100 |
| | Total | 101 | | 100 | |

Valid cases 101 Missing cases 2

## B.4 I would leave if I could

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 23 | 22,3 | 22,8 | 22,8 |
| Disagree | -1 | 23 | 22,3 | 22,8 | 45,5 |
| Neither | 0 | 19 | 18,4 | 18,8 | 64,4 |
| Agree | 1 | 21 | 20,4 | 20,8 | 85,1 |
| Very strongly agree | 2 | 15 | 14,6 | 14,9 | 100 |
| | Total | | | 100 | |

Valid cases 101 Missing cases 2

## B.5 The bank is well run

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 19 | 18,4 | 18,6 | 18,6 |
| Disagree | -1 | 30 | 29,1 | 29,4 | 48 |
| Neither | 0 | 36 | 35 | 35,3 | 83,3 |
| Agree | 1 | 14 | 13,6 | 13,7 | 97,1 |
| Very strongly agree | 2 | 3 | 2,9 | 2,9 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

## B.6 My work makes me tense

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 17 | 16,5 | 16,8 | 16,8 |
| Disagree | -1 | 15 | 14,6 | 14,9 | 31,7 |
| Neither | 0 | 34 | 33 | 33,7 | 65,3 |
| Agree | 1 | 26 | 25,2 | 25,7 | 91,1 |
| Very strongly agree | 2 | 9 | 8,7 | 8,9 | 100 |
| | Total | 101 | | 100 | |

Valid cases 101 Missing cases 2

## B.7 The bank's directors are overpaid

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 3 | 2,9 | 2,9 | 2,9 |
| Disagree | -1 | 4 | 3,9 | 3,9 | 6,8 |
| Neither | 0 | 27 | 26,2 | 26,2 | 33 |
| Agree | 1 | 28 | 27,2 | 27,2 | 60,2 |
| Very strongly agree | 2 | 41 | 39,8 | 39,8 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## B.8 I feel secure in my job

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 19 | 18,4 | 18,6 | 18,6 |
| Disagree | -1 | 23 | 22,3 | 22,5 | 41,2 |
| Neither | 0 | 32 | 31,1 | 31,4 | 72,5 |
| Agree | 1 | 21 | 20,4 | 20,6 | 93,1 |
| Very strongly agree | 2 | 7 | 6,8 | 6,9 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

## B.9 The bank is poorly run

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 17 | 16,5 | 16,7 | 16,7 |
| Disagree | -1 | 16 | 15,5 | 15,7 | 32,4 |
| Neither | 0 | 35 | 34 | 34,3 | 66,7 |
| Agree | 1 | 23 | 22,3 | 22,5 | 89,2 |
| Very strongly agree | 2 | 11 | 10,7 | 10,8 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

## B.10 I am happy at work

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 10 | 9,7 | 10 | 10 |
| Disagree | -1 | 10 | 9,7 | 10 | 20 |
| Neither | 0 | 21 | 20,4 | 21 | 41 |
| Agree | 1 | 49 | 47,6 | 49 | 90 |
| Very strongly agree | 2 | 10 | 9,7 | 10 | 100 |
| | Total | 100 | | 100 | |

Valid cases 100 Missing cases 3

## B.11 I would "call in sick" to attend a job interview with another company

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 37 | 35,9 | 36,3 | 36,3 |
| Disagree | -1 | 20 | 19,4 | 19,6 | 55,9 |
| Neither | 0 | 20 | 19,4 | 19,6 | 75,5 |
| Agree | 1 | 20 | 19,4 | 19,6 | 95,1 |
| Very strongly agree | 2 | 5 | 4,9 | 4,9 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

## B.12 A bank clerk's role has changed from one of service to one of selling

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 3 | 2,9 | 2,9 | 2,9 |
| Disagree | -1 | 7 | 6,8 | 6,9 | 9,8 |
| Neither | 0 | 10 | 9,7 | 9,8 | 19,6 |
| Agree | 1 | 28 | 27,2 | 27,5 | 47,1 |
| Very strongly agree | 2 | 54 | 52,4 | 52,9 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

## B.13 I am only working here because of the poor state of the job market at present

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 43 | 41,7 | 42,2 | 42,2 |
| Disagree | -1 | 15 | 14,6 | 14,7 | 56,9 |
| Neither | 0 | 19 | 18,4 | 18,6 | 75,5 |
| Agree | 1 | 16 | 15,5 | 15,7 | 91,2 |
| Very strongly agree | 2 | 9 | 8,7 | 8,8 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

## B.14 If I knew then what I know now I would not have joined this bank.

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 29 | 28,2 | 28,4 | 28,4 |
| Disagree | -1 | 17 | 16,5 | 16,7 | 45,1 |
| Neither | 0 | 29 | 28,2 | 28,4 | 73,5 |
| Agree | 1 | 13 | 12,6 | 12,7 | 86,3 |
| Very strongly agree | 2 | 14 | 13,6 | 13,7 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

Number of Valid Observations (Listwise) = 97.00

| Variable | Mean | StdDev | Min | Max | N | Label |
|---|---|---|---|---|---|---|
| B.1 | .49 | 1.05 | -2.0 | 2.0 | 103 | I get a lot from my |
| B.2 | .43 | 1.13 | -2.0 | 2.0 | 103 | My abilities are und |
| B.3 | -.08 | 1.02 | -2.0 | 2.0 | 101 | Others are paid more |
| B.4 | -.18 | 1.39 | -2.0 | 2.0 | 101 | I would leave if I c |
| B.5 | -.47 | 1.04 | -2.0 | 2.0 | 102 | The bank is well run |
| B.6 | -.05 | 1.20 | -2.0 | 2.0 | 101 | My work makes me ten |
| B.7 | .97 | 1.04 | -2.0 | 2.0 | 103 | The bank's directors |
| B.8 | -.25 | 1.18 | -2.0 | 2.0 | 102 | I feel secure in my |
| B.9 | -.05 | 1.22 | -2.0 | 2.0 | 102 | The bank is poorly r |
| B.10 | .39 | 1.12 | -2.0 | 2.0 | 100 | I am happy at work |
| B.11 | -.63 | 1.29 | -2.0 | 2.0 | 102 | I would "call in sic |
| B.12 | 1.21 | 1.07 | -2.0 | 2.0 | 102 | A bank clerk's role |
| B.13 | -.66 | 1.39 | -2.0 | 2.0 | 102 | I am only working he |
| B.14 | -.33 | 1.37 | -2.0 | 2.0 | 102 | If I knew then what |

---

# Personal Details:

## C.1 Gender

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Female | 1 | 63 | 61,2 | 61,2 | 61,2 |
| Male | 2 | 40 | 38,8 | 38,8 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## C.2 Age

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| 16 - 21 | 1 | 15 | 14,6 | 14,6 | 14,6 |
| 22 - 29 | 2 | 37 | 35,9 | 35,9 | 50,5 |
| 30 - 39 | 3 | 25 | 24,3 | 24,3 | 74,8 |
| 40 - 49 | 4 | 23 | 22,3 | 22,3 | 97,1 |
| 50 - 59 | 5 | 3 | 2,9 | 2,9 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## C.3 Marital status

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Single | 1 | 33 | 32 | 32 | 32 |
| With long term partner | 2 | 63 | 61,2 | 61,2 | 93,2 |
| Other | 3 | 7 | 6,8 | 6,8 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## C.4 Qualifications

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| No formal qualifica | 1 | 4 | 3,9 | 3,9 | 3,9 |
| O levels/GCSEs/CSEs | 2 | 36 | 35 | 35,3 | 39,2 |
| A levels | 3 | 21 | 20,4 | 20,6 | 59,8 |
| BTec | 4 | 5 | 4,9 | 4,9 | 64,7 |
| Diploma/certificate | 5 | 7 | 6,8 | 6,9 | 71,6 |
| Degree | 6 | 2 | 1,9 | 2 | 73,5 |
| Banking certificate | 7 | 4 | 3,9 | 3,9 | 77,5 |
| ACIB | 8 | 22 | 21,4 | 21,6 | 99 |
| Other | 10 | 1 | 1 | 1 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

## D.1 Area of work

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Accounts department | 1 | 16 | 15,5 | 15,5 | 15,5 |
| Cash Tills | 2 | 14 | 136,6 | 13,6 | 29,1 |
| Enquiries/customer service | 3 | 15 | 14,6 | 14,6 | 43,7 |
| Foreign desk | 4 | 1 | 1 | 1 | 44,7 |
| Loans department | 5 | 18 | 17,5 | 17,5 | 62,1 |
| Securities department | 6 | 6 | 5,8 | 5,8 | 68 |
| Management | 7 | 21 | 20,4 | 20,4 | 88,3 |
| Computer department | 8 | 2 | 1,9 | 1,9 | 90,3 |
| Other | 9 | 4 | 3,9 | 3,9 | 94,2 |
| Secretarial | 10 | 4 | 3,9 | 3,9 | 98,1 |
| Costings/charges | 11 | 1 | 1 | 1 | 99 |
| Sales | 12 | 1 | 1 | 1 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## D.2 Time with current bank

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Less than 1 year | 1 | 2 | 1,9 | 1,9 | 1,9 |
| 1 - 2 years | 2 | 4 | 3,9 | 3,9 | 5,8 |
| 2 - 5 years | 3 | 23 | 22,3 | 22,3 | 28,2 |
| 5 - 10 years | 4 | 26 | 25,2 | 25,2 | 53,4 |
| More than 10 years | 5 | 48 | 46,6 | 46,6 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## D.3 Time in current branch

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Less than 1 year | 1 | 18 | 17,5 | 17,8 | 17,8 |
| 1 - 2 years | 2 | 24 | 23,3 | 23,8 | 41,6 |
| 2 - 5 years | 3 | 38 | 36,9 | 37,6 | 79,2 |
| 5 - 10 years | 4 | 13 | 12,6 | 12,9 | 92,1 |
| More than 10 years | 5 | 8 | 7,8 | 7,9 | 100 |
| | Total | 101 | | 100 | |

Valid cases 101 Missing cases 2

## D.4 Pay range

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Less than £10,000 | 1 | 29 | 28,2 | 28,4 | 28,4 |
| £10 - 15,000 | 2 | 45 | 43,7 | 44,1 | 72,5 |
| £15 - 20,000 | 3 | 11 | 10,7 | 10,8 | 83,3 |
| £20 - 25,000 | 4 | 6 | 5,8 | 5,9 | 89,2 |
| More than £25,000 | 5 | 11 | 10,7 | 10,8 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

## D.5 Full time or part time

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Full-time | 1 | 96 | 93,2 | 94,1 | 94,1 |
| Part-time | 2 | 6 | 5,8 | 5,9 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

## Question:

*The use of computers has increased over the last two decades. What are your views of them in general and on their use in banking in particular? Please indicate whether you agree with the following statements:*

## E.1 I have had much experience of computers and their possible applications

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 15 | 14,6 | 14,6 | 14,6 |
| Disagree | -1 | 15 | 14,6 | 14,6 | 29,1 |
| Neither | 0 | 29 | 28,2 | 28,2 | 57,3 |
| Agree | 1 | 29 | 28,2 | 28,2 | 85,4 |
| Very strongly agree | 2 | 15 | 14,6 | 14,6 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## E.2 Viruses are a major threat to computer users

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 3 | 2,9 | 2,9 | 2,9 |
| Disagree | -1 | 7 | 6,8 | 6,8 | 9,7 |
| Neither | 0 | 59 | 57,3 | 57,3 | 67 |
| Agree | 1 | 22 | 21,4 | 21,4 | 88,3 |
| Very strongly agree | 2 | 12 | 11,7 | 11,7 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## E.3 Hackers are a major threat to computer users

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 3 | 2,9 | 2,9 | 2,9 |
| Disagree | -1 | 8 | 7,8 | 7,8 | 10,8 |
| Neither | 0 | 47 | 45,6 | 46,1 | 56,9 |
| Agree | 1 | 26 | 25,2 | 25,5 | 82,4 |
| Very strongly agree | 2 | 18 | 17,5 | 17,6 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

## E.4 If a colleague used unauthorised software or hardware they should be dismissed

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 1 | 1 | 1 | 1 |
| Disagree | -1 | 10 | 9,7 | 9,8 | 10,8 |
| Neither | 0 | 47 | 45,6 | 46,1 | 56,9 |
| Agree | 1 | 23 | 22,3 | 22,5 | 79,4 |
| Very strongly agree | 2 | 21 | 20,4 | 20,6 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

## E.5 I would "turn a blind eye" if colleague amended their credit card limit using a branch terminal

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 61 | 59,2 | 59,8 | 59,8 |
| Disagree | -1 | 20 | 19,4 | 19,6 | 79,4 |
| Neither | 0 | 11 | 10,7 | 10,8 | 90,2 |
| Agree | 1 | 5 | 4,9 | 4,9 | 95,1 |
| Very strongly agree | 2 | 5 | 4,9 | 4,9 | 100 |
| | Total | 102 | | 100 | |

Valid cases 102 Missing cases 1

## E.6 I have a good understanding of computers

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 13 | 12,6 | 12,6 | 12,6 |
| Disagree | -1 | 19 | 18,4 | 18,4 | 31,1 |
| Neither | 0 | 40 | 38,8 | 38,8 | 69,9 |
| Agree | 1 | 21 | 20,4 | 20,4 | 90,3 |
| Very strongly agree | 2 | 10 | 9,7 | 9,7 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## E.7 I would alter the balance of my account if I knew that I would not get caught

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 82 | 79,6 | 81,2 | 81,2 |
| Disagree | -1 | 7 | 6,8 | 6,9 | 88,1 |
| Neither | 0 | 8 | 7,8 | 7,9 | 96 |
| Agree | 1 | 2 | 1,9 | 2 | 98 |
| Very strongly agree | 2 | 2 | 1,9 | 2 | 100 |
| | Total | 101 | | 100 | |

Valid cases 101 Missing cases 2

## E.8 Bank clerks are in general honest

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 1 | 1 | 1 | 1 |
| Disagree | -1 | 1 | 1 | 1 | 1,9 |
| Neither | 0 | 7 | 6,8 | 6,8 | 8,7 |
| Agree | 1 | 37 | 35,9 | 35,9 | 44,7 |
| Very strongly agree | 2 | 57 | 55,3 | 55,3 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## E.9 Computers bank my job easier

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 0 | 0 | 0 | 0 |
| Disagree | -1 | 4 | 3,9 | 3,9 | 3,9 |
| Neither | 0 | 8 | 7,8 | 7,8 | 11,7 |
| Agree | 1 | 37 | 35,9 | 35,9 | 47,6 |
| Very strongly agree | 2 | 54 | 52,4 | 52,4 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## E.10 I enjoy using computers

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 4 | 3,9 | 3,9 | 3,9 |
| Disagree | -1 | 6 | 5,8 | 5,8 | 9,7 |
| Neither | 0 | 21 | 20,4 | 20,4 | 30,1 |
| Agree | 1 | 40 | 38,8 | 38,8 | 68,9 |
| Very strongly agree | 2 | 32 | 31,1 | 31,1 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## E.11 I have acquired good understanding of computers from bank training courses

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 25 | 24,3 | 24,3 | 24,3 |
| Disagree | -1 | 22 | 21,4 | 21,4 | 45,6 |
| Neither | 0 | 32 | 31,1 | 31,1 | 76,7 |
| Agree | 1 | 17 | 16,5 | 16,5 | 93,2 |
| Very strongly agree | 2 | 7 | 6,8 | 6,8 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## E.12 I have a poor understanding of the computer system that the bank uses

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Very strongly disagree | -2 | 24 | 23,3 | 23,3 | 23,3 |
| Disagree | -1 | 28 | 27,2 | 27,2 | 50,5 |
| Neither | 0 | 27 | 26,2 | 26,2 | 76,7 |
| Agree | 1 | 14 | 13,6 | 13,6 | 90,3 |
| Very strongly agree | 2 | 10 | 9,7 | 9,7 | 100 |
| | Total | 103 | | 100 | |

Valid cases 103 Missing cases 0

## E.13 Do you write computer programs?

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| No | 0 | 100 | 97,1 | 99 | 99 |
| Yes | 1 | 1 | 1 | 1 | 100 |
| | Total | 101 | | | |

Valid cases 101 Missing cases 2

## E.14 Do you have a modem?

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| No | 0 | 88 | 85,4 | 87,1 | 87,1 |
| Yes | 1 | 13 | 12,6 | 12,9 | 100 |
| | Total | 101 | | | |

Valid cases 101 Missing cases 2

Number of Valid Observations (Listwise) = 100.00

| Variable | Mean | Std Dev | Min | Max | N | Label |
|---|---|---|---|---|---|---|
| E.1 | .14 | 1.26 | -2.0 | 2.0 | 103 | I have had much expe |
| E.2 | .32 | .88 | -2.0 | 2.0 | 103 | Viruses are a major |
| E.3 | .47 | .97 | -2.0 | 2.0 | 102 | Hackers are a major |
| E.4 | .52 | .96 | -2.0 | 2.0 | 102 | If a colleague used |
| E.5 | -1.25 | 1.14 | -2.0 | 2.0 | 102 | I would "turn a blin |
| E.6 | -.04 | 1.14 | -2.0 | 2.0 | 103 | I have a good unders |
| E.7 | -1.63 | .87 | -2.0 | 2.0 | 101 | I would alter the ba |
| E.8 | 1.44 | .75 | -2.0 | 2.0 | 103 | Bank clerks are in g |
| E.9 | 1.37 | .79 | -1.0 | 2.0 | 103 | Computers bank my jo |
| E.10 | .87 | 1.04 | -2.0 | 2.0 | 103 | I enjoy using comput |
| E.11 | -.40 | 1.22 | -2.0 | 2.0 | 103 | Have acquired good u |
| E.12 | -.41 | 1.26 | -2.0 | 2.0 | 103 | I have a poor unders |
| E.13 | .01 | .10 | .0 | 1.0 | 101 | Do you write compute |
| E.14 | .13 | .34 | .0 | 1.0 | 101 | Do you have a modem? |

Question:

## H.1 Have you ever committed a crime?

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| No | 0 | 65 | 63,1 | 65 | 65 |
| Yes | 1 | 35 | 34 | 35 | 100 |
| | Total | 100 | | 100 | |

Valid cases 100 Missing cases 3

*If yes please tick those categories that apply:*

## H.1A Substance abuse

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| No | 0 | 93 | 90,3 | 93 | 93 |
| Yes | 1 | 7 | 6,8 | 7 | 100 |
| | Total | 100 | | 100 | |

Valid cases 100 Missing cases 3

## H.1B Shoplifting

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| No | 0 | 96 | 93,2 | 96 | 96 |
| Yes | 1 | 4 | 3,9 | 4 | 100 |
| | Total | 100 | | 100 | |

Valid cases 100 Missing cases 3

## H.1C General theft

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| No | 0 | 97 | 94,2 | 97 | 97 |
| Yes | 1 | 3 | 2,9 | 3 | 100 |
| | Total | 100 | | 100 | |

Valid cases 100 Missing cases 3

## H.1D Pilfering at work

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| No | 0 | 92 | 89,3 | 92 | 92 |
| Yes | 1 | 8 | 7,8 | 8 | 100 |
| | Total | 100 | | 100 | |

Valid cases 100 Missing cases 3

## H.1E Traffic offence

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| No | 0 | 68 | 66 | 68 | 68 |
| Yes | 1 | 32 | 31,1 | 32 | 100 |
| | Total | 100 | | 100 | |

Valid cases 100 Missing cases 3

## H.1F Other offence

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| No | 0 | 99 | 96,1 | 99 | 99 |
| Yes | 1 | 1 | 1 | 1 | 100 |
| | Total | 100 | | 100 | |

Valid cases 100 Missing cases 3

## H.2 Have you ever considered taking funds, or other assets, from your employer?

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| No | 0 | 98 | 95,1 | 98 | 98 |
| Yes | 1 | 2 | 1,9 | 2 | 100 |
| | Total | 100 | | 100 | |

Valid cases 100 Missing cases 3

## Question:

*It is acknowledge that the chances of your committing a crime against your employer are slim, but if you did what do you think would be most likely to motivate you? Please rank each of the following for their relative strength (5 being the strongest motivator, 1 the weakest):*

*If a friend or member of your family needed money*
*Revenge*
*Peer pressure*
*Boredom*
*If you needed the money*

## H.3A If a friend or member of family needed money

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Weakest motivator | 1 | 4 | 3,9 | 5,9 | 5,9 |
| | 2 | 6 | 5,8 | 8,8 | 14,7 |
| | 3 | 9 | 8,7 | 13,2 | 27,9 |
| | 4 | 22 | 21,4 | 32,4 | 60,3 |
| Strongest motivator | 5 | 27 | 26,2 | 39,7 | 100 |
| | Total | 68 | | | |

Valid cases 68 Missing cases 35

## H.3B Revenge

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Weakest motivator | 1 | 11 | 10,7 | 16,2 | 16,2 |
| | 2 | 12 | 11,7 | 17,6 | 33,8 |
| | 3 | 32 | 31,1 | 47,1 | 80,9 |
| | 4 | 5 | 4,9 | 7,4 | 88,2 |
| Strongest motivator | 5 | 8 | 7,8 | 11,8 | 100 |
| | Total | 68 | | 100 | |

Valid cases 68 Missing cases 35

## H.3C Peer pressure

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Weakest motivator | 1 | 19 | 18,4 | 27,9 | 27,9 |
| | 2 | 21 | 20,4 | 30,9 | 58,8 |
| | 3 | 17 | 16,5 | 25 | 83,8 |
| | 4 | 9 | 8,7 | 13,2 | 97,1 |
| Strongest motivator | 5 | 2 | 1,9 | 2,9 | 100 |
| | Total | 68 | | 100 | |

Valid cases 68 Missing cases 35

## H.3D Boredom

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Weakest motivator | 1 | 53 | 51,5 | 77,9 | 77,9 |
| | 2 | 9 | 8,7 | 13,2 | 91,2 |
| | 3 | 0 | 0 | 0 | 91,2 |
| | 4 | 3 | 2,9 | 4,4 | 95,6 |
| Strongest motivator | 5 | 3 | 2,9 | 4,4 | 100 |
| | Total | 68 | | 100 | |

Valid cases 68 Missing cases 35

## H.3E If you needed the money

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Weakest motivator | 1 | 10 | 9,7 | 14,7 | 14,7 |
| | 2 | 7 | 6,8 | 10,3 | 25 |
| | 3 | 4 | 3,9 | 5,9 | 30,9 |
| | 4 | 19 | 18,4 | 27,9 | 58,8 |
| Strongest motivator | 5 | 28 | 27,2 | 41,2 | 100 |
| | Total | 68 | | 100 | |

Valid cases 68 Missing cases 35

## Question:

*Please rank the following for their importance (9 being the most important and 1 being the least) in preventing you from acting criminally:*

*The belief that such behaviour is immoral*
*The knowledge that such behaviour is illegal*
*Security measures*
*Procedures*
*Fear of being caught*
*Fear of prison*
*What my family would think*
*What my friends would think*
*What my peers would think*

## H.4A The belief that such behaviour is immoral

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Least important | 1 | 8 | 7,8 | 8,1 | 8,1 |
| | 2 | 3 | 2,9 | 3 | 11,1 |
| | 3 | 5 | 4,9 | 5,1 | 16,2 |
| | 4 | 2 | 1,9 | 2 | 18,2 |
| | 5 | 10 | 9,7 | 10,1 | 28,3 |
| | 6 | 6 | 5,8 | 6,1 | 34,3 |
| | 7 | 3 | 2,9 | 3 | 37,4 |
| | 8 | 16 | 15,5 | 16,2 | 53,5 |
| Most important | 9 | 46 | 44,7 | 46,5 | 100 |
| | Total | 99 | | 100 | |

Valid cases 99 Missing cases 4

## H.4B The knowledge that such behaviour is illegal

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Least important | 1 | 2 | 1,9 | 2 | 2 |
| | 2 | 7 | 6,8 | 7,1 | 9,2 |
| | 3 | 1 | 1 | 1 | 10,2 |
| | 4 | 6 | 5,8 | 6,1 | 16,3 |
| | 5 | 7 | 6,8 | 7,1 | 23,5 |
| | 6 | 7 | 6,8 | 7,1 | 30,6 |
| | 7 | 8 | 7,8 | 8,2 | 38,8 |
| | 8 | 28 | 27,2 | 28,6 | 67,3 |
| Most important | 9 | 32 | 31,1 | 32,7 | 100 |
| | Total | 98 | | 100 | |

| | | | |
|---|---|---|---|
| Valid cases | 98 | Missing cases | 5 |

## H.4C Security measures

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Least important | 1 | 15 | 14,6 | 15,3 | 15,3 |
| | 2 | 22 | 21,4 | 22,4 | 37,8 |
| | 3 | 9 | 8,7 | 9,2 | 46,9 |
| | 4 | 15 | 14,6 | 15,3 | 62,2 |
| | 5 | 11 | 10,7 | 11,2 | 73,5 |
| | 6 | 9 | 8,7 | 9,2 | 82,7 |
| | 7 | 6 | 5,8 | 6,1 | 88,8 |
| | 8 | 8 | 7,8 | 8,2 | 96,9 |
| Most important | 9 | 3 | 2,9 | 3,1 | 100 |
| | Total | 98 | | 100 | |

Valid cases 98 Missing cases 5

## H.4D Procedures

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Least important | 1 | 31 | 30,1 | 31,6 | 31,6 |
| | 2 | 17 | 16,5 | 17,3 | 49 |
| | 3 | 15 | 14,6 | 15,3 | 64,3 |
| | 4 | 5 | 4,9 | 5,1 | 69,4 |
| | 5 | 14 | 13,6 | 14,3 | 83,7 |
| | 6 | 5 | 4,9 | 5,1 | 88,8 |
| | 7 | 4 | 3,9 | 4,1 | 92,9 |
| | 8 | 2 | 1,9 | 2 | 94,9 |
| Most important | 9 | 5 | 4,9 | 5,1 | 100 |
| | Total | 98 | | 100 | |

Valid cases 98 Missing cases 5

## H.4E Fear of being caught

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Least important | 1 | 6 | 5,8 | 6,1 | 6,1 |
| | 2 | 8 | 7,8 | 8,2 | 14,3 |
| | 3 | 8 | 7,8 | 8,2 | 22,4 |
| | 4 | 13 | 12,6 | 13,3 | 35,7 |
| | 5 | 8 | 7,8 | 8,2 | 43,9 |
| | 6 | 6 | 5,8 | 6,1 | 50 |
| | 7 | 17 | 16,5 | 17,3 | 67,3 |
| | 8 | 9 | 8,7 | 9,2 | 76,5 |
| Most important | 9 | 23 | 22,3 | 23,5 | 100 |
| | Total | 98 | | 100 | |

Valid cases 98 Missing cases 5

## H.4F Fear of prison

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Least important | 1 | 16 | 15,5 | 16,3 | 16,3 |
| | 2 | 2 | 1,6 | 2 | 18,4 |
| | 3 | 17 | 16,5 | 17,3 | 35,7 |
| | 4 | 8 | 7,8 | 8,2 | 43,9 |
| | 5 | 6 | 5,8 | 6,1 | 50 |
| | 6 | 10 | 9,7 | 10,2 | 60,2 |
| | 7 | 11 | 10,7 | 11,2 | 71,4 |
| | 8 | 11 | 10,7 | 11,2 | 82,7 |
| Most important | 9 | 17 | 16,5 | 17,3 | 100 |
| | Total | 98 | | 100 | |

Valid cases 98 Missing cases 5

## H.4G What my family would think

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Least important | 1 | 3 | 2,9 | 3,1 | 3,1 |
| | 2 | 1 | 1 | 1 | 4,1 |
| | 3 | 12 | 11,7 | 12,2 | 16,3 |
| | 4 | 6 | 5,8 | 6,1 | 22,4 |
| | 5 | 11 | 10,7 | 11,2 | 33,7 |
| | 6 | 5 | 4,9 | 5,1 | 38,8 |
| | 7 | 31 | 30,1 | 31,6 | 70,4 |
| | 8 | 12 | 11,7 | 12,2 | 82,7 |
| Most important | 9 | 17 | 16,5 | 17,3 | 100 |
| | Total | 98 | | 100 | |

Valid cases 98 Missing cases 5

## H.4H What my friends would think

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Least important | 1 | 7 | 6,8 | 7,1 | 7,1 |
| | 2 | 15 | 14,6 | 15,3 | 22,4 |
| | 3 | 5 | 4,9 | 5,1 | 27,6 |
| | 4 | 13 | 12,6 | 13,3 | 40,8 |
| | 5 | 9 | 8,7 | 9,2 | 50 |
| | 6 | 27 | 26,2 | 27,6 | 77,6 |
| | 7 | 6 | 5,8 | 6,1 | 83,7 |
| | 8 | 4 | 3,9 | 4,1 | 87,8 |
| Most important | 9 | 12 | 11,7 | 12,2 | 100 |
| | Total | 98 | | 100 | |

Valid cases 98 Missing cases 5

## H.4I What my peers would think

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Least important | 1 | 20 | 19,4 | 20,4 | 20,4 |
| | 2 | 7 | 6,8 | 7,1 | 27,6 |
| | 3 | 10 | 9,7 | 10,2 | 37,8 |
| | 4 | 10 | 9,7 | 10,2 | 37,8 |
| | 5 | 28 | 27,2 | 28,6 | 76,5 |
| | 6 | 9 | 8,7 | 9,2 | 85,7 |
| | 7 | 1 | 1 | 1 | 86,7 |
| | 8 | 1 | 1 | 1 | 87,8 |
| Most important | 9 | 12 | 11,7 | 12,2 | 100 |
| | Total | 98 | | 100 | |

Valid cases 98 Missing cases 5

## H.5 Starsign

| Value label | Value | Frequency | Percent | Valid Percent | Cum Percent |
|---|---|---|---|---|---|
| Aries | 1 | 8 | 7,8 | 9,1 | 9,1 |
| Taurus | 2 | 10 | 9,7 | 11,4 | 20,5 |
| Gemini | 3 | 6 | 5,8 | 6,8 | 27,3 |
| Cancer | 4 | 12 | 11,7 | 13,6 | 40,9 |
| Leo | 5 | 5 | 4,9 | 5,7 | 46,6 |
| Virgo | 6 | 10 | 6,7 | 11,4 | 58 |
| Libra | 7 | 8 | 7,8 | 9,1 | 67 |
| Scorpio | 8 | 8 | 7,8 | 9,1 | 76,1 |
| Sagittarius | 9 | 3 | 2,9 | 3,4 | 79,5 |
| Capricorn | 10 | 4 | 3,9 | 4,5 | 84,1 |
| Aquarius | 11 | 6 | 5,8 | 6,8 | 90,9 |
| Pisces | 12 | 8 | 7,8 | 9,1 | 100 |
| | Total | 88 | | 100 | |

Valid cases 88 Missing cases 15

## a selection of answers to the question "What do you think prevents you or your colleagues from behaving in a criminal way?"

*"It is morally wrong, creating guilt and feeling of worthlessness, I could not look my children in the eye if I was thieving (and endeavouring to bring them up to be honest)."*

*"The way we were brought up by parents, etc."*

*"We have morals, and I could not live with the guilt."*

*"No inclination, have been brought up to respect the law."*

*"Self respect and knowing my employer has great trust in me."*

*"Morals, Honesty, Trust."*

*"As we work so tightly as a team, the fear of letting yourself, your colleagues and the society down would be too great. Also the fear of dismissal and the personal shame would personally prevent me, together with the guilt!"*

*"Trust and respect for each other."*

*"Job security and being able to rely on your staff, honesty is very important."*

*"A lot depends on your background, the way parents have brought you up."*

*"It would not even occur to them. I have complete trust in everyone I work with and believe it is vice versa."*

*"Being trusted by colleagues."*

*"Being in a trusted position."*

*"Early parental influence*
*settled now into a strong family relationship*
*setting the right example to my children."*

*"Immoral, we're in a position of trust, both from bank and customers' point of view. The disgrace if caught."*

*"A sense of right and wrong."*

*"Understanding the difference between right and wrong."*

*"Fear of prison."*

*"Good upbringing by honest hardworking parents."*

*"Threat of dismissal."*

*"Financial positions."*

*"Because, in general, bank staff are honest."*

*"Morally unacceptable and there is no need to act in a criminal way. Natural sense of right and wrong. Upbringing. Anti-social."*

*"Attitude of mind. Upbringing as a child. Education."*

*"Respect for bank and customers."*

*"Being brought up correctly - being a criminal is wrong. Humiliation if you were to be caught. Fear of losing a secure, well paid job."*

*"Immoral - I know how I would feel if someone acted in a criminal way towards my family or I."*

*"basic honesty relating to choice of employment."*

*"The type of trust that people place in you when you handle their money each day."*

*"Loyalty; trust; honesty; upbringing; I want to keep my job and provide a future for myself, my wife and children. I have, unfortunately, seen people who could not resist temptation! They were caught!"*

*"We do not consider the personal value of the transactions we deal with, they are only pieces of paper and numbers."*

*"We need our jobs but at the same time feel short changed by the bank which could lead to some marginal decisions by staff re pilfering, availing ourselves of facilities, ie photocopying, etc."*

*"Because people trust you in dealing with all aspects of their finances."*

*"Its morally wrong to steal, I think that most of us would not be able to live with ourselves or the guilt. Its not how we're brought up."*

*"Personal standards."*

*"Being trusted."*

*"Not the sort of people we are."*

*"Honesty and moral duty when dealing with other people's money."*

*"The thought of losing a job and hurting others. Also most people are generally honest with a good character."*

*"Moral values taught as a child."*

*"Fear of consequences Vs level of benefits attainable."*

*"General disgrace of being caught."*

*"The majority of people working for the bank are honest and have an understanding of what is right and what is wrong which would prevent them even contemplating the behaviour."*

*"Resultant problems when caught."*

*"The degree of moral upbringing that one receives as a child and the relationship with one's family. If someone has a good self-image they are also less likely to commit crimes."*

*"Basic honesty and fear of being discovered and paying the price. Presumably staff are selected and vetted before being hired."*

*"Too much respect for what would happen if we did and also it's not in my own nature to do so."*

*"The loss of a job and a criminal record which would make it impossible to get another job."*

*"It's not the way that I was taught to behave by my parents. I know what is wrong."*

*"The fact that we are honest people."*

*"I am just not the sort of person to act in a criminal way."*

*"Honesty or fear of 'the sack'."*

*"Good upbringing - understanding the difference between right and wrong. The prospect of being rogered in prison!"*

*"Personal conscience and ethics. Christian principles."*

1. Robert Maxwell's misues of pension funds
2. The theft of an unlocked bicycle/ theft of £100 from the till
3. A loans officer takes out loans in a false name
4. A junior clerk makes phone calls to a boyfriend in Australia. The total cost of the calls increases the branch's telephone bill by over £100 a month
5. A clerk who is on self certified sick leave spends the day writing a computer programme to help a local charity manage its books
6. A clerk manages to access the computer system and instructs it to pay one penny of interest due to all the bank's customers' deposit accounts to his account instead
7. A bank manager and a junior clerk act together to transfer £1,000,000 via CHAPS and then SWIFT to an account they have opened in South America
8. The Barlow Clowes Affair - the senior official of an investment firm defrauds many millions of pounds
9. A clerk is using a computer at work to write a number of computer programmes for his own personal use
10. A manager transfers £100,000 from a branch sundry account to a large corporate customer's account the day before he must report to his senior manager about the borrowing position of said client, the transfer takes the client below their overdraft limit. The following day he transfers the money back and has the statements retyped
11. Three women attack and mug a man on his way home late at night
12. A clerk takes a box of envelopes home
13. A clerk rings his mother every day. The cost of these phone calls adds £15 to the branch's monthly phone bill
14. A computer operator at the foreign department delays payments to branch customers holding the money on a deposit account for a day so that he earns interest on the money at the customers' expense
15. A clerk uses a word processor at work to prepare her CV
16. A clerk increases her credit card limit without authority. She needs the money to pay a gambling debt
17. A clerk uses the photocopier to make 100 copies of his CV
18. A clerk uses a terminal at his branch to place money on deposit over night in London in the name of a large corporate customer. He completes all necessary procedures but removes the entries before they can be processed and the customer debited. When the branch receives the interest payment from their head office three days later he makes appropriate entries to credit his account with the £4,000 interest earned
19. A clerk telephones his girlfriend to tell her he is working late. The call costs the bank £1.47
20. A clerk uses a terminal to increase his overdraft limit without authorisation. He needs the money to pay the rent
21. A man is shot by a terrorist on a train. The terrorists escapes by jumping from the moving train

| Table 1: Ranking of cases from *acceptable* 1 to *unacceptable* 20. | Main | Pilot |
|---|---|---|
| A clerk telephones his girlfriend to tell her he is working late. The call costs the bank £1.47 | 1 | 1 |
| A clerk uses a word processor at work to prepare her CV | 2 | 2 |
| A clerk who is on self certified sick leave spends the day writing a computer programme to help a local charity manage its books | 3 | 3 |
| A clerk uses the photocopier to make 100 copies of his CV | 4 | 4 |
| A clerk rings his mother everyday. The cost of these phone calls adds £15 to the branch's monthly phone bill | 5 | 5 |
| A clerk takes a box of envelopes home | 6 | 6 |
| A clerk is using a computer at work to write a number of computer programmes for his own personal use | 7 | 7 |
| A junior clerk makes phone calls to a boyfriend in Australia. The total cost of the calls increases the branch's telephone bill by over £100 a month | 8 | 8 |
| A clerk uses a terminal to increase his overdraft limit without authorisation. He needs the money to pay the rent | 9 | 9 |
| A computer operator at the foreign department delays payments to branch customers holding the money on a deposit account for a day so that he earns interest on the money at the customers' expense | 10 | 12 |
| A clerk increases her credit card limit without authority. She needs the money to pay a gambling debt | 11 | 10 |
| A clerk manages to access the computer system and instructs it to pay one penny of interest due to all the bank's customers' deposit accounts to his account instead | 12 | 13 |
| A manager transfers £100,000 from a branch sundry account to a large corporate customer's account the day before he must report to his senior manager about the borrowing position of said client, the transfer takes the client below their overdraft limit. The following day he transfers the money back and has the statements retyped | =13 | 14 |
| A loans officer takes out loans in a false name | =13 | 15 |
| A clerk uses a terminal at his branch to place money on deposit over night in London in the name of a large corporate customer. He completes all necessary procedures but removes the entries before they can be processed and the customer debited. When the branch receives the interest payment from their head office three days later he makes appropriate entries to credit his account with the £4,000 interest earned | 15 | 16 |
| Three women attack and mug a man on his way home late at night | 16 | 11 |
| A bank manager and a junior clerk act together to transfer £1,000,000 via CHAPS and then SWIFT to an account they have opened in South America | 17 | 17 |
| The Barlow Clowes Affair - the senior official of an investment firm defrauds many millions of pounds | 18 | 19 |
| Robert Maxwell's misuse of pension funds | 19 | 20 |
| A man is shot by a terrorist on a train. The terrorists escapes by jumping from the moving train | 20 | 18 |

*Ignores question 2 as this one differs between the pilot sample and the others*

| Table 2: Differences between Main sample and student sample. The scores given are the averages for the samples scores using magnitude scaling. | Student | Main |
|---|---|---|
| A clerk telephones his girlfriend to tell her he is working late. The call costs the bank £1.47 | 1,8 | 2,3 |
| A clerk uses a word processor at work to prepare her CV | 2,7 | 8,5 |
| A clerk who is on self certified sick leave spends the day writing a computer programme to help a local charity manage its books | 8,3 | 12,3 |
| A clerk uses the photocopier to make 100 copies of his CV | 10,7 | 25 |
| A clerk rings his mother everyday. The cost of these phone calls adds £15 to the branch's monthly phone bill | 14,5 | 28 |
| A clerk takes a box of envelopes home | 17 | 38 |
| A clerk is using a computer at work to write a number of computer programmes for his own personal use | 15 | 68 |
| A junior clerk makes phone calls to a boyfriend in Australia. The total cost of the calls increases the branch's telephone bill by over £100 a month | 66 | 78 |
| A clerk uses a terminal to increase his overdraft limit without authorisation. He needs the money to pay the rent | 53 | 170 |
| A computer operator at the foreign department delays payments to branch customers holding the money on a deposit account for a day so that he earns interest on the money at the customers' expense | 178 | 182 |
| A clerk increases her credit card limit without authority. She needs the money to pay a gambling debt | 93 | 186 |
| A clerk manages to access the computer system and instructs it to pay one penny of interest due to all the bank's customers' deposit accounts to his account instead | 174 | 224 |
| A manager transfers £100,000 from a branch sundry account to a large corporate customer's account the day before he must report to his senior manager about the borrowing position of said client, the transfer takes the client below their overdraft limit. The following day he transfers the money back and has the statements retyped | 214 | 257 |
| A loans officer takes out loans in a false name | 302 | 257 |
| A clerk uses a terminal at his branch to place money on deposit over night in London in the name of a large corporate customer. He completes all necessary procedures but removes the entries before they can be processed and the customer debited. When the branch receives the interest payment from their head office three days later he makes appropriate entries to credit his account with the £4,000 interest earned | 234 | 288 |
| Three women attack and mug a man on his way home late at night | 347 | 331 |
| A bank manager and a junior clerk act together to transfer £1,000,000 via CHAPS and then SWIFT to an account they have opened in South America | 813 | 398 |
| The Barlow Clowes Affair - the senior official of an investment firm defrauds many millions of pounds | 977 | 589 |
| Robert Maxwell's misuse of pension funds | 1.000 | 832 |
| A man is shot by a terrorist on a train. The terrorists escapes by jumping from the moving train | 2.089 | 851 |

*Ignores question 2 as this one differs between the pilot sample and the others*

*"The questions which are work related are more serious when you are in a position of trust and you or your staff abuse that trust. For example the loans officer fraud and the theft are serious and effect the society as well as the other individual s at that branch. The questions which are more thought provoking are those you can actually prevent from happening rather than the terrorist question for example." (Referring to the section dealing with the weighting of certain actions).*

*"Misuse of trust has been taken into account when scoring some of the questions. Crimes against people that are unable to fight back or are unaware of the crime, are not even to be compared to someone using their employer's telephone to advise a partner they will be working late."*

# general quotes

*"The bank is trying to place a sales culture unto all staff - although many of those staff fulfil an administrative role and have little access to customers for selling. Result - Demotivation."*

*"As a career in the bank becomes less likely and the systems are centralised, the opportunity and availability of fraud will become greater. Cost savings mean less work is double checked and supervisors have less time to fully monitor their staff. Junior staff are already adopting an attitude of 'I don't care', which I consider will increase."*

*"It is not just banking which has changed over the last 10 - 20 years."*

*"Amount of responsibility is never acknowledged whether verbally or in real terms, ie salary. Managers above branch level are slow to thank staff for a job well done, or extra work carried out, they expect it and take too much for granted."*

*"These areas will always be changing in importance. With the various 'early retirements' and 'voluntary severance" packages seen recently, job security and benefits come out higher than most."*

*"The Banking Culture has changed significantly, particularly in the last 6 years. New entrants in this time have not witnessed such large scale changes as those of us who have been working for a longer period. It really could be a case of adapt to survive."*

*"Standards of service have had to be improved as a direct result of media coverage and the customer now being able to 'challenge' their bank manager - service should always come before sales. The latter will not be achieved without the former."*

*"Banking has lost the 'job for life' and 'good career' image, people working within the banking network no longer feel that this is the case."*

*"Offences against people are worse than those involving money."*

*"I enjoy my job but the current situation in the world of finance has increased the pressure to 'hard sell' products which I disagree with ."*

*"Dishonesty is dishonesty."*

*"When I joined the bank in 1985 straight from school I had an image of what a banker was. It was a highly conservative image and effected the way I behaved. When I was not working I was aware that the people I met might be customers and therefore maintained that image. Things seemed to have changed a lot since then."*

# References.


**Adams J.S. (1963)**
"Towards an understanding of inequity" Journal of Abnormal Social Psychology Vol 67 pages 422-36

**Allen B. (1975)**
"Embezzler's guide to the computer" Harvard Business Review July-August, pages 79-89.

**Anderson R.J. (1994)**
"Why Cryptosystems Fail." Communications of the ACM November 1994, Vol. 37, No. 11, pp. 32-40.

**Arrow K (1974)**
The Limits of Organization W.W. Norton & Co., New York.

**Asch S.E. (1955)**
"Opinions and Social Pressure" in Frontiers of Psychological Research. Readings from Scientific American selected by Coopersmith S. (1964) W.H. Freeman & Co., San Francisco and London, pp107-111.

**Aubert V. (1952)**
"White-Collar Crime and Social Structure" American Journal of Sociology Vol 58 pages 263-71

**Audit Commission (1985)**
Computer Fraud Survey H.M.S.O., London.

**Audit Commission (1987)**
Survey of Computer Fraud and Abuse H.M.S.O., London.

**Audit Commission (1994)**
"Opportunity Makes a Thief: An Analysis of Computer Abuse" H.M.S.O., London

**Bankers Monthly** April 1989, page 42.

**Banking Act 1979**

**Bellow S. (1975)**
Humboldt's Gift, Secker & Warburg, London.

**Bhide A. & Stevenson H.H. (1990)**
"Why Be Honest if Honesty Doesn't Pay" Harvard Business Review September-October, pages 121-129.

**Bill on Computer Misuse (The Anti-Hacking Bill) 1989**
H.M.S.O., London.

**Bonini C.P. (1964)**
"Simulation of Organizational Behaviour" in Management Controls. New Directions in Basic Research **(Eds) Bonini, Jaedicke & Wagner**, McGraw Hill Book Co., New York, pp. 91-101.

**Box S.(1987)**
Recession, Crime and Punishment. MacMillan, London.

**Branscomb A.W. (1991)**
"Common Law for the Electronic Frontier: Networked Computing challenges the laws that govern information and ownership" Scientific American September, pages 112-116.

**Breed B. (1979)**
White Collar Bird John Clare Books, London.

**British Banking Association (1994)**
Annual Abstract of Banking Statistics Vol 11, Statistical Unit, British Banking Association, London.

**Buchan J (1992)**
"Too much interest on junk" The Spectator 25 January, pages 25-26.

**Budd L. & Whimster S. (Ed.)(1992)**
Global Finance and Urban Living: A Study of Metropolitan Change Routledge, London.

**Campbell A. & Muncer S. (1990)**
"Causes of Crime: Uncovering a Lay Model" Criminal Justice and Behavior Vol. 17, No. 4, pages 410-419.
**C.B.I. (1990)**
Crime - managing the business risk: A joint CBI/Crime Concern Working Group Report. Confederation of British Industry, London.
**C.B.I. (1991)**
Safeguard your systems: Management guidelines for information systems security. Confederation of British Industry, London.
**Clinard & Yeager (1982)**
Corporate Crime Free Press, New York
**Clough B. & Mungo P. (1992)**
Approaching Zero: Data Crime and The Computer Underworld Faber & Faber Ltd., London.
**Coldwell R.A. (1990)**
"Computer Cime: A Sociological Perspective" in Hughes G (ed) Essays on Computer Law Longmans, London, pp. 217-223.
**Coleman J.W. (1989)**
The Criminal Elite: The Sociology of White Collar Crime St. Martin's Press, New York.
**Collier P., Dixon R. & Marston C. (1991)**
"A Computer fraud Survey in the UK" OMEGA Vol. 19, No. 1, pp. 55-67.
**Comer M.J.(1985)**
Corporate Fraud McGraw Hill Book Company Ltd., London.
**Companies Act 1985**
H.M.S.O., London.
**Companies Act 1989**
H.M.S.O., London.
**Computer Misuse Act 1990**
H.M.S.O., London.
**Conklin (1977)**
Illegal but not Criminal: Business Crime in America Prentice Hall Inc., New Jersey.
**Criminal Damage Act 1971**
**Cringely R.X. (1992)**
Accidental Empires: How the boys of Silicon Valley make their millions, battle forreign competition, and still can't get a date Viking, London.
**Cressey P. & Scott P. (1992)**
"Employment, Technology and Industrial Relations in UK Clearing Banks" New Technology, Work and Employment, pp. 83-96
**The Daily Telegraph**
July 20, 1992
**Denning D.E. (1991)**
"A debate on Electronic Publishing, Constitutional Rights and Hacking" Communications of the ACM (Vol. 34, No. 3), pp. 23-43.
**Dewdney A.K. (1988)**
The Armchair Universe: An Exploration of Computer Worlds. W.H. Freeman & Co., New York.
**Ditton J. (1977)**
Part-Time Crime: An Ethnography of Fiddling and Pilferage The Macmillan Press Ltd., London.
**Doswell R. & Simons G.L. (1986)**
Fraud and Abuse of IT Systems N.C.C. Publications, Manchester.
**Downes D. & Rock P. (1988)**
Understanding Deviance Clarendon Press, Oxford.
**Elmer-Dewitt P. (1994)**
"Battle for the Internet" Time, July 25, pp. 34-40.

**The Economist**
"If it please yer 'onour" page 118, October 1 1988; "With a little help from NatWest's friends" page 79-80 January 7 1989; "Anatomy of a cover-up" page 84-86 January 28 1989; "The Blue Arrow Affair. The buck stops where?" page 23-26 March 7 1992.

**Ermann M.D. & Lundman R.J. (1982)**
Corporate Deviance Holt, Rinehart & Winston, New York.

**Euromoney (1990)**
"The Confessions of Ivan Boesky" July, pages 50-52.

**Eysenck H. (1977)**
Crime and Personality Routledge & Kegan Ltd, London.

**Figlio R.M. (1978)**
The National Survey of Crime Severity: Result of the Pretest Monograph, Department of Criminology, University of Pennsylvania.

**The Financial Times**
February 12, 15/16 and 18 1992

**Fishbein M. (1980)**
"A Theory of Reasoned Action: Some Applications and Implications" Nebraska Symposium on Motivation, 1979 University of Nebraska Press, Lincoln and London, pp. 65-110.

**Fishbein M. (1967)**
"A Consideration of Beliefs, and Their Role in Attitude Measurement." in Fishbein M. (Ed.). Readings in Attitude Theory and Measurement John Wiley & Sons, Inc. New York, pp 257-266.

**Fishbein M. (1967)**
"A Behavior Theory Approach to the Relations between Beliefs about an Object and the Attitude Toward the Object" in Fishbein M. (Ed.). Readings in Attitude Theory and Measurement John Wiley & Sons, Inc. New York, pp 389-400.

**Fishbein M. & Ajzen I. (1975)**
Belief, Attitude, Intention and Behaviour: An Introduction to Theory and research Addison-Wesley Ltd., London.

**Fishbein M. & Anderson L.R. (1965)**
"Prediction of Attitude from the Number, Strength, and Evaluative Aspects of Beliefs about the Attitude Object: A Comparison of Summation and Congruity Theories" Journal of Personality and Social Psychology, Vol. 2, pp 437-443.

**Fishbein M. & Raven B.H (1962)**
"The AB Scales: An Operational Definition of Belief and Attitude" Human Relations, Vol. 15, pp 35-44.

**Flory S.M., Phillips T.J., Reidenbach R.E., & Robin D.P. (1992)**
"A Multidimensional Analysis of Selected Ethical Issues in Accounting." The Accounting Review Vol. 67, No. 2, pages 284-302

**Forester T. (1987)**
High-Tech Society: The Story of the Information Technology Revolution Basil Blackwell Ltd., Oxford.

**Fraud Trials Committee (1986)**
Improving the Presentation of Information to Juries in Fraud Trials: A Report of Four Research Studies by the M.R.C. Applied Psychology Unit, Cambridge H.M.S.O., London.

**Friedrichs O. (1992)**
"White-Collar Crime and the Definitional Quagmire: A Provisional Solution" Journal of Human Justice Vol 3 No 2 Spring pages 5-21

**Ganesan R. & Sandhu R. (1994)**
"Securing Cyberspace. " Communications of the ACM November 1994, Vol. 37, No. 11, pp. 29-31.

**Geis G. & Meier R.F. (1977) - Eds.**
White-Collar Crime: Offenses in Business, Politics, and the Professions The Free Press, New York.

**Gellerman S.W. (1989)**
"Managing Ethics from the Top Down." Sloan Management Review Winter, Vol. 30, N° 2, pp 73-79.

**Gill C. (1985)**
Work, Unemployment and New Technology Polity Press, Cambridge.
**Gold & Schrifreen v. R. (1988)**
AC 1063.
**Greenburg J. (1990)**
"Employee Theft as a Reaction to Underpayment Inequity: The Hidden Cost of Pay Cuts" Journal of Applied Psychology Vol.75, No. 5, pages 561-568.
**Hadden T. (1983)**
"Fraud in the City: The Role of the Criminal Law." Criminal Law Review pages 500-511.
**Haffner K. & Markoff J. (1992)**
Cyberpunk: Outlaws and Hackers on the Computer Frontier Touchstone, New York
**Hall D.T. & Lawler E. E. (1977)**
"Job Pressures and Research Performance" in Current Trends in Psychology. Readings from American Scientist. Selected by **Janis I.L.** William Kaufman, Inc., Los Altos, California, pp 291-300.
**Handy C. (1985)**
Understanding Organizations, Third Edition, Penguin Business Library, London.
**Handy C. (1989)**
The Age of Unreason Business Books Ltd., London.
**Handy C. (1994)**
The Empty Raincoat: Making Sense of the Future Hutchinson, London.
**Handy C. (1995)**
Beyond Certainty: The Changing Worlds of Organizations Hutchinson, London.
**Handy C. (1995)**
"How do you manage people whom you do not see? Trust and the virtual organization." Harvard Business Review May-June, pp 40-50.
**Hayes J. (1990)**
"Employee Theft Is No. 1 Problem Facing Today's Busy Retailers" Discount Store News September 17.
**Hearnden K. (1986)**
"Computer Crime: Multi-million pound Problem?" Long Range Planning Vol. 19, No. 5, pages 18 to 26
**Henry S. (1978)**
The Hidden Economy: The context and control of Borderline crime Martin Robertson, London.
**Henry S. and Milovanavic D. (1991)**
"Constitutive Criminology: The Maturation of Critical Theory." Criminology Vol. 29, No. 2, pp. 293-316.
**Heron W. (1957)**
"The Pathology of Boredom" in Frontiers of Psychological Research. Readings from Scientific American selected by Coopersmith S. (1964) W.H. Freeman & Co., San Francisco and London, pp 82-86.
**Herzberg F. (1966)**
"The Motivation-Hygiene Theory" pages 86-90 in Management and Motivation edited by Vroom V.H. and Deci E.L. (1989) Penguin Business Publications.
**Herzberg F. (1968)**
"One more time: How do you motivate employees?" Harvard Business Review (January-February), pp. 53- 62.
**Hilton A. (1987)**
City within a State: A Portrait of Britain's Financial World I.B. Tauris & Co. Ltd., London.
**Høeg P. (1994)**
Miss Smilla's feeling for snow Flamingo, London.
**Homans G.C. (1961)**
Social Behaviour: Its Elementary Forms Harcourt Brace, New York.
**Home Office (1990)**
Criminal Statistics England and Wales 1989 H.M.S.O., London.

**Home Office (1992a)**
Criminal Statistics England and Wales 1990 H.M.S.O., London.
**Home Office (1992b)**
Prison Statistics England and Wales 1990 H.M.S.O., London.
**Hughes G. (Ed.) (1990)**
Essays on Computer Law Longman, Melbourne.
**Hunt J.W. (1986)**
Managing People at Work. McGraw-Hill, London.
**Huntington I.K. (1992)**
Fraud: Prevention and Detection Butterworths, London.
**The Independent**
February 28, 1995;
**Janis I.L. (1972)**
Victims of Group-Think, Houghton Mifflin, Boston.
**Janis I.L. & Mann L (1977)**
"Coping with Decisional Conflict" in Current Trends in Psychology. Readings from American Scientist. Selected by **Janis I.L.** William Kaufman, Inc., Los Altos, California, pp 306-316.
**Johnson G. (1992)**
"Managing Strategice Change - Strategy, Culture and Action" Long Range Planning, Vol. 25, No. 1, pp. 28 to 36
**Jones E.E. (1977)**
"How Do People Perceive the Causes of Behavior?" in Current Trends in Psychology. Readings from American Scientist. Selected by **Janis I.L.** William Kaufman, Inc., Los Altos, California, pp 317-322.
**Justice (1984)**
Fraud Trials Justice Educational and Research Trust, London.
**Katz R. (1978)**
"Job longevity as a situational factor in job satisfaction." Administrative Science Quarterly (No. 23), pp. 204-223.
**Kelley D. (1991)**
"Worker Participation and Economic Democracy: The Potential and the Limitation of Two Seperate Movements in Reducing Corporate and Occupational Crime" working draft presented at the Annual Meeting of the American Society of Criminology.
**Kinkead G. (1984)**
"Ivan Boesky, Money Machine" Fortune August 6, pages 102-104
**Kanter R.M. (1983)**
The Change Masters: Corporate Entrepreneurs at Work Allen & Unwin, London.
**Kanter R.M. (1989)**
When Giants Learn to Dance Simon & Schuster, London.
**Kramer R.C. (1982)**
"Corporate Crime: An Organizational Perspective" in Wickman P. & Daily T. (eds) White-Collar and Economic Crime pages 75-94, Lexington Books, Lexington, Mass.
**Kramer R.C. (1992)**
"The Space Shuttle Challenger Explosion: A Case Study of State-Corporate Crime" in Schlegel K. & Weisburd D. White-Collar Crime Reconsidered pages 241-243, Northeastern University Press, Boston.
**Krauss & MacGahan (1979)**
Computer Fraud and Countermeasures Prentice Hall.
**Law Commission (1988)**
Computer Misuse Working Paper No. 110 H.M.S.O., London.
**Law Commission (1987)**
Criminal Law Conspiracy to Defraud Working Paper No. 104. H.M.S.O., London.
**Leigh L.H. (1982)**
The Control of Commercial Fraud Heinemann, London.
**Levi M. (1981)**
The Phantom Capitalists: The Organisation and Control of Long-Firm Fraud Heinemann, London.

**Levi M. (1987)**
Regulating Fraud: White-Collar Crime and the Criminal Process Tavistock Publications, London and New York.
**Levin B. (1992)**
"A terminal case of Virus" The Times January 3, 1991.
**Levy S. (1994)**
Hackers: Heroes of the Computer Revolution. Penguin, London.
**Likert R. (1932)**
"A Technique for the Measurement of Attitudes" Arch. Psychol., Vol. 140, pp 1-55.
**Likert R. (1961)**
New Patterns of Management. McGraw-Hill, New York.
**Likert R. (1967)**
The Human Organization. McGraw-Hill, New York.
**Lipman and MacGraw (1988)**
"Employee Theft: A $40 Billion Industry." The Annals of the American Academy 498, July.
**Lodge M. (1981)**
Magnitude Scaling: Quantitative Measurement of Opinions Sage Publications Ltd. London.
**Lottier S. (1942)**
"A Tension Theory of Criminal Behavior" American Sociology Review Dec Vol 42 pages 840-8.
**Lumsden & Co. v. London TSB (1971)**
1. Lloyd's Rep. 114; 9 LDB 198.
**Lundell (1989)**
Virus: The Secret World of Computer Invaders that Breed and Destry Contemporary Books, New York.
**McClelland D. (1961)**
The Achieving Society. Van Nostrand, Princeton, New Jersey.
**McClelland D. & Burnham D.H. (1976)**
"Power is the great motivator." Harvard Business Review March-April 1976, pp. 100-110.
**MacGregor D. (1957)**
"The Human Side of Enterprise" pages 306-319 in Management and Motivation edited by Vroom V.H. and Deci E.L. (1989) Penguin Business Publications.
**Macintosh N.B. (1985)**
The Social Software of Accounting and Information Systems John Wiley & Sons Ltd.
**Manne H.G. (1966)**
"In Defence of Insider trading" Harvard Business Review November-December, pages 113-122.
**Margerison C.J. (1988)**
Managerial Consulting Skills: A Practical Guide Gower Publishing Co. Ltd., UK
**Marton A. (1990)**
"In the Belly of the Beast" Regardie's March, pages 88-100.
**Maslow A.H. (1943)**
"A Theory of Motivation" pages 27-41 in Management and Motivation edited by Vroom V.H. and Deci E.L. (1989) Penguin Business Publications.
**Mattera P. (1985)**
Off the books: The rise of the Underground Economy. Pluto Press, London.
**May M. (1989)**
"How a Hacking Law Could Weaken Security" The Times, April 20, 1989.
**Melton G.B. (1986)**
"Introduction: The Law and Motivation" Nebraska Symposium on Motivation, 1985 University of Nebraska Press, Lincoln and London, pp. xiii-xxvii.
**Melton G.B. & Saks M.J. (1986)**
"The Law as an Instrument of Socialization and Social Structure" Nebraska Symposium on Motivation, 1985 University of Nebraska Press, Lincoln and London, pp. 235-277.

**Milgram S. (1963)**
"Behavioural Study of Obedience" Journal of Abnormal and Social Psychology, Vol. 67, No. 4, 371-378.
**Morgenson G. (1991)**
"We're all right, Jack" Forbes May 13, pages 74-76.
**Morris R. (1964)**
"Female Delinquency and Relational Problems" Social Forces Vol 43.
**Morris R. (1965)**
"Attitudes Towards Delinquency by Delinquents, Non-Delinquents and their Friends" British Journal of Criminology
**Moyer R.C. (1970)**
"Berle and Means Revisited: The Conglomerate Merger" Business and Society Spring, pages 20-29.
**Muftic S. (1989)**
Security Mechanisms for Computer Networks Ellis Horwood Ltd., Chichester, UK.
**Norman A.R.D. (1983)**
Computer Insecurity Chapman and Hall, London.
**Nuttal N. (1990)**
"BT Policy on hacking criticized by Police" The Times, May 28.
**Nuttal N. (1990)**
"Friday 13th Virus Alert" The Times July 12.
**O'Shea J. (1991)**
The Daisy Chain: How Borrowed Billions Sank a Texas S&L Simon & Schuster, London.
**Peters T. (1992)**
Liberation Management: Necessary Disorganisation for the Nanosecond Nineties Macmillan, London.
**Pirsig R.M. (1992)**
Lila: An Inquiry into Morals Black Swan, London.
**Porter L.W. & Lawler E.E. (1968)**
"What job attitudes tell about motivation" Harvard Business Review (January-February), pp. 118-126.
**Press L. (1994)**
"Commercialization of the Internet." Communications of the ACM November 1994, Vol. 37, No. 11, pp. 17-21.
**Price Waterhouse (1996)**
The Paradox Principles: How High-Performance Companies Manage Chaos, Complexity, and Contradiction to achieve Superior Results The Price Waterhouse Change Intergration© Team, Irwin Professional Publishing, Chicago, London, Singapore.
**Quarterman (1990)**
The Matrix: Computer Networks and Conferencing Systems Worldwide Digital Press, Bedford, Mass.
**Quinney R. (1964)**
"The Study of White-Collar Crime: Toward a Reorientation in Theory and Research" Journal of Criminal Law, Criminology, and Police Science Vol 55, No 2.
**Randall J. (1995)**
"Agenda", The Sunday Times March 12, 1995, page 2.2.
**Raymond E. S. (1993)**
The New Hacker's Dictionary, second edition The M.I.T. Press, Cambridge, MA.
**Raymond E. S. (1991)**
The New Hacker's Dictionary The M.I.T. Press, Cambridge, MA.
**Rogerson S.C. (1992)**
"In Defence of White Collar Criminals: Why they deserve special treatment." Canterbury Business School at the University of Kent, Working Paper No 17. Originally presented to the annual meeting of the American Society of Criminology, November 3-8, 1992.

**Ross I.C. and Zander A. (1957)**
"Need Satisfactions and Employee Turnover" pages 61-71 in Management and Motivation edited by Vroom V.H. and Deci E.L. (1989) Penguin Business Publications.
**Rushkoff D. (1994)**
Cyberia: Life in the Trenches of Hyperspace. Flamingo, London.
**Saaty T.L. (1980)**
The Analytic Hierachy Process: Planning, Priority, Setting, Resource Allocation. McGraw-Hill International Book Company.
**Scase R. & Goffee R. (1989)**
Reluctant Managers: Their Work and Lifestyles Unwin Hyman, London.
**Scarbrough H. & Corbett J.M. (1992)**
Technology and Organization: Power, Meaning and Design Routledge, London.
**Schein E.H. (1988)**
Organizational Psychology Prentice-Hall, Englewood Cliffs, NJ.
**Schlegel K. & Weisburd D. (Eds.) (1992)**
White-Collar Crime Reconsidered Northeastern Press, Boston.
**Seidler L.J., Andrews F. and Epstein M.J. (1977)**
The Equity Funding Papers: The Anatomy of a Fraud John Wiley & Son, New York.
**Sherif C.W. (1980)**
"Social Values, Attitudes, and Involvement of the Self" Nebraska Symposium on Motivation, 1979 University of Nebraska Press, Lincoln and London, pp 1-64.
**Sherif C.W. (1981)**
Attitude and Attitude Chane: the Social Judgement-Involvement Approach, Greenwood, London.
**Sherif M (1956)**
"Experiments in Group Conflict" in Frontiers of Psychological Research. Readings from Scientific American selected by Coopersmith S. (1964) W.H. Freeman & Co., San Francisco and London, pp 112-116.
**Simmons G.J. (1994)**
"Cryptanalysis and Protocol Failures." Communications of the ACM November 1994, Vol. 37, No. 11, pp. 56-65.
**Simon D.R. & Eitzen D.S. (1990)**
Elite Deviance Allyn & Bacon, Boston,MA.
**Sterling B. (1992)**
The Hacker Crackdown: Law and Disorder on the Electronic Frontier Bantam Books, New York
**Stoll C.(1991)**
The Cuckoo's Egg Pan Books, London.
**Stone D.G. (1990)**
April Fools: An Insider's Account of the Rise and Collapse of Drexel Burnham Donald I. Fine Inc., New York.
**Suedfeld P. (1977)**
"The Benefits of Boredom: Sensory Deprivation Reconsidered" in Current Trends in Psychology. Readings from American Scientist. **Janis I.L.** (ed) William Kaufman, Inc., Los Altos, California, pp 281-290.
**Sutherland E. (1940)**
"White-Collar Criminality" American Sociological Review Feb, pages 1-12.
**Sutherland E. (1949)**
White-Collar Crime Dryden Press, New York.
**Sutherland J. (1984)**
The Guardian, April 12, 1984.
**Tappan P.W. (1947)**
"Who is the Criminal?" American Sociology Review Vol 12, pages 96-102.
**Tapper C. (1987)**
""Computer Crime": Scotch Mist?" Criminal Law Review, pp. 4-22
**Taylor R. (1993)**
"Going for Broke: How banking mismanagement lost £ thousands of Billions." Simon & Schuster, London.

**Taylor W. (1992)**
"Crime? Greed? Big Ideas? What Were the '80s About?" Harvard Business Review January-February, pages 32-45.
**Theft Act 1968**
**Theft Act 1978**
**Thurstone L.L. (1929)**
"Theory of Attitude Measurement" Psychology Review, Vol. 36, pp 222-241.
**Time July 25, 1994, page 34.**
**The Times**
February 3, 1990; February 10, 1990; May 2, 1990; May 7, 1990; May 25, 1990; June 8, 1990; August 18, 1990; October 15, 1990; November 22, 1990; February 6, 1991; August 6, 1993; March 22, 1995
**Tournier v. National Provincial and Union Bank of England [1924]**
1 K. B. 461
**Violano M. (1989)**
"The High-Tech Future of Foiling Fraud and Forgery" Bankers Monthly April 1989
**Violano M. (1989)**
"Are Employees Robbing Your Bank?" Bankers Monthly April 1989.
**Walker G.L. (1985)**
The Chronicles of Doodah Houghton Mifflin Company, Boston, MA.
**Wasik M. (1991)**
Crime and the Computer Clarendon Press, Oxford.
**Webber C. (1984)**
"Computer Crime or Jay-walking on the Electronic Highway." Criminal Law Quarterly (No. 26), pp. 217-250.
**West H. (1987)**
Fraud, the growth industry Kogan Page, London.
**Weizenbaum J. (1993)**
Computer Power and Human Reason, Penguin Books.
**Wilkinson R. (1973)**
The Broken Rebel: A study in culture, politics, and authoritarian character. Croom Helm Ltd., London.
**Wilson D.C. (1992)**
A Strategy of Change: Concepts and Controversies in the Management of Change Routledge, London.
**Wood C. (1988)**
Boom and Bust: The Rise and Fall of the World's Financial Markets Sidgwick & Jackson, London.
**Wolfe T. (1987)**
The Bonfire of the Vanities Picador, London.