I certify that the thesis entitled:

The evolving nature of fraud investigation and prevention

submitted for the degree of:

Master of Science (Research)

is the result of my own research, except where otherwise acknowledged, and that this thesis in whole or in part has not been accepted for an award, including a higher degree, to any other university or institution.

Full Name........Paul John SULLIVAN...........................................
(Please Print)
Signed..................................Date.......15/06/2002.....

Signature Redacted by Library
Consultation of Thesis

Please sign this form to indicate that you have used this thesis in accordance with the *Access to Thesis* form signed by the author of this thesis.

<table>
<thead>
<tr>
<th>NAME (please print)</th>
<th>SIGNATURE</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>L. VASIU</td>
<td>Signature Redacted by Library</td>
<td>23.04.03</td>
</tr>
<tr>
<td>R. LINES</td>
<td>Signature Redacted by Library</td>
<td>19.06.03</td>
</tr>
</tbody>
</table>

...
THE EVOLVING NATURE OF FRAUD INVESTIGATION AND PREVENTION

by

Paul John Sullivan

B.Com (Newcastle) M.Bus (Research)(VUT)

Submitted for the degree of Master of Science (Research)

Faculty of Science & Technology

Deakin University,

Australia.
Acknowledgments

This doctoral thesis is dedicated to the memory of my friend and mentor, the late Dr Roger Coldwell. Without his guidance and encouragement this thesis would not have been possible.

I would like to express my appreciation to my supervisor, Dr Josette Coldwell, for supervising this research since 1996 and for all her support and encouragement. I would also like to express my appreciation to the New South Wales Police Academy at Goulburn, New South Wales and to the senior management of the corporations who participated within this research project.

Special thanks must go to my children Emma, Bethany and Sean who have tolerated my absences due to my dedication to this research. Without their understanding I would not have been able to complete this thesis.

Paul J Sullivan, B.Com (Newcastle) M.Bus (VUT)
# CONTENTS

*Declaration*

*Acknowledgments*

*Table of Contents*

*Appendices*

*Tables*

*Abstract*

## Chapter One – INTRODUCTION

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Introduction</td>
<td>14</td>
</tr>
<tr>
<td>1.2 Research Goals</td>
<td>18</td>
</tr>
<tr>
<td>1.3 Significance of the Study</td>
<td>21</td>
</tr>
<tr>
<td>1.4 Methodology</td>
<td>23</td>
</tr>
<tr>
<td>1.5 Subjects</td>
<td>27</td>
</tr>
<tr>
<td>1.6 Surveys</td>
<td>29</td>
</tr>
<tr>
<td>1.7 Research Issues and Limitations</td>
<td>30</td>
</tr>
<tr>
<td>1.8 Ethics</td>
<td>21</td>
</tr>
</tbody>
</table>

## Chapter Two – LITERATURE REVIEW

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Introduction</td>
<td>34</td>
</tr>
<tr>
<td>2.2 Fraud issues</td>
<td>35</td>
</tr>
<tr>
<td>2.3 The Effects of Advances in Computing Technology</td>
<td>39</td>
</tr>
<tr>
<td>2.4 The Impact of the Internet</td>
<td>45</td>
</tr>
</tbody>
</table>
2.5 Investigative Issues .................................................................49
  2.5.1 Commonwealth Law Enforcement Board .........................50
  2.5.2 The Sullivan Report ..........................................................53
  2.6 Fraud Prevention ..................................................................58
  2.7 Summary .............................................................................65

Chapter Three - THE EVOLUTION OF FRAUD .................................69
  3.1 Introduction ........................................................................71
  3.2 The History of Fraud ............................................................72
  3.3 What Constitutes a Fraud? ......................................................74
  3.4 Computer Related Crime ......................................................77
  3.5 Types of Crimes defined .......................................................78
    3.5.1 United Nations definition .............................................78
    3.5.2 Interpol definition .......................................................79
    3.5.3 Other definitions .......................................................79
  3.6 Security Problems with Computers .......................................82
  3.7 Offences ..............................................................................85
    3.7.1 Hacking/Cracking .......................................................86
    3.7.2 Software Theft/Piracy .................................................87
    3.7.3 Telecommunications fraud .........................................87
    3.7.4 Credit Card Fraud .....................................................89
    3.7.5 Other Related Issues to Computer Crime ......................90
  3.8 Computer Related Fraud .....................................................94
    3.8.1 Computer Related Fraud techniques ..........................95
  3.9 Summary ............................................................................99
### Chapter Four - THE INCIDENCE AND COST OF FRAUD

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>102</td>
</tr>
<tr>
<td>4.2</td>
<td>The incidence and cost of fraud in Australia</td>
<td>103</td>
</tr>
<tr>
<td>4.3</td>
<td>The Perpetrators of Fraud in Australia</td>
<td>107</td>
</tr>
<tr>
<td>4.4</td>
<td>The United States of America incidence and cost of fraud</td>
<td>112</td>
</tr>
<tr>
<td>4.5</td>
<td>The KPMG Survey</td>
<td>115</td>
</tr>
<tr>
<td>4.6</td>
<td>Summary</td>
<td>118</td>
</tr>
</tbody>
</table>

### Chapter Five - THE COST OF POLICING FRAUD

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>121</td>
</tr>
<tr>
<td>5.2</td>
<td>The Cost of Policing and the Current Success of Reactive Measures</td>
<td>121</td>
</tr>
<tr>
<td>5.3</td>
<td>The Sullivan Report</td>
<td>123</td>
</tr>
<tr>
<td>5.4</td>
<td>Investigative Issues to Consider</td>
<td>126</td>
</tr>
<tr>
<td>5.5</td>
<td>The level of computer skills within the New South Wales Police</td>
<td>127</td>
</tr>
<tr>
<td></td>
<td>Service</td>
<td></td>
</tr>
<tr>
<td>5.6</td>
<td>New South Wales Police officers Attitudes to Computer Related Crime</td>
<td>129</td>
</tr>
<tr>
<td>5.7</td>
<td>The Requirements for the Retrieval of Computer based evidence</td>
<td>134</td>
</tr>
<tr>
<td>5.8</td>
<td>Issues to consider with search warrants</td>
<td>136</td>
</tr>
<tr>
<td>5.9</td>
<td>Basic steps to Consider for the search and seizure of evidence</td>
<td>138</td>
</tr>
<tr>
<td>5.10</td>
<td>Summary</td>
<td>144</td>
</tr>
</tbody>
</table>
Chapter Six - THE QUESTIONNAIRES AND SURVEYS ........................................146

6.1 Introduction ..........................................................................................147
6.2 The Survey of Potential Victims ..........................................................148
6.3 The Questionnaires ..............................................................................151
6.4 The Analysis of Convicted Fraud Offenders .........................................152

Chapter Seven - THE RESULTS ..................................................................154

7.1 Introduction ..........................................................................................155
7.2 The Results of the Survey of Potential Victims of Fraud .................156
7.3 The Results Regarding Attitudes to White Collar Crime .................176
7.4 The Results Regarding Attitudes to crime prevention .....................181
7.5 The Results from the examination of fraud offenders .....................184
7.6 Summary ..............................................................................................188

Chapter Eight - DISCUSSION OF THE RESULTS 189

8.1 Introduction ..........................................................................................155
8.2 Discussion of the Results of the survey of Potential Victims of Fraud ...190
8.3 Discussion of the Results regarding Attitudes to White Collar Crime ...206
8.4 Discussion of the Results from the Survey of Student Police Officers .207
8.5 Discussion of the Results relating to Attitudes to Crime Prevention ...209
8.6 Discussion of the Results of the Analysis of Fraud Offenders ...........211
8.7 Summary ..............................................................................................214
Chapter Nine – IMPLICATIONS OF THIS STUDY AND CONCLUSIONS ......215

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Introduction</td>
<td>216</td>
</tr>
<tr>
<td>9.2</td>
<td>An Alternative to the Current Investigation Methodologies</td>
<td>220</td>
</tr>
<tr>
<td>9.3</td>
<td>Conclusions</td>
<td>220</td>
</tr>
<tr>
<td>9.4</td>
<td>Further research</td>
<td>230</td>
</tr>
</tbody>
</table>

REFERENCES & BIBLIOGRAPHY ................................................................. 232
## APPENDICES

<table>
<thead>
<tr>
<th></th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>The survey questions for senior government and commercial executives</td>
<td>242</td>
</tr>
<tr>
<td>A2</td>
<td>The questionnaire for student police officers</td>
<td>248</td>
</tr>
<tr>
<td>A3</td>
<td>The questionnaire for detectives</td>
<td>250</td>
</tr>
<tr>
<td>A4</td>
<td>The Statistical Analysis of the classification of offences according to perceived seriousness by Detectives</td>
<td>252</td>
</tr>
<tr>
<td>A5</td>
<td>The Statistical Analysis of the classification of offences according to perceived seriousness by Detectives</td>
<td>253</td>
</tr>
<tr>
<td>A6</td>
<td>The Statistical Analysis of the responses from Detectives re possible subjects for detective training</td>
<td>254</td>
</tr>
</tbody>
</table>
TABLES

Table 1  A Summary of the Research Methodology by Chapter ..........26
Table 2  Property Crimes Reported to the Police, 1991-1992 to 1995-1996 compiled by the Australian Institute of Criminology 1997 ..............104
Table 3  Criminal Justice Statistics from the Australian Institute of Criminology 106
Table 4  Fraud Offenders compiled by the Australian Institute of Criminology 109
Table 5  New South Wales Court Statistics 1996 compiled by the New South Wales Bureau of Crime Statistics and Research ...............................109
Table 6  Recorded Crime in the United Kingdom from June 1993 to June 1997 compiled by the Home Office Research and Statistics Directorate ....118
Table 7  Respondents ranking of computer fraud against other offences ....122
Table 8  Respondent's ranking of credit card fraud against other offences ....122
Table 9  Respondent's assessment of hacking as an offence ...............................131
Table 10  1994-95 Police Expenditure Australian Institute of Criminology in a Statistical Profile of Crime in Australia .................................................132
Table 11  Size of Police Forces Australian Institute of Criminology in a Statistical Profile of Crime in Australia ........................................................133
Table 12  The position held by the respondent ..............................................156
Table 13  The Number of Known Incidents of Fraud in the Past Five Years ....158
Table 14  The Loss Associated with the Fraud ..............................................159
Table 15  How the Fraud was Discovered .....................................................160
Table 16  Offender Status ..............................................................................161
Table 17  Fraud Offenders Classified by Employment Type ......................162
Table 18  Whether or not Victims of Fraud Reported the Matter to Police ....162
Table 19  The Motivation to Report a Fraud to Police ................................163
Table 20  The Motivation not to Report a Fraud to Police .........................164
Table 21  The Most Important Issue if a Fraud occurred within the Organisation 165
Table 22  The Most Appropriate course of Action if a Fraud occurred within the Organisation ..........................................................166

Table 23  Will fraud will increase over the next five years in Australia ...............167

Table 24  The Reason behind this Perceived Increase in Fraud .............................168

Table 25  Perceived Areas where this Increase in Fraud will Occur ....................169

Table 26  The Existence of Fraud Reporting Framework ....................................169

Table 27  The Existence of Fraud Prevention Programmes ...............................170

Table 28  The Adequacy of these Fraud Prevention Programmes ........................171

Table 29  Interest Shown by the Board of Directors re Fraud Prevention ............171

Table 30  Preferred Course of Action in the event of Fraud ...............................173

Table 31  The Overall Results from the Survey ...............................................174

Table 32  The Overall Results from the Survey Classified by Industry ................175

Table 33  Classification of Offences According to Perceived Seriousness by Detectives ......................................................................................177

Table 34  Classification of Offences According to Perceived Seriousness by Student Police Officers ..............................................................179

Table 35  Responses from Detectives re possible subjects for Detectives Training 182

Table 36  Details of Arrested Fraud Offenders ....................................................185

Table 37  Victim Details based on Industry .......................................................187
ABSTRACT

This thesis is concerned with the evolution of fraud investigation and prevention in light of the advances in computing technology. These recent advances have impacted upon traditional fraud offences as well as creating a range of new crimes. The financial significance of fraud is growing whereas law enforcement and the judicial system appear to be unable to meet the demands of these emerging crimes and its victims. This research compares the responses of our present and future investigators with those of our current business leaders from the government and the commercial sectors.

This research establishes the needs of corporate decision-makers and the attitudes of police with regard to fraud. Data relating to persons arrested and convicted of fraud was also analysed to identify the issues that may be responsible for the non-reporting of offences to police by victims.

The research found that victims are seeking solutions that are not available through law enforcement, for example financial compensation. Law enforcement also under-utilises the potential of proactive responses to prevent offences and they are reluctant to acknowledge the benefits of preventative measures and to incorporate this strategy within criminal investigation training programmes. The lack of deterrence offered by the judicial system does not make the situation any better. The police function is still primarily a reactive one.

In order to overcome fraud and to be able to adapt to changes there needs to be collaboration between stakeholders. This requires a joint effort from the police, government, commerce and the victims of fraud. An innovative model involving stakeholders has been formulated that represents an alternative to the current system. This approach utilises the financial resources and expertise from the commercial sector as well as the skills of criminal investigators from the police. This means adopting a combined package of both reactive and proactive measures in order to minimise the impact of fraud. This model will be adaptive and will be able to accommodate any future requirements arising out of further inevitable advances in computer technology.
Chapter One  INTRODUCTION

1.1 Introduction
1.2 Research Goals
1.3 Significance of the Study
1.4 Methodology
1.5 Subjects
1.6 Surveys
1.7 Research Issues and Limitations
1.8 Ethics

This chapter lays the foundations underpinning this research. It introduces the current situation and options for victims of fraud and it explains the mechanisms that are used to establish the objectives of this research. This chapter also identifies the difficulties involved with defining an evolving crime, such as fraud, and it introduces the question, which is pivotal to this research, as to whether or not traditional law enforcement procedures are sufficient to deal with such evolving crimes. Finally, the research methodology is also described as well as the research structure on a chapter-by-chapter basis.
1.1 Introduction

Police and law enforcement agencies have had a virtual monopoly over the investigation of criminal activities ever since Sir Robert Peel introduced the equivalent of modern day law enforcement. Consequently, it would be fair to say that society has relied heavily upon the effectiveness and the capabilities of law enforcement to remedy any illegal activities. However, with increasing demands upon police time, resources and staffing together with limited budgets, it is debatable as to whether or not the monopoly situation that law enforcement holds over criminal investigation should be relaxed opening the way for a multi-skilled union between the victims of crime and the police. Part of the stimulus for this adaptation has probably come from the introduction and the rapid advancement of computing technology. The widespread use of computers has not only changed the lives of most individuals, businesses and governments but also those of police and investigators and the way that they should investigate crime and gather evidence in the process.

Popular opinion seems to associate computer related crime with predominantly financial offences. However, as computer technology has been accepted and adopted by all manner of persons, this technology can be associated with virtually all offences, be they traditional or technology based, simply on the basis that a computer is a storehouse of evidence and therefore valuable information.

Computing technology has also generated a whole new range of offences, some of which include unauthorised and illegal intrusions into computer systems and databases such as hacking or cracking, cellular telephone cloning, telecommunications fraud and software piracy or theft. The advancements in computing technology have also added a new dimension to a number of traditional offences such as embezzlement, larceny, homicide, paedophilia and the supply of illicit drugs. This is probably due to the fact that these offences can now be committed electronically.
rather than manually. The availability and widespread use of computing equipment throughout the business and domestic community has also increased the number of potential victims and therefore the quantity of computer based evidence.

Society's capacity to effectively investigate fraud could, arguably, be viewed as the evolution of criminal investigation. In order to keep pace with the demands of modern criminal investigation and the subsequent strain placed upon the resources of law enforcement, this evolutionary process could easily incorporate the use of skilled personnel from both the police and non-police sectors. This would provide this potential new team adequate resources and access to state-of-the-art equipment to cope and keep pace with investigations. It is possible for police to be able to create this environment by forging stronger links with the commercial sectors of industry and academia forming multi-skilled teams of investigators. This should share the burden of investigating fraud between the relevant stakeholders while at the same time providing a service to the general public and victims that this offence demands.

The aim of this research is to explore and verify the attitudes, capabilities and the procedures of traditional law enforcement investigators particularly within the area of fraud and to identify whether or not these attitudes, capabilities and procedures are sufficient to cope with the demands of twenty-first century criminal investigations. Data utilised during this research has largely come from the largest police service in Australia, the New South Wales Police Service; however, references are made to a number of other Australian and international law enforcement agencies. Regardless of the majority of the results emanating from the New South Wales Police Service it is the author's opinion that these results, generally, could be viewed as typical of law enforcement both within Australia and internationally.

As Greycar in (Grabosky, 1996, page 2) emphasises "...we have recognised that police cannot be everywhere. More so than ever, law enforcement agencies require the cooperation and assistance of the community in order to control crime. This is
especially the case in the climate of fiscal austerity that will be a fact of life for the foreseeable future..." He goes further to identify crime as a changing and evolving situation. He defines fraud as an offence that is "...as old as commerce itself, it may be expected to take new forms in the Twenty-First century..." More importantly, Graycar states that, "...one quickly notes that these trends, and the variety of fraud which may be expected to accompany them, are beyond the capacity of law enforcement agencies alone to control...".

The author's approach to this research is to investigate the attitudes of criminal investigators to investigating fraud and computer related offences as well as their attitudes towards the development of proactive measures such as training in fraud prevention for future detectives. This research also examines the needs of victims of fraud in relation to the victim's priorities after an offence has occurred, the possibility of reimbursement of stolen funds or assets, the punishment or otherwise of the alleged offender and solutions to avoid further offences.

On the basis of this evidence this research also considers alternative responses to traditional methods of investigation, particularly the possibility of a relationship between stakeholders and law enforcement. An alternative is to form multi-skilled teams of investigators comprising of members of the police service and non-police jointly funded by the public and private sectors.

The current predicament that society faces is expressed in a statement made by the New South Wales Police Assistant Commissioner Jeff Jarratt in Seymour (1997, page 2). In that statement he says "the level of fraud is so high police can no longer deal with the huge number of cases coming across their desks". He goes further to say "white collar crime is estimated to have risen by twenty five per cent in the 1995/96 financial year, with New South Wales Police investigating cases valued at $189 million in 1996". This statement is typical of the comments made by law enforcement personnel. For example, the former chief of the Victoria Police Major Fraud Squad,
Commander Allen Bowles is quoted in Simpson (1997, page 11) as saying "White-collar fraud is on the rise and police forces do not have the resources to cope with it..." and "...fraud is going through the roof...".

The investigation of fraud is itself not an easy task. The term fraud is a generic one and the offence has wide parameters unlike clearly defined offences such as murder or robbery. The offence of fraud results from a variety of motives, some of which do not always involve financial gain. Fraud can also emanate from a broad spectrum of dishonest, corrupt, deceptive and unethical practices for an even wider number of reasons. The Macquarie dictionary (1995) defines fraud as "deceit, trickery, sharp practice or breach of confidence by which it is sought to gain some unfair or dishonest advantage." That definition could encompass many situations. However, fraud by its very nature is a far-reaching, broad-based offence and elements of fraud could be present in virtually every part of human interaction.

The rapid advancements in computing technology have made the investigation of a complex offence such as fraud even more complex and more expensive to investigate, placing further demands upon limited resources. The offence of fraud will be better understood by examining the offence from two different aspects, namely, Traditional Offences, and New Offences.

Traditional offences include such crimes as embezzlement, the various types of larceny, forgery and counterfeiting, false pretences and deception. New offences include such crimes as hacking or unauthorised access to a computer system, software piracy or theft, telecommunications fraud and privacy issues. Less costly technology has also added a new perspective to old offences such as counterfeiting and forgery and the Internet have provided a new avenue to commit more traditional offences.

The increasing extent of fraud raises the question whether the public purse should pay for the inability of the private sector to "get their house in order"? This was an issue raised in the police investigation in 1992 of insurance fraud emanating from the
Newcastle Earthquake in 1989. The Task Force Choke Final Report (1992), which is examined in greater detail in later chapters, identified many of the problems associated with fraud and the resulting deficiencies in the operating procedures of the various insurance companies. The issue of alternatives to the community’s sole reliance upon the police has long been the subject of debate as seen in Swanton (1993) who suggests that perhaps the private sector should finance their own private protection based on the needs of the victims. He identifies that the services provided by the police contradict what the victims of crime require and therefore consideration should be given to using non-police to service these needs.

Similarly to what Swanton identifies, in order to gain the most out of scarce resources it is suggested that alternatives to current methodologies to combat fraud are sought so that taxpayers’ money can be better utilised in fighting crimes of violence such as murder, rape and robbery.

1.2 Research Goals

This study concerns the application and the success of traditional methods used by criminal investigators to investigate fraud offences in light of the emergence of new offences stemming from the rapid advancement of information and telecommunications technologies. It examines the success of these methods by surveying traditional victims of fraud, and it suggests possible ways in which shortfalls may be overcome. The attitudes of police investigators are also examined to determine their perception of the significance of computer-related offences, traditional white-collar crime and the introduction of fraud prevention training to future criminal investigators.

The research goals for this project and the criteria for their selection are as follows:

1. To examine the incidence, impact and changing nature of fraud,
An examination of fraud statistics will be examined in order to identify the social and financial impact of fraud. The effect of advances in computing technology will also be examined to ascertain the impact that these advances have on the investigation of fraud as well as the manner in which law enforcement investigates these new crimes.

2. To determine the attitudes of police investigators towards the investigation of fraud,

A vital part of the complete package of responses toward the mitigation of fraud is the reactive or investigative response. Therefore, it is necessary that criminal investigators' attitudes towards investigating white-collar crimes be measured. It is the author's experience that, within the New South Wales Police Service, as with other law enforcement and non-police agencies, financial crimes are not the only offence that criminal investigators have to investigate. It is therefore necessary that the significance of investigating fraud offences is measured in order to determine the priority that criminal investigators give to investigating fraud offences when faced with managing multiple investigations.

3. To determine the attitudes of police investigators towards the significance of the investigation of computer-related crimes,

It is necessary to determine whether or not law enforcement accepts the significance that computing technology has had upon the investigation of crime and whether or not it is capable and willing to adapt to meet these demands.

4. To determine the needs of stakeholders compared with the service that is provided in the course of traditional criminal investigation and,

To address the overall issue of fraud, the needs of the victims of fraud must be determined so that their requirements can be compared with the services that are provided by law enforcement. It can then be determined whether or not the current
services provided are adequate or not, and if not, alternatives to these methodologies can then be considered.

5. To seek alternatives to the current investigation methodologies.

This is dependent upon the degree of satisfaction that victims of fraud have with the current services provided to them by law enforcement and the responses given by these stakeholders in relation to their requirements. This could mean the implementation of pro-active and reactive responses but also the creation of a multi-skilled team of police and stakeholders to develop and implement a complete package of strategies rather than reliance upon single elements. The effectiveness of these alternatives can only be measured and evaluated by constant interaction with the victims of fraud.

Another vital part of the package of responses aimed at the mitigation of fraud is the proactive or preventative response. It is essential that criminal investigators should appreciate the importance and relevance of proactive measures within the full ambit of responses to fraud. Historically, the New South Wales Police Service, as with other law enforcement services, predominantly provides an investigative response. Fraud prevention strategies are an essential component in the mitigation of fraud. However the implementation, if any, of these strategies is largely dependent upon the attitudes of those who could be relied upon to implement any future policies. This research goal also examines alternatives to the current system of the public funding of criminal investigations and whether or not there are more effective means available in order to provide this service to the community.

In order to proceed with these research goals, it is necessary to examine the offence of fraud by undertaking a review of the available literature in the areas of:

- Fraud offences,
- Computer related crime,
• The effects of technology on fraud,

• Attitudes to fraud, and

• Fraud prevention methodologies.

The survey results are examined in the context of:

• Statistical data relating to the extent and cost of fraud on a national and international basis,

• Findings reported in academic papers relating to the success or otherwise of traditional criminal investigation procedures,

• The current circumstances under which most criminal investigations are undertaken,

• The impact of proactive measures compared to purely reactive responses,

• Alternatives to the current traditional methods, and

• The funding of criminal investigation with regard to fraud.

1.3 Significance of this Study

There are no studies known to the author that focus specifically upon the broad issues associated with the mitigation of most varieties of fraud offences. There have been a number of individual studies undertaken which examine single issues. For example some of the individual studies that focus on specific areas are:


• Various aspects of Fraud – The Australian Institute of Criminology.
A more complete picture can only be obtained by examining the effectiveness of current investigative procedures and any possible alternatives to these procedures, the effects of advancements in computing technology on fraud, the requirements of potential victims of fraud and the effective use of fraud prevention.

A study of existing literature on this subject indicates there has been little research undertaken with respect to the success or otherwise of the current traditional methods of investigating fraud and the impact that technology has had on these historic procedures and methodologies. Most of the available literature is from the commercial sector and the motivation for this literature seems to be financial or based on self-interest such as Arthur Andersen (1997) and Coopers & Lybrand (1997). Both of these publications predominantly focus on the risks that are faced by corporations from an audit perspective and the effect that these risks have on the operation and performance of the corporation.

Research conducted by the Association of Certified Fraud Examiners (1997) indicates that while there has been a significant increase in the incidence of fraud there has not been any significant changes made to the manner in which investigations are carried out and the outcomes that they hope to achieve. There appears to have been very little research undertaken with regard to the viability and benefits of forming multi-skilled teams of police and non-police utilising both proactive and reactive measures and the effects that would follow from the injection of personnel and funds from the commercial sector.

Similarly little research exists which examines the effects that funding non-violent crimes, such as fraud, would have on the ability of law enforcement to re-direct and inject further resources into the area of violent crimes such as murder, rape and robbery. Again, there is little research focusing on the source of the problem of fraud that provides a number of options rather than merely punishing the offender with a gaol term, fine or suspended sentence.
This research proposes and examines the viability of alternative solutions to those procedures that have been traditionally seen as the primary and only option available to victims of fraud. Also, rather than focusing on singular and industry-based issues, this research examines the entire problem of fraud focusing on:

- The ability and long term viability of the traditional provider of fraud services,
- The level of service provided by law enforcement,
- The needs of the victims, and
- Possible solutions to this predicament.

1.4 Methodology

Here the research methodology is described and the reasons for selecting the research criteria are described and presented in detail. Table 1 provides a summary of the research reported on a chapter-by-chapter basis. This diagram highlights the chapters of this research, that respectively:

1. Sets the scene for the current situation with regard to fraud investigation and depicts the methodology that is used to achieve the research goals;

2. Reviews the current and available literature in the areas of fraud investigation, fraud prevention and computer-related crime;

3. Provides an historical summary of the offence starting with the various types of fraud and their origins, progressing to the current offences generated by advances in computing technology;

4. Identifies the impact and cost of this offence on the community,
5. Illustrates investigative issues and those procedures that are adopted by law enforcement in the course of an investigation, and

6. Examines the cost of providing a police service to the community.

7. Reports on the results from the collection of data, by way of personal interview and self-completing questionnaire.

8. Discusses the results and highlights issues arising from the results from the personal interviews, the sample of actual criminal cases and self-completing questionnaires;

9. Concludes this research with recommendations for further research.

The combined effect of these chapters is intended to portray the current effectiveness of investigative issues and their impact upon potential victims of fraud. These chapters set the scene for reactive and proactive fraud prevention and at the same time they stimulate a number of questions that will be dealt with in the survey of both police and potential fraud victims. These questions and issues that need to be examined are:

1. The attitudes of police investigators towards computer related offences.

2. The attitudes of police investigators towards the investigation of fraud offences.

3. The attitudes of police investigators towards the importance of preventative measures within training for potential investigators.

4. The needs of stakeholders compared with the service that is provided in the course of traditional criminal investigation.

5. Alternatives to the current investigation methodologies.

6. Alternatives to the current funding of criminal investigation with regard to fraud.
The level of service for fraud investigations provided by law enforcement agencies, mainly the New South Wales Police Service is identified together with the needs and demands of victims of fraud, leading to the creation of an alternative methodology that is acceptable to both groups together with the preferred investigative needs of potential victims.
Table 1  A Summary of the Research Structure By Chapter

Chapter One
Introduction

Chapter Two
Literature Review

Chapter Three
Evolution of Fraud

Chapter Four
The Incidence and Cost of Fraud

Chapter Five
The Cost of Policing

Chapter Six
The Questionnaires

Chapter Seven
The Results

Chapter Eight
Discussion of Results

Chapter Nine
Conclusion
1.5 Subjects

The main subjects of this research are the two dominant participants in the process of investigating and preventing fraud, namely, the police investigators and the potential victims of fraud in both the commercial and government sectors. By extension, the judicial system also becomes a minor subject of this research on the basis of the sentences handed out to criminals who have committed fraud and, whether or not these punishments are suitable and relevant as a deterrent to committing fraud. Actual case studies of convicted fraud offenders are also analysed and compared.

The police population surveyed can be further sub-divided into student police officers and detectives. Student police officers have just commenced their careers in criminal investigations and their attitudes towards various criminal offences should be more flexible and less influenced by institutional ideologies. As a consequence student police officers’ responses could perhaps be seen to be more representative of the population at large.

Detectives, on the other hand, could be seen to be more institutionalised and they have been employed and are operational within their individual careers long enough to have definite attitudes and professional beliefs.

The police participants who were surveyed in relation to financial crimes and their attitudes were all studying at the New South Wales Police Academy in Goulburn for the twelve months ending December 1995. They were selected at random over that twelve-month period and the surveys were self-completing with a one hundred per cent participation and return.

The detectives who were surveyed in relation to fraud prevention training were stationed at a number of police stations around the State. Surveys were facsimiled to every police station in the State of New South Wales that accommodated criminal
investigators and the responses from these self-completing questionnaires were returned by way of facsimile with a return of approximately thirty per cent.

All of the persons who participated in the survey of potential fraud victims were selected at random. These persons were personally interviewed as opposed to a self-completing questionnaire and all of these persons were senior executives within either the government sector or the commercial sector.

A fourth sample of data has also been obtained from the computer records of the New South Wales Police Service Criminal History database. This sample contains a detailed examination of a random sample of twenty-eight case studies of persons who have been arrested, charged and convicted of fraudulent offences. These case studies relate to actual instances of persons arrested for fraudulent activities. The examination of these case studies is intended to shed some light on the various means by which fraud is committed, what group of persons predominantly commits these frauds, the nature of the offences and the punishment given to these offenders by the Criminal Courts.

The findings from this survey are then compared to the findings regarding the police and their attitudes to computer-related crimes and fraud prevention issues. These findings will then be compared to the results from interviews with senior executives from large commercial and government organisations with regard to the corporate needs of potential fraud victims. The results from this survey will also identify:

- The sex and age of the offender,

- The punishment or sentence given to the offender after conviction,

- The amount of the financial loss,

- The person's employment status and

- Whether or not that person was an employee of the victim of the crime.
By highlighting particular traits of convicted fraud offenders and their method of operation, it may assist in identifying certain high-risk groups of persons who have a propensity towards committing fraud. In the overall scheme of fraud prevention this may assist in targeting such high-risk groups in order to minimise the commission of fraud by employees.

1.6 Surveys

As described in 1.5 the populations for these surveys are the police and the commercial and governments sectors. The police component of the survey can be further divided into two categories according to the subject of the survey, namely:

1. Attitudes to fraud, and

2. Attitudes to fraud prevention as a part of the Detectives Education Programme for criminal investigators at the New South Wales Police Academy.

The sample size for the survey on attitudes to fraud at the New South Wales Police Academy at Goulburn, New South Wales was five hundred and ten respondents consisting of student police officers and detectives. These respondents were studying at the Police Academy at the time of this survey.

The sample size for the survey, on attitudes to fraud prevention as a part of the Detectives Education Programme, was fifty-one respondents consisting of experienced criminal investigators selected a random from around the State of New South Wales. Every Police Station within the State, that had criminal investigators on staff, was sent a self-completing questionnaire.
The sample size for the survey of senior executives from the commercial and government sectors was thirty respondents. These respondents were selected randomly and unlike the police respondents, they were each interviewed personally from a predetermined schedule of questions.

At the time the sample size of twenty-eight actual computer fraud cases studied was determined by the availability of data. At that moment when the sample was taken there were only twenty-eight cases on the police database.

1.7 Research Issues and Limitations

This section considers aspects that relate to the reliability and validity of the data. Part of this study was undertaken only at the New South Wales Police Academy from recently recruited student police officers and experienced detectives. This institution has its own distinct culture that may have permeated through to the detectives. This culture may have influenced the responses from the student police officers in particular, whose academic achievement and behaviour has an effect upon their graduation.

The sample of detectives surveyed about fraud prevention methodologies was comparatively small when compared to the large number of respondents from the previous questionnaire. This survey amounted to only fifty-one respondents. Greater confidence could be placed in the findings and conclusions with a larger proportion of the population however, every detective's office in the State of New South Wales was canvassed in the course of this research.
The sample size of thirty corporations and respondents from the ranks of senior executives from the commercial and government sectors was also comparatively small, however this was seen as a realistic and achievable sample.

1.8 Ethics

All of the responses provided by police were anonymous. The only identifiable feature from their responses was their location at the time that this questionnaire was completed. The responses received from questionnaires from detective's offices across the State were also anonymous and unidentifiable.

Individuals within the commercial and government sectors were interviewed personally. However no detail was recorded of the specific company or department nor was there any details recorded of the individual who provided the information. In all cases, both police and non-police, only the position held by the respondent within their respective organisation was requested and recorded.

The details obtained by the author, with regard to an examination of a random sample of twenty-eight case studies of persons who have been arrested, charged and convicted of fraudulent offences, have been obtained with the approval of Assistant Commissioner Christine Nixon of the New South Wales Police Service. These case studies have been retrieved from the New South Wales Police Criminal History database and they relate to actual instances of persons arrested for fraudulent activities. None of the persons within these case studies are identifiable. The only identifiable features of the offenders are their individual ages, sex and whether or not they were in the employ of the victim of their crime. All of the reports and data obtained from the New South Wales Police Service have been done so with their approval.
All respondents were informed and all respondents gave approval that the information that they provided and the results stemming from that information were for the express purpose of this doctoral research and that this information would be published.
Chapter Two  LITERATURE REVIEW

2.1 Introduction
2.2 Fraud Issues
2.3 The Impact of Advances in Computing Technology
2.4 The Impact of the Internet
2.5 Investigative Issues
2.6 Fraud Prevention
2.7 A Summary of Implications for this Study

The previous chapter has described the research aims and the manner in which they are to be achieved. This chapter focuses on the literature that covers the subject of this research, namely fraud issues in general, the effects of advances in computing technology upon fraud, the impact of the Internet upon fraud, investigative issues and fraud prevention.
2.1 Introduction

This section reviews the available literature that relates to the issues covered by this research, namely:

1. The current and emerging risks associated with fraud,

2. The effectiveness and the ability of current investigative bodies to cope with these challenges,

3. Alternatives to current investigation methodologies, and

4. Effective ways in which to minimise these identifiable risks.

This literature includes academic journals, cases reported through the printed media, industry-based publications, government journals and commercial publications. This research is unique in that it focuses specifically upon all of the relevant fraud issues associated with the mitigation of fraud rather than interest-based and industry-based issues.

There isn't any literature known to the author that incorporates each of the above issues in points one to four. However, there is a considerable amount of literature written about individual issues such as, industry-based fraud, the effects that computing technology has had upon the commission of fraud, the impact of the Internet and proactive and reactive measures that have been developed to mitigate the impact of fraud. The bulk of the available literature emanates from the commercial sector on an industry-by-industry basis such as insurance fraud and superannuation fraud and it is therefore not as publicly available as information emanating from government departments such as the Australian Institute of Criminology.

In order to cover all of the areas of this research identified previously the available literature will be reviewed according to individual topics namely:
1. Fraud issues,

2. The effects of advances in computing technology upon fraud,

3. The impact of the Internet,

4. Investigative issues, and

5. Fraud prevention.

2.2 Fraud Issues

In this section the industry-based fraud literature will be examined together with academic and government publications on fraud. The purpose of this examination is to scrutinise the industry-specific responses to fraud in order to identify the effectiveness of any procedures.

As previously stated much of the available information on the subject of fraud has focused upon only a small portion of the problem, rather than concentrating on the entire issue. This is arguably due in part to self-interest and the scope of fraud that can virtually be attached to every form of human interaction. Publications that are typical of this include;

- Deloitte Touche Tohmatsu (1996): *Best Practice Guide to the Detection of Superannuation Fraud* which identifies the risks involved in creating and participating in superannuation funds and,

- Morris, R. (1994): *Credit Cards, Fabrication Techniques for Genuine and Counterfeits* which highlights a number of methods for duplicating and creating
credit cards. Morris also identifies a number of risks in using credit cards and he provides recommendations in order to minimise these risks.


Baldock raised a number of issues and they are particularly relevant to this research as well as also being common to most varieties of fraud. The most significant points raised by him in relation to this research are:

- Fraud, by community standards, is an acceptable crime.

- He cites inadequate legislation, prosecution and media coverage as a reason for this communal attitude and that government should, "...send a clear message to the general community that insurance fraud is a criminal offence and that persons who commit insurance fraud will be treated accordingly." (Baldock, 1997 p2)

- He claims that police do not view this particular type of fraud as a major concern, implying that the investigation of insurance fraud would be given a low priority in the workload of an investigator.

- He recognises the inadequacies of the current law enforcement bodies to cope with insurance fraud. As a result of this situation many of Australia's major insurance companies and banks have created their own investigative response.

It is possible that these banks and insurance companies have created their own internal investigation sections due to dissatisfaction with the services that are provided by law enforcement agencies. It may also be due to their desire that their industry-specific requirements can be concentrated on by their own investigators who are also under their control whereas traditional law enforcement is not.
• Baldock also recognises the success of combined police and insurance company task forces such as Task Force Choke. This specialist unit was created to investigate allegations of insurance fraud emanating from the Newcastle Earthquake in 1989. Despite a number of industry-based requests this specialist unit was disbanded in 1993. Baldock also highlights the futility of disbanding these specialist units after they had achieved their specific investigations.

*Task Force Choke Final Report* (1993): *The New South Wales Police Service*, identified the success of a multi-skilled team of both police and non-police during the earthquake Task force. On page eleven of the report it went further to say that "...it is felt from an summary of the investigation that the liaison between the police and insurance industry is being greatly enhanced by the creation of an Insurance Unit at the Fraud Section..." Not only was Task Force Choke disbanded in 1993 but the Insurance Unit was disbanded at the same time as the closure of the Fraud Section and the creation of the then Fraud Enforcement Agency in 1994. Up until the time of this research it was unknown whether or not the New South Wales Police Service has created permanent industry-specific investigation units.

A significant feature of this report was that it laid the blame for any insurance fraud squarely on the shoulders of the insurance industry on the grounds that "...they did not have a suitable contingency plan in position" (p.11). This statement gives support to Baldock’s opinion that the police do not and should not take responsibility for fraud and that it is the police perception that fraud is more an industry problem rather than being a law enforcement problem. Overall the *Task Force Choke Report* identifies areas of fraud risk and blame without providing recommendations to rectify risks within the industry, suggesting that the insurance industry as a whole should be proactive and responsible for their own problems.

Other industry-based publications relating to fraud, which are typical of the response to combating fraud, include Deloitte Touche Tohmatsu (1996), which covers specific
problems associated with superannuation fraud. This publication provides solutions and proactive recommendations to minimise the risks associated with superannuation fraud and it identifies fraud risks from an industry-specific perspective. It recommends that an effective response to fraud should include a package of both proactive and reactive responses. This paper focuses upon micro issues only and it does not address the broad based problems such as the non-reporting of offences, the effectiveness or ineffectiveness of current investigative methodologies, reasons why offences are not reported to law enforcement and solutions to these problems.

The Australian Institute of Criminology publishes a number of quality publications on fraud by authors such as Grabosky and Smith covering a broad range of issues. In one such publication Grabosky and Smith (1996) successfully identify the social, economic and technical changes in relation to the offence of fraud. As early as 1996 they identified specific commercial areas where there could be an up-surge in offences such as Electronics Funds Transfers, industrial espionage and telecommunications fraud on a global scale. History has proven these assertions to be correct. They also recommend that the management of these fraud risks, from a proactive planning perspective, is the preferred course of action. This would involve the compilation and analysis of data from both government and non-government sources.

There have been a number of other quality publications such as “Organisations as Victims of Fraud and How They Deal with It” Smith (1999) and “Professional Advisers and White Collar illegality: Towards Explaining and Excusing Professional Failure” Grabosky (2000). In Smith (1999) consideration was given to a number of ways in which to increase the probability of victims of fraud reporting matters through traditional avenues whereas Grabosky (2000) discussed the methodologies behind the failure of professionals in dealing with fraud. Both publications confronted a number of relevant issues such as the preferred courses of action of victims of fraud and the failure of external audit to identify fraud, however, like other papers, they still touch on micro issues rather than the entire predicament. The approach to combating fraud
needs to be identified and totally re-defined from start to finish rather than individual
responses to isolated problems, which seem to be the focus of much of the literature to
date. For that reason most of the available literature is still industry-focused responses
to fraud.

In summary, the available literature on fraud discusses the offence predominantly on
an industry-by-industry basis. While that literature is detailed in its evaluation of
specific industries it does not focus on fraud from the broad perspective that is
required in order to achieve the goals of this research.

2.3 The Effects of Advances in Computing Technology

In this section, the literature relating to the impact of computing technology and how
and why it is has affected the commission of fraud is discussed. Decades ago
accounting records would have been maintained in hard copy journals and ledgers. For
funds to be illegally redirected by offenders those records would have had to be
corrupted. Arguably, today those same records would be maintained on a computer
and therefore the successful criminal would have no choice but to have a general
knowledge of computing in order to carry out offences. This isolated instance is but
one of a number of examples depicting the impact that computing technology has had
on the commission of fraud. Computers are now viewed as an essential tool and an
essential part of our lives and for those reasons alone the impact of advances in
technology must be considered when examining criminal investigation issues.
According to Wockner (2001) a report by the Independent Commission Against
Corruption identified opportunities for electronic corruption that were increasing on a
daily basis and that the automation and speed of new technology means traditional
auditing procedures are ineffective.
According to Smith (1998a) "...the most profound technological developments which has taken place in recent years have involved computer and telecommunications systems..." Grabosky and Smith (1996) extend this by stating that the development of these information systems has provided opportunities for the commission of a wide range of criminal acts. The rapid advances in computing technology have had the most significant impact on the traditional offence of fraud by providing:

- Affordable computing technology and equipment, which can be utilised by victims and also by criminals. Access to affordable state-of-the-art equipment has given criminals the ability to produce better quality forgeries in crimes such as counterfeiting credit cards and holograms, documents and cheques; and

- The circulation and dissemination of information, training and the means to commit offences via the Internet.

Many households, businesses and institutions have access to computing technology and this has created a situation where not only has the number of potential victims risen, but also the number of possible offenders. By extension, it would be fair to say that the number of computer literate persons would be considerably greater now thereby increasing the number of possible offenders and crimes.

Grabosky and Smith (1996) state "...In the realm of fraud, expanding computer literacy will increase the number of prospective offenders, while new technologies allow easier and cheaper access to a much larger pool of prospective victims." They identify electronic funds transfers fraud and telecommunications fraud as two areas of potential for fraudulent activities and more specifically smart card and stored value card technology together with home shopping utilising electronic cash as rich avenues of fraud in the future.

This opinion is reinforced by a major Australian law firm, Minter Ellison, which states that "...computer fraud and electronic funds transfers have greatly increased the risks
of banks making and receiving mistaken payments," and "banks must be aware of the risks of dealing with money received by mistake." Marriott (1988 p29-37)

Johnson (1997) identifies situations where criminals have claimed to have hacked into pagers owned by members of the White House staff capturing private messages about President Clinton by using eavesdropping equipment. Johnson also reveals that criminals are also using the latest technology to create forged documents as part of frauds estimated to be worth billions of dollars a year in the United States. Situations such as this raise the question of whether or not law enforcement has kept pace and are able to keep pace with, the rapid advances in computing technology and education.

In 1997, the Office of Strategic Crime Assessments (OSCA) in conjunction with the Victoria Police undertook a joint study of computer related crime, the findings of which were documented in the Computer Crime and Security Survey (OSCA 1997). This survey of over three hundred Australian companies purported to be the first of its kind in Australia. Its purpose in surveying corporations, government agencies, financial and medical institutions and universities across Australia was to gather data, to gauge the extent of the threat of computer related crime and to assist law enforcement agencies. According to this document the study aims were "...to

- Identify the major trends in emerging information technologies and to assess their potential impact on the nature and extent of cyber-based crime over the next five to ten years, and

- To provide preliminary advice on the strategies and policies that may be required to meet the threat posed by crime in cyberspace.

The survey established that Australian industry is under threat from criminal activity and their findings indicated that:

- Australian industry is subject to a significant level of computer security incidents at a rate comparable to the United States,

- The main threat comes from employees however there are growing incidents of an external menace,
• The primary target of attacks is Australia’s banking and finance industry, and

• Survey data support the assertion that there is a direct correlation between our increasing dependence on sophisticated information technologies and a growing level of vulnerability to electronic attack."

OSCA (1997) recommends that Australian law enforcement should contemplate how to stimulate greater cooperation between the private sector and law enforcement in order to reduce the threat however the project falls short in offering solutions. This survey merely confirms that the commercial sector is vulnerable to this type of crime. The positive side of this survey is that it provides a springboard and a starting point for future comparison and analysis. However this survey also generates a number of questions:

• Now that this menace has been identified to us how do we attack it and minimise its impact, and

• Does traditional law enforcement have the physical and financial ability to investigate these new and evolving offences?

Some answers to these questions are provided in the United Nations (1995), which focuses, in part, on the prevention and control of computer-related crime. According to this report a resolution was adopted at the 1990 meeting of the Eighth United Congress, with regard to computer related crimes. This resolution called upon the member States of the United Nations to intensify their efforts to combat computer crime by considering the following measures:

• Modernisation of national criminal laws and procedures, including measures to:

  1. Ensure that existing offences and laws concerning investigative powers and admissibility of evidence in judicial proceedings adequately apply and, if necessary, make appropriate changes,
2. In the absence of laws that adequately apply, create offences and investigative and evidentiary procedures, where necessary, to deal with this novel and sophisticated form of criminal activity, and

3. Provide for the forfeiture or restitution of illegally acquired assets resulting from the commission of computer related crimes.

- Improvement of computer security and prevention measures, taking into account the problems related to the protection of privacy, the respect of human rights and fundamental freedoms and any regulatory mechanisms pertaining to computer usage,

- Adoption of measures to sensitize the public, the judiciary and law enforcement agencies to the problem and the importance of preventing computer related crimes,

- Adoption of adequate training measures for judges, officials and agencies responsible for the prevention, investigation, prosecution and adjudication of economic and computer related crimes,

- Elaboration, in collaboration with interested organisations, of rules of ethics in the use of computers and the teaching of these rules as part of the curriculum and training in informatics, and

- Adoption of policies for the victims of computer related crimes that are consistent with the United Nations Declaration of Basic Principles of Justice for Victims of Crime and the Abuse of Power. This should include the restitution of illegally obtained assets and measures to encourage victims to report such crimes to the appropriate authorities.

Within the resolution of the Eighth Congress there was also a recommendation that the Committee on Crime Prevention and Control should promote international efforts in the development and dissemination of a comprehensive framework of guidelines
and standards that would assist member states in dealing with computer related crime. It also recommended that this committee should initiate and develop further research and analysis in order to find new ways in which member states may deal with the problem of computer related crime in the future. It was also recommended that these issues should be considered by an ad hoc meeting of experts.

Computer related crime, which incorporates most of the current fraud offences, is a crime that is truly international in that the crime does not recognise, nor do any state or national borders restrict it. Therefore, the only realistic response to a crime of this nature is an international response. As a consequence of the resolutions from the Eighth Congress and the Committee on Crime Prevention and Control the United Nations Manual (1995) was developed. This manual maintains all of the elements within the resolution ratified by the Eighth United Nations Congress and it addresses both proactive and reactive issues with regard to computer related crime.

This manual addresses the problem of computer related crime by recommending that law enforcement agencies should have broad-based ethics training, computer security and curriculum including codes of conduct and behaviour for computer users. Reactive issues, such as comprehensive training for law enforcement and judicial staff, the confiscation of illegally obtained assets and the modernisation of criminal laws are recommendations that will effectively and realistically confront this crime.

Further recommendations call for the global standardisation of investigation techniques, legislation and training. The manual also suggests that law enforcement agencies need to improve computer security, to develop preventative measures, training, curriculum, to train the judiciary and investigators up to a uniform standard in both proactive and reactive techniques. This report also recommends that the general public, the judiciary and law enforcement agencies should all be sensitised to the problem at hand. This manual provides a benchmark for proactive and reactive responses in the war against computer related crime.
Similarly, in 1994 a steering committee was created by Interpol to examine international investigative issues and to arrange a meeting of international experts in the field of computer related crime. As a consequence, a manual, Interpol (1995) was created which created guidelines and recommendations similar to those of the United Nations. Following on from that manual, in 1995, *The First International Conference on Computer Crime* was organised at the headquarters of Interpol, at Lyon in France. The conference was well attended by delegates from Europe, Asia and the Americas with Australia represented by the author, who was a keynote speaker. The resolutions stemming from this conference and those from the following conference in 1996 will be discussed further in this chapter however, in summary, very little solid progress was made apart from the universal agreement to hold further meetings.

In summary, the recommendations made by OSCA, Interpol and the United Nations are still only recommendations and they can only be introduced voluntarily. According to the United Nations manual much of the success in addressing these issues, appears to have been achieved in and isolated to Western Europe. It is questionable whether or not the many forms of government, religion, culture and economic position across the globe can agree to this universal change. While there are nations outside of Western Europe that do not adopt the preventative, legislative and investigative issues highlighted in this document, there will always be weaknesses and therefore loopholes for criminals to utilise.

### 2.4 The Impact of the Internet

The Internet has been hailed as a bastion of free speech with a worldwide platform for anyone who has something to say and has the right equipment and the ability to do so (Babin, 1996). It provides rapid communications to millions of persons or clients, it
provides a facility for mass marketing, access to data, electronic commerce and
electronic banking, to name but a few services. It would be fair to say that the Internet
has provided many persons with information at their fingertips that normally would
have taken a considerable amount of time to acquire. Within the developed nations,
industrialists, business managers, academics and most persons generally have access
to the world-wide-web and electronic mail now. These same persons can now
converse quickly and reliably with persons of similar interests around the world and
they can also access information from a variety of global sources and disseminate this
information as they see fit.

However, has this increased use, availability and access to the Internet also assisted
criminals with their activities? Criminals are no different to legal entrepreneurs in that
they too need information to learn their respective trades as well as regular access to
peers with whom to discuss issues. The Internet provides a potential vehicle for this
education and information dissemination.

According to Babin (1996), the Internet is an unregulated conglomeration of
companies, individuals, governments, educational institutions, and other organisations
that have agreed, in principle, to use a standard set of communication protocols.
Arguably, because of the lack of regulation over the Internet, it is wide open to
exploitation by the criminals.

There are no police officers on the Information Superhighway waiting to apprehend
offenders who have strayed outside of any guidelines and this leaves Internet users to
regulate each other according to the reigning norms of the moment. According to
Harris (1996, page 13), "...there seems to be a vast difference in the standards for the
behaviour of normal citizens in the suburbs as opposed to those who travel in
cyberspace." Harris goes further to say that, "...cyberspace is also a virtual trap where
faceless, nameless con artists can rejuvenate and recycle old scams that have been
controlled and restricted in the physical market." For example, some of these recycled
Scams involve selling products that do not perform as they are advertised or hot tips on company shares that are expected to rise dramatically.

The Internet can also be utilised by the criminal element as shown by Sullivan (1996a). In a report prepared for the New South Wales Police Service on computer related crime he suggests that the Internet provides:

- Access to offensive material such as child pornography,

- Money laundering,

- A forum and a network for paedophile groups,

- Access to offensive software such as virus generators and tutorials, encryption software, hacking tools and credit card generators,

- Fraud tools such as password crackers and system interrogators,

- Access to information, and

- The resurgence of scams such as
  - Bogus and disguised advertising
  - Exaggerated or false product claims
  - The sale of goods at inflated prices, and
  - Insider information on stocks.

Johnson (1997, page 32) reports some of the findings from the Symposium on Economic Crime in Cambridge, United Kingdom, where delegates were told that "... computers and the Internet were fast becoming popular tools for criminals..."

Delegates were also warned that "...a new breed of fraudsters are using new
technology to steal vast quantities of money..." More importantly, it was stated that "...if the law has not been able to keep up with the internationalisation of crime, in either its reach or its resources, the prospect of criminals and in particular organised crime, moving into cyberspace is fundamentally more threatening."

At the Second International Conference on Computer Crime at Interpol headquarters in Lyon, France Babin recommended that, due to the insecurity of the Internet and electronic mail, the Internet only be used for the following non-confidential police procedures (Babin,1996):

- Police-to-police information exchange on the topics of unclassified procedure or technical matters,

- The exchange of general information with the public,

- Sharing of criminal and safety information with the public, for example missing persons reports, general crime alerts and requesting public assistance in crime solving,

- Police FTP servers for general police techniques and information,

- Reaching experts on the Internet, and

- The promotion of police fraternity and camaraderie.

Babin does not focus on the problems associated with using the Internet that should be addressed before trusting the current technology with confidential criminal histories, fingerprint details and intelligence. From the above list it suggests that Babin would not use the Internet for routine police investigations and inquiries, which is law enforcement's main function.

In summary, the problems with police using the Internet are:
• It is not owned by any one person or group who could therefore be held responsible for its operation, its control or monitoring its activities,

• The inability to securely transfer confidential information and,

• It crosses a number of cultural and political boundaries making it difficult, if not impossible, to standardise acceptable practice. For example some countries may find certain types of nudity both morally and legally offensive while yet another country may not and feel quite comfortable disseminating this type of material. The Internet is a true multinational tool.

2.5 Investigative issues

This section reviews literature on purely investigative issues such as operating procedures and practices. There is little academic literature available on this subject. Most of the available information stems from either law enforcement or from the government, illustrated in the following documentation.

Interpol Computers and Crime International Criminal Police Organisation (1995) is a manual developed by the Interpol Computer Crime Working Group for and on behalf of the law enforcement community in Europe. It is an attempt to give a broad summary of computer crime issues and to provide guidance for law enforcement officers who may come across computers in the natural course of their investigations. Similar versions and ideologies were planned for the rest of the world. However, up until the time of this research, the author is unaware of any progress in this area.

The main thrust of this publication is its emphasis on dedicated training for investigators to enable them to cope with the demands of a new era of investigation. This is the logical starting point for addressing this investigative issue. Interpol recognises and is attempting to address a global problem; however, it does not address
the entire problem of fraud in the same manner as the United Nations, merely an aspect of it.

This manual was a precursor to the First and Second International Conferences on Computer Crime held at Interpol Headquarters Lyon, France in 1995 and 1996. Most of the fifty countries that were represented at these conferences conceded that their law enforcement agencies had only a limited response and appreciation of the problems associated with computer related crime and that the legislation and training of investigators were of great concern. Only countries such as the United Kingdom, Canada and the United States of America had any firm policy and procedures governing the investigation of computer related crime. The remaining countries, which included Australia, had very little in the way of investigative procedures and methodologies and possibly due to this fact, the 1995 conference focused more on the awareness and identification of the various types of crimes.

The Second International Conference on Computer Crime in 1996 unfortunately only concentrated again on peripheral issues and awareness of crimes rather than suitable legislation, training issues, the impact of the various technologies and the overall quest for viable solutions. After recognising that computer related offences were a global issue the coordinators at Interpol then left it to individual regions to organise the training of their own investigators rather than developing a standard course. A common complaint was that only the Europeans were gaining access to specialised courses whereas all other countries were left to organise their own.

2.5.1 The Commonwealth Law Enforcement Board

In 1996, the Australian Commonwealth Law Enforcement Board, in consultation with Commonwealth departments and agencies, co-ordinated the development of a Commonwealth-wide review of fraud control arrangements, which was reported in;

This document outlines the principles of fraud control and the development of national standards for Commonwealth agencies. It provides a standard set of policies and directions to assist Commonwealth departments and agencies in carrying out their responsibilities to combat fraud against their programs. Outlined within this document are the agency responsibilities for fraud prevention, reporting of fraud information, fraud investigation case handling and training of agency fraud investigators.

The Commonwealth has established a standard by which all Commonwealth agencies must abide. This standard consists of eight phases or various levels of a fraud investigation. It is mandatory that each of these stages be performed in order that the investigation is deemed to be an effective and efficient investigation. The eight stages are:

- Agency - legislation and powers,
- Inter-agency relationships,
- Allegation of fraud, initial consideration/subsequent action – reactive responses,
- Investigation management methodologies and support – case management,
- Operational practices,
- Investigation report or brief of evidence – evidentiary issues,
- Investigation result and review; and
- Recovery actions.

The Commonwealth Law Enforcement Board (1996 p 10) also defines an efficient investigation and an effective investigation as "..."
An efficient investigation

An investigation completed in accordance with legislative requirements within a suitable time and at a reasonable cost, having taken into account the nature and complexity of the investigation, availability of resources (both material and human) and the aim of the investigation.

An effective investigation

Is an investigation that satisfactorily proves or disproves an allegation or achieves an acceptable conclusion.

In the case of a proven allegation, an effective investigation:

- Deals appropriately with the offender(s) in either the criminal, civil, administrative or disciplinary jurisdictions, or both,

- May improve controls - fraud prevention,

- Deters others from attempting to commit similar offences, and

- Improves public confidence in the integrity of the agency.”

These standards have been created by the Australian Commonwealth to be used by and for the benefit of its own agencies. Regardless, the principles that are identified in this document are still relevant for use outside of those government agencies. Possibly, due to the fact that this document has been created by and for the government, it has ignored an important investigative aspect, namely, the cost and funding of this initiative. I believe this investigation package is too standard an approach to an offence that has many varieties and complexities as previously illustrated. The author believes that it is difficult to develop standard operating procedures that can be applied successfully to every type of offence.
2.5.2 The Sullivan Report

Sullivan (1996a) compiled this report as a result of a period of time acting as a consultant for and on behalf of the State Commander of the New South Wales Police Service and the Special Technical Investigations Bureau. The purpose of this consultancy was to research various aspects of computer-related crime, part of which included the next generation of fraud namely, computer fraud and the retrieval of computer-based evidence. He saw the ability to investigate computer-related crime effectively as not just the introduction of a new concept but, the adaptation of police investigative techniques to cope with the demands of twenty-first century policing. With that in mind, the report was designed to keep the New South Wales Police Service up to date on the most current practices for the retrieval, analysis and investigation of computer-related crime. Sullivan emphasised the importance of the role of education as he believed that all police should have the ability to recognise, appreciate, respond and investigate technical crimes.

During the course of this research for the New South Wales Police Service, the author identified two distinct schools of thought regarding the effective retrieval, analysis and investigation of computer-related crime. Firstly, there are the computer technicians who believed that the retrieval of computer-based evidence should be left to them and to those persons who have an in-depth knowledge of computer technology as well as standard operating procedures. Alternatively there are non-technical persons who believe that, due to the present levels of user-friendly technology, the retrieval and analysis of computer-based evidence can be achieved in collaboration with computer skilled persons. Sullivan took the view that this approach would result in a response that would achieve large-scale results, rather than limited results by using only trained personnel conversant with the operation of the machinery and not its dynamics. This would conform to the current system within the police service for the introduction and
accreditation of complex equipment such as the Police radar and the Breathalyzer for example.

Sullivan's philosophy was that education is the logical starting point for the development of the necessary skills to investigate new technical crimes, and the next generation of recognised offences. He recommended that all police, both investigators and uniformed police, have access to this training, rather than merely specialist investigators. Uniformed Police are usually the first to arrive at crime scenes and they therefore must have at least an appreciation of the crime so that they don’t inadvertently destroy potential evidence. Sullivan claims it is essential all police have an ability to recognise potential computer related crime evidence in the same fashion they can identify the potential evidentiary value of a blood stained weapon or an Indian hemp plant.

In order to provide uniformed police officers with an appreciation of the requirements of this type of crime Sullivan recommended that they be trained in such basic subjects as:

1. Computer hardware and software,
2. How information is stored on a computer, i.e. file systems,
3. MS DOS operating system,
4. Windows Operating system,
5. Wide Area Networks (Internet) and Local Area Networks,
6. Computer related crime offences, and
7. The identification of exhibits.

Criminal investigators, specialist and general, are the persons who will take the responsibility for investigating computer-related crimes and for that reason Sullivan recommended that all criminal investigators be additionally trained in the operation,
search, seizure and analysis of computer based evidence incorporating whatever retrieval equipment is chosen. It would involve such subjects as:

1. Computer hardware and software,
2. How information is stored on a computer,
3. MS DOS operating system,
4. Windows Operating system,
5. Wide Area Networks (Internet) and Local Area Networks,
6. Computer related crime offences,
7. The identification of exhibits,
8. An introduction to the forensic analysis of data,
9. Search procedures involving computers, seizing the hardware and copying on site,
10. Operating procedures for a computer containing suspect data,
11. Copying, storing and analysing potential evidence, and
12. Locating evidence on a computer.

The final stage of most investigations is proving the prosecution case before the court. Sullivan recommended that, due to the technical nature of this offence, police should not be trained with a view to them giving expert evidence. Realistically, police could not be expected to be able to provide the technical expert evidence at court and therefore the reliance on police to do so could weaken the prosecution case. Sullivan saw difficulties in creating and maintaining police who are capable of providing expert evidence in the area of computer related crime within a police environment. Apart from the cost effectiveness of providing this service statewide, it is questionable whether or not the police service could retain staff members who have sufficient and commercially attractive skills.
Sullivan saw the weak link in the chain of investigation as being the police, unless the emphasis is taken away from those persons and placed on to the *Standard Operating Procedures*, the retrieval equipment and the use of independent expert witnesses and evidence. A case can be lost in a court of law if the matters rely solely on an individual’s qualifications as that person’s actions are open to varying interpretations. Sullivan therefore supported the belief that it was the retrieval equipment and independent expert witnesses who needed to be scrutinised and accredited rather than the police who merely use the equipment, much in the same way as the police radar and breath testing equipment is currently.

Expert witnesses and their evidence could be utilised to support the prosecution case and the *Standard Operating Procedures* used by the criminal investigators if and when the need arises. There are however, a number of issues that must be considered when using expert witnesses. Firstly, qualifications by themselves do not make a person an expert in the eyes of the court and, therefore, a person’s work experience, the number of years that the person has performed those duties and any tertiary qualifications that can support this experience must be present. An example of the need to qualify expert witnesses is identified in the Task Force Choke Final Report (1992). During criminal proceedings for persons arrested for fraudulent activities during rectification works with regard to the Newcastle earthquake in 1989, the author witnessed a number of supposed expert witnesses who gave evidence in conflict with that of other expert witnesses and in the process, jeopardising the prosecution case. With that in mind, the field of computer related crime is a vast area crossing many areas of expertise thereby requiring specialist evidence. Sullivan recommends that a strong relationship between the police service and academia be established in order to provide this service on demand.

In the process of compiling this report for the New South Wales Police Service, Sullivan conducted research in the United Kingdom with a number of law enforcement Computer Crime Sections and into their methods of operation. Sullivan
examined the level of training, the standard operating procedures and the use of expert witnesses utilised by New Scotland Yard (1996), South Yorkshire Police (1996), Thames Valley Police (1996) and West Mercia Constabulary (1996). Sullivan found that these law enforcement agencies have close relationships with universities and as such if police are confronted with the need for technical and expert evidence such as an unfamiliar operating system, police have access to independent and qualified assistance. If and when police encounter problems outside of the capabilities of their own internal staff, it would be necessary to rely upon the expertise of persons who are conversant with these systems to retrieve and retain any potential evidence. Another reason that Sullivan saw for a police and university liaison was the use of vetted and correctly qualified academics as persons who could participate within a panel of experts. The notion of a panel of persons, rather than just one person giving evidence dismisses the potential risk of bias stemming from any long term association with the police and therefore negates any possible allegations of corruption. Sullivan therefore recommended that a similar relationship between the police and academia be established in New South Wales.

There are other advantages in maintaining a relationship with academia, such as training and the availability and use of computing equipment. Most of the equipment currently available for the retrieval of computer-based evidence is primarily for windows-based and Macintosh-based equipment. Even though stand-alone personal computers, and therefore potential evidence, are by far the most common and they will make up the vast majority of all retrieval cases confronted by police there are still other operating systems which will require specialist assistance. Some of these systems are Unix and Linux that Universities often possess. Any relationship that the police have with academia would negate the need to purchase this type of equipment. A relationship between the police and academia could also be beneficial from a training perspective in that specialists from academia could be used. It would be fair to say that the latest technology and training that is available would be an advantage to
the police and, more specifically to criminal investigation. The police could nullify the need to spend public money on costly and constantly changing technology and training expert police witnesses and, in doing so, forsake other projects. It is difficult to justify purchasing, for example, expensive computing equipment in times of fiscal austerity.

2.6 Fraud prevention

Much of the documentation on fraud prevention emanates from the United States of America and, more particularly the large chartered accounting firms. This is evidenced by publications from Arthur Andersen (1997): Managing Integrity Risk, Coopers & Lybrand (1997): Poor Internal Controls Linked to Corporate Underperformance, Deloitte, Touche Tohmastu (1996): Best Practice Guide to the Detection of Superannuation Fraud and KPMG (1997): 1997 Fraud Survey. Perhaps, this is in response to their individual needs and those of their clients. There is, however, a growing portfolio of literature in Australia generated by the Commonwealth Law Enforcement Board and the Australian Institute of Criminology.

Both the public and private sectors, in Australia, are under increasing competitive, regulatory and shareholder pressure to assess and manage their business risks more effectively. In the past, investigators and management have used their skills and resources to investigate financial frauds and illegal acts in retrospect. While this reactive ability continues to be important, investigators and victims of fraud are still heavily relying on this response as the answer to an escalating crime. As such they are continuing to inject the majority of scarce resources into this area. The logical starting point would be to minimise the prospect of fraud occurring and therefore avoid serious damage to their organisation's reputation and shareholder wealth in the first place rather than reacting to the problem after it has occurred. Smith (1998) believes that the logical starting point is education where persons are made to realise and accept the ramifications of their actions while Chisholm (2000) examines the financial and social benefits of implementing fraud prevention programmes. While the concepts
of both authors are sound they too recognise that there are limitations in the implementation of narrow guidelines.

Perhaps the most comprehensive guide for the implementation of fraud prevention programmes has been adopted by the Commonwealth Law Enforcement Board (CLEB) in their Best Practice for Fraud Control Fraud Control Policy of the Commonwealth (1996). The Commonwealth has recognised the futility of past measures to combat fraud and illegal acts and it has developed the necessary measures to effectively minimise this risk. This complete package of anti-fraud practices, that has been developed by the Australian Commonwealth, includes both reactive and pro-active measures and is perhaps the most complete and comprehensive methodology of its type in this country. This document outlines the Commonwealth's requirements for the preparation, evaluation and review of fraud control documents with the sole intention of fraud prevention within Commonwealth Government departments. These same methodologies, espoused by the Commonwealth, could quite easily be adopted by the private sector. These requirements stem directly from the government's decisions on fraud control.

CLEB identifies the need for commitment to fraud prevention at all levels for the protection of the nation's assets. They also claim that this philosophy is more than simply relying on the preparation of documents. At the centre of the Commonwealth's fraud prevention response is the acceptance of the relevance and importance of risk management. On the first page of this document it states that, "...This represents a departure from the traditional reliance upon centrally generated procedures which, if followed uncritically and to the letter, were supposed to protect the Commonwealth from losses through fraud, but in practice, tended to induce a false sense of confidence."

In contrast, the philosophy adopted by the Commonwealth is the utilisation of risk management techniques that they hope will provide their managers with more clearly
defined and identifiable potential weaknesses in their controls, thereby making the most effective use of control mechanisms. CLEB (page 2) believes that this will provide a more flexible fraud control, thereby enabling the adjustment of relevant resource allocations and control mechanisms with minimal administrative costs and disruption. They also recognise that this type of approach necessitates a continuing evaluation of the effectiveness and cost-efficiency of control mechanisms that, in turn will facilitate the review of fraud control arrangements that are required every two years as a minimum. The reasoning behind the need for a review within two years would be on the basis that, as the offence of fraud is constantly changing, there would therefore be a need to review and change the fraud prevention strategies in line with the offence.

The Commonwealth's risk assessment process is a means of examining risk and acting on its findings. As such, it is more than just a bi-annual defined process to which an agency has to adhere. The complexity of the organisational environment and the speed of change means that there needs to be flexibility for management and recognition by them of the iterative and ongoing nature of the risk assessment process and the fraud control response. A major role in highlighting areas of fraud control deficiency rests with both internal and external agency audits and program evaluation. One of the key elements in the Commonwealth's risk assessment process is the development of a methodology for approaching the task. CLEB's methodology is:

1. Capable of being consistently applied across all the agency's programs; capable of providing a supportable rating of the risks of fraud,

2. Amenable to fine-tuning as appropriate, and

3. Capable of being replicated.
The benefit of CLEB's fraud prevention methodologies are, they are capable of adapting to a changing offence and are therefore not restricted. The commercial sector does not appear to share this same commitment to fraud and its prevention.

In Australia, KPMG (1995) conducted a survey examining risk management policies and found that a majority (65%) of Australian companies polled do not have formal risk management policies in place. The Australian Institute of Company Directors (AICD) and KPMG commissioned the survey.

Highlights of the survey include:

1. The survey found that 43% of directors from listed companies indicated their company did not have formal risk policies in place. According to Colin Flynn, a partner with KPMG, this may indicate that "Australian directors are personally liable and financially at risk because of the formal Australian Stock Exchange (ASX) listing rule requirement that annual disclosures on these matter must be made."

2. The areas most frequently mentioned by company directors as the company's top three risks were customer satisfaction, human resource management and information technology. Treasury and fraud were considered the least critical risks.

3. Only 30% of directors adopted a structured and documented approach for managing customer satisfaction compared to about 45% for treasury.

This adverse attitude towards fraud and fraud prevention is not only confined to Australia according to Ernst & Young and KPMG in The Observer (1995). In the United Kingdom, Ernst & Young's fraud unit reports that the number of employers with an explicit fraud prevention policy fell from 59% to 23% between 1992 and 1994 and they suggest that job insecurity is a major cause of fraud. In 1997 KPMG reported that fraud was at its highest point in the eight years since they started keeping records
and, in particular, fraud in the United Kingdom could be worth up to £190 million, excluding the £900 million Barings Bank losses.

In 1997 Louis Harris Associates, for Coopers & Lybrand (1997), conducted a detailed survey on fraud prevention and risk management and the results of that survey, like those of KPMG, reinforced the commercial sector's lack of support for fraud prevention and in some cases, ignorance of its effectiveness. The study surveyed three hundred executives made up of one hundred Chief Executive Officers, one hundred Chief Financial Officers and one hundred middle managers as well as two hundred non-management employees in companies ranging in size from $250 million to more than $30 billion.

It identified that Chief Executive Officers (CEO's) of large corporations in the United States of America overwhelmingly believe that risk analysis and internal controls are critical to the success of their companies. However, this survey revealed that most corporate leaders are not effectively controlling risk, nor are they leading others in their companies to do so. The report found that most of the senior executives who were surveyed had an outdated view of control and that they did not fully appreciate its link to corporate performance. They also seemed unaware that their own attitudes had permeated their companies, appearing far more sanguine than any other group in the survey about the efficiency of their control practices. The survey indicated that employees are not being taught how to identify risk and that they had little incentive to report risk or wrongdoing once they found it.

While nine out of ten senior executives who were surveyed agreed that effective internal controls were critical to effective management, most were also confined to a very narrow definition of the term "internal control." More than half of all CEO's, fifty-six per cent, believed that a "clean audit" equates with sufficient internal controls. A "clean audit" is accounting jargon for an external audit that reports that a client's financial statements are presented fairly in accordance with generally accepted
accounting principles. In reality, though, a clean audit will not guarantee that even financial reporting controls are effective. According to Arthur Andersen (1997) an effective internal control structure should go beyond financial and accounting issues to encompass many other measures of soundness, including adherence to laws and industry standards, strict internal ethics policies and honesty in dealing with customers.

Page three of the survey also revealed that the majority of senior executives interviewed, eighty per cent, agreed that even though most companies stress internal control, "when it comes down to compensation, making the numbers is what really matters." The survey suggests that too many senior executives fail to realise that they must set the right tone at the top. When staff views CEO’s as not leading by example it is easy for employees to regard internal controls as an impediment to productivity, and to jettison them in a misguided effort to “make the numbers”. Arthur Andersen (1997) reinforces this point however they go one step further by adding that when a CEO does not lead by example and does not set the right tone at the top it is a possible precursor to internal fraud.

The survey also emphasised that internal controls are directly linked to operating results and that companies with high levels of internal control are more likely to have rapid growth, success in meeting corporate objectives and increasing return on equity which is the triple crown in corporate success. At companies with weak internal control, these qualities are usually scarce. As noted, the study highlighted a wide perception gap between senior and middle management regarding the effectiveness of their companies' internal controls. In almost every aspect of an organisation’s control environment, middle managers and non-management employees were significantly more critical than senior executives about the efficiency of the companies' control practices.
1. While 40% of middle managers say that persons in their companies try to work around internal controls when they are thought to be in the way, only 23% of CEOs believe that this happens at their companies.

2. Only 11% of CEOs believe that the messenger of bad news takes a real risk in their company, but more than one third of middle managers and nearly half of all non-management employees disagree.

3. Middle managers are three times as likely as CEOs to give their companies low marks for monitoring internal controls.

4. Middle managers are twice as likely as CEOs to give their companies low marks for both developing and implementing procedures to deal with risk as well as communicating risks and related controls to employees.

5. Middle managers and non-management employees are three times as likely as executives to give their companies low marks for defining key areas of authority and establishing appropriate lines of reporting.

6. While 82% of CEOs believe they lead by personal example in adhering to their firm's mission and vision, fewer than four in ten non-management employees agree.

From a lack of performance-based compensation, to wide variances in perceived standards of accountability, to poor implementation of control processes, the survey paints an unnerving picture. Executives must learn to see internal controls as proactive and beneficial to corporate growth. Then, effective control must be applied by teaching a common language and utilising an organised approach throughout the organisation and to every area of its core business, including strategic planning, product development and sales. The survey concludes that "...only by adopting such an integrated framework will companies achieve their corporate objectives and enhance profits."
2.7 Summary

This section summarises the implications derived from the literature. The literature reviewed in this chapter covered the topics listed in section 2.1 namely,

1. Fraud issues,

2. The effects of advances in computing technology upon fraud,

3. The impact of the Internet,

4. Investigative issues, and

5. Fraud prevention.

The reasoning behind this division of research topics was that there is very little available literature that incorporates all of these significant issues sought by this research; however, there is a considerable amount of literature specifically written about these individual issues. The investigation of this individual material gave a fragmented but comprehensive summary of the fraud picture. The salient points that came out of the review of this literature were:

1. Literature on fraud discusses risk issues from an industry based perspective such as credit card fraud, superannuation fraud or insurance fraud typified by Deloitte, Touche Tohmatsu (1996),

2. Police do not view fraud as a major concern as expressed by Adam Greycar in Grabosky and Smith (1996),

3. The current law enforcement bodies cannot cope with fraud. See Balduck (1997),
4. The success of previous initiatives and fraud investigations when they are undertaken as a joint operation between the police and corporate sectors. See Baldock (1997),

5. Police do not, cannot and should not take sole responsibility for fraud.

6. It is the police perception that fraud is more an industry problem rather than being a law enforcement problem. See Task Force Choke Report New South Wales Police Service (1992),

7. It is believed that there could be an up-surge in offences such as electronics funds transfers, industrial espionage and telecommunications fraud on a global scale. See Grabosky and Smith (1996),

8. Computing technology has touched virtually every aspect of our lives. See Office of Strategic Crime Assessments (1996),

9. Law enforcement has not kept pace with these rapid advances in computing technology and education while the criminal element has. See United Nations Manual On The Prevention and Control of Computer Related Crime (1995),

10. The future will see an increase in the frequency of computer related fraud offences. See Office of Strategic Crime Assessments (1996),

11. Globally, law enforcement lacks the resources and the training to be able to properly investigate computer-related offences See United Nations Manual On The Prevention and Control of Computer Related Crime (1995),

12. The Internet has made available to criminals a forum for discussion, a medium of communication and a training facility. See Sullivan (1996b),

14. Most large companies do not have a fraud risk control plan. See KPMG (1997) and,

15. The management of these fraud risks, from a proactive planning perspective, is the preferred course of action. This would involve the compilation and analysis of data from both government and non-government sources. See Grabosky and Smith (1996),

The scenario painted by the available literature is far from acceptable and the situation would arguably appear to do more to encourage criminal activity than deterring it. Most of the available literature tends to focus on only individual issues and as a result it provides isolated solutions. The most effective way to address the problem of fraud is to attack the entire problem from a macro perspective while still concentrating on micro issues. The individual fragmented literature does not set clear boundaries on feasible solutions to this predicament apart from literature from the United Nations (1995) and the Commonwealth Law Enforcement Board (1996) and the implementation of the methodologies recommended by this literature is restricted by the same problem of availability of resources. It is the aim of this research to examine the feasibility and the available options that may address this problem of lack of resources.

The areas of fraud that require closer study are the focus of this research. The attitudes of police criminal investigators need to be examined in order to determine their knowledge and attitudes towards investigating computer related offences and in general, the investigation of fraud offences. The attitudes of police criminal investigators also need to be examined with regard to their perceived importance of preventative measures within training for potential investigators.
The needs of stakeholders or victims of fraud need to be examined and then compared to the current service that is provided in the course of traditional criminal investigation. In the process alternatives to the current investigation methodologies need to be identified and alternatives to the current funding of criminal investigation with regard to fraud.
Chapter Three  

THE EVOLUTION OF FRAUD

3.1 Introduction

3.2 History of Fraud

3.3 What Constitutes a Fraud

3.4 Computer Related Crime

3.5 Types of Crimes defined

3.5.1 United Nations definition.

3.5.2 Interpol definition

3.5.3 Other definitions

3.6 Offences

3.6.1 Hacking/Cracking

3.6.2 Software Theft/Piracy

3.6.3 Telecommunications fraud

3.6.4 Credit Card Fraud

3.6.5 Other Related Issues to Computer Crime

3.7 Computer Related Fraud

3.7.1 Computer Related Fraud techniques

3.7.2 Summary
Chapters one and two have provided a description of the environment and situation surrounding the investigation of fraud and given a review of the available literature. The previous chapters have also explained the broad nature and the constantly changing and evolving nature of the offence and suggested that a contributing factor to the pace of this evolution is the advances in computing technology. This chapter follows the origin and evolution of fraud in detail. In the process it defines and identifies those offences that are traditional and those that are new offences that have been generated by advances in computing technology. This chapter also provides insight into the characteristics of these crimes and possible problems that may confront investigators during the course of an investigation involving crimes of this nature.
3.1 Introduction

The offence of fraud has a unique position within the spectrum of criminal activity. Essentially, the offence is committed without violence and usually with more initiative and intelligence when compared to other crimes. This is particularly the case within the area of computer related fraud. This opinion stems from the author’s experience as a detective at the fraud section of the New South Wales Police Service with over sixteen years as a criminal investigator. Many persons who had been arrested for fraud were seen to possess many independent and combined skills in order to be able to commit the offence in the first place. Some of these common trends included some knowledge of accounting principles and practices, an understanding of computers and their methods of operation, an above average level of intelligence and above average people and communication skills. This additional perceived or actual intelligence, arguably, placed these offenders in the upper echelon of criminals.

Again, based on the author’s experience gained during the course of many criminal investigations as a detective, it was quite often heard from a variety of persons that fraud was a so-called victimless crime. However, this is far from the truth. During my investigations of insurance fraud emanating from the Newcastle earthquake in 1989 I witnessed considerable apathy and little sympathy from both builders and householders alike with regard to insurance companies who paid out large sums of money on numerous fraudulent insurance claims. I saw a marked change in attitude when insurance premiums rose significantly in the Newcastle region, notwithstanding the fact that a portion of that rise would have been attributed to an allowance for increased risk. This misconceived perception of fraud as being victimless is an incorrect view. The predominant motivation for the offender is greed as the offender secretly steals, by deception or by dishonesty, the assets of another person or organisation.
According to Snell (1996) fraud is now Australia’s greatest crime, costing every household $2,660.00 each year. Of all crimes it accounts for sixty-nine per cent of total losses to the community and has a national price tag of $13.7 billion or 3.4 per cent of Gross Domestic Product. Snell goes further to say “Fraud has a bigger impact in the community than any other crime”.

A recent KPMG (1997, page 2) study estimated that corporate fraud was costing Australian business about $15 billion a year. The study explains that the State police forces are under-resourced, while companies leave themselves wide open to fraud by not instituting risk management programs. The report concludes by stating,

"...One of the big problems we have is that law enforcement agencies can’t keep up. If you come to me with a problem, unless there are extenuating circumstances it might be six, eight, twelve months before I can put a detective on it ... That’s not providing a good service for the community. It doesn’t receive the economic backing that other crimes do."

3.2 The History of Fraud

Historically, the origins of fraud in Australia, like those of many other Commonwealth countries, stems from the English common law which was implemented at the time of colonisation in 1788. Over time this common law was supplemented by legislation in order to overcome deficiencies. One such deficiency was identified in the basic common law offence involving the theft of property, identified as larceny.

In Vermeesch and Lindgren (1990, page 44) Sir Frederick Jordan, a Chief Justice of the New South Wales Supreme Court, describes larceny as "...a composite thing made up of the taking away of a chattel belonging to another person, coupled with a purpose on the part of the taker permanently to deprive the owner of the property in the thing taken. If such a taking for such a purpose occurs without the consent of the owner and not under a genuine claim of right, the crime of larceny is committed."
Sir Frederick Jordan further stated "...the law of larceny received its definition when society was in a relatively primitive state. The criminal law then protected a man from being deprived of his goods against his will; but from mere cheating he was expected to protect himself. Hence, cheating, itself was not a crime at common law. It followed that if a man were induced to consent to part with his property in goods to a cheat by a deception, however fundamental, a consent of this kind made the taking not merely not larcenous but not criminal. However fraudulently the proposal may have been made by the cheat, there is no larceny if the owner knowingly gave his consent to that proposal."

In order to gain a conviction against an offender suspected of larceny, all eight individual proofs, or elements of the crime, needed to be proven. If only one of those elements was unable to be proven the offence of larceny was not committed. In the case of fraud where the property was obtained by the offender with the consent of the owner by way of some form of deception or trick, the offence of larceny cannot be established.

The first significant development in the law relating to larceny came in 1473 in what was called the Carriers Case (Huntington, 1992). In this case a carrier was hired to transport bales to Southampton but instead he took them elsewhere, broke open the bales and removed the contents for his own use. This person was charged with larceny even though this person had the consent of the owner to take the bales. The offence was eventually proven and the offender found guilty as charged as it was established that the offender had broken open the bales to steal the contents. This case was the precursor for the offence of larceny as a bailee. Another major development in the evolution of fraud offences came in the early fifteenth century when it was established that a servant could be convicted of stealing his master's property even though that servant was given custody of that property with the consent of the owner or master (Huntington, 1992). This decision eventually created the offence of larceny as a clerk or servant.
The issue of obtaining property by trick or deception was confronted midway through the eighteenth century when the offence of false pretences was created as was the new offence of larceny by trick. Over time other deficiencies were identified within the law relating to larceny which eventually saw the creation of offences such as embezzlement in R v Bazely, obtaining a benefit by deception and larceny by finding (Weston, 1987).

3.3 What Constitutes a Fraud?

As discussed in the previous section, the offence of fraud has evolved from the historic deficiencies of other common law offences that could not cope with crimes that fell outside of those parameters. The various States of Australia have a combination of codified law and common law each with their own responses to fraud and each with their own proofs for each offence. For that reason this research will focus upon the modus operandi of the offence rather than individual offences.

The New South Wales Crimes Act (1901) does not have a specific offence of fraud. Rather, the term “fraud” is a generic term that incorporates a number of differing offences where the offender has gained a benefit for himself or for another person through the use of deception. The Macquarie dictionary (1995) defines fraud as “deceit, trickery, sharp practice or breach of confidence by which it is sought to gain some unfair or dishonest advantage.” That definition is broad and it could encompass many situations however, fraud by its very nature is a far-reaching, broad based offence and elements of fraud could be present in virtually every element of human interaction.

The offence of fraud results from a variety of motives, some of which do not always involve financial gain. Fraud can also evolve from a broad spectrum of dishonest, corrupt, deceptive and unethical practices for a wide number of reasons. The types
and ramifications of fraud are vast and complicated and as there are no hard and fast parameters for the definition of fraud as it is often left to the individual circumstances to dictate whether or not the matter is civil or criminal. Nevertheless, fraud can be divided into two categories: real fraud and constructive fraud.

In the Detective's Education Programme, (New South Wales Police, 1994, page 31) real or actual fraud is defined as "...an act or omission committed by a person with the fraudulent intention of committing what that person must have known to be a fraud". This category of fraud would include traditional offences such as the various larcenies, embezzlements and forgeries as well as scams committed by tricksters. This category would also include the offences in the fast-growing arena of cyberspace that has emerged as the new frontier for scam artists (Babin, 1996). There are approximately 15 million Internet users in the United States alone and this number is increasing each month. The largest commercial online services are estimated to have more than five million subscribers in the United States. All of these online users are potential targets from the scam artist's point of view.

According to Lawrence (1996) the same things that have aroused the attention of law enforcement bodies in the past in traditional print and broadcast media have now emerged within the area of the Internet. Actual or Real frauds would include such things as questionable online advertising overstating claims of product effectiveness. Examples of this type of offence include:

1. Overstated claims such as cures for obesity, cancer or other illnesses;

2. Use of exaggerated titles to describe an investment opportunity can indicate a scam;

3. Exaggerated claims of potential earnings or profit;

4. Claims of inside information with regard to cheap stocks promising high returns and
5. Promotions for exotic investments such as ostrich farming, gold mining, or wireless cable TV.

Constructive frauds are acts or omissions that could be construed to be against the best interests of the general public. This fraud may not involve the loss of property but could include corrupt commissions and those matters that include deception, for example police accepting bribes.

As most frauds are committed against corporations rather than individuals, perhaps an easier interpretation of fraud is that developed by Arthur Andersen (1997, page 15) who places fraud with the following categories.

Employee Fraud

Where employees, customers or suppliers individually, or in collusion, perpetrate fraud against the company, resulting in financial loss or the loss of resources.

Management Fraud

Where management and/or employees issue misleading financial statements with intent to deceive the investing public and the external auditor or engage in bribes, kickbacks, influence payments and other schemes for the benefit of the organisation.

Illegal Acts

Are offences that involve willful violations of laws or governmental regulations, or put simply, breaking the law. Illegal acts should be broadly constructed to include, for example, violations of environmental laws or securities regulations, but should be restricted to those that are integrity related. Illegal acts committed against the organisation by third parties, for example, organised criminals, are also included within this category.
Unauthorised Use

Involves the use of the organisation's physical, financial, information and other assets for unauthorised or unofficial purposes by employees or others resulting in loss of competitive advantage.

These categories, together with an additional category of External Fraud, will be the thrust of this research and their use is merely to simplify the issues surrounding the offence. External fraud includes those same offences committed against a corporation with the target being the resources of that organisation. The aim of this research is to determine whether or not current and traditional law enforcement has the ability and the resources to effectively address these offences to the satisfaction of the victims of this crime.

3.4 Computer Related Crime

The purpose of this section is to establish the nature and definition of computer related crime and the relationship and the impact that this offence has on the traditional offence of fraud and the investigative responses provided by law enforcement.

History has provided a number of examples of new technology that has been introduced with the initial intention of making our lives easier. As is so often the case, the intention of the user determines the outcome and in the case of computer technology the potential for criminal activity was quickly ascertained. In 1943 Harvard University switched on the Mark I digital computer and as soon as 1958, the first recorded case of computer abuse occurred (Marro, 1995).
3.5 Computer Related Crime Defined

In order to understand how, why and where computer related crime fits into the area of fraud it is firstly necessary that the nature of the offence be defined. According to Hayward (1995) there is a lack of uniformity when it comes to understanding and defining the offence. In some countries, according to Hayward, malicious physical damage to a computer is perceived and statistically recorded as computer crime. The United Nations Manual on the Prevention and Control of Computer Related Crime (1995) avoids defining the crime and admits that attempting to define computer related crime presents a myriad of problems. The International Criminal Police Organization (Interpol) in *Computers and Crime: Functionality and Evidence* (1995) also admits to international confusion in attempting to define computer crime however both organisations do present parameters that can be used as a guideline.

3.5.1 United Nations Definition

The United Nations Manual (1995) highlights the difficulty of an internationally recognised definition. The manual follows the same path as Sessions (1991) by accepting that a computer can be used for “...criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are generally subject everywhere to criminal sanctions. The computer has also created a host of potentially new misuses or abuses that may, or should, be criminal as well...”

The manual admits that there is no internationally recognised definition of computer related crime and to strive for that aim often creates inaccuracies; “...rather, functional definitions have been the norm”. Finally, the manual admits that in relation
to computer related crime "...a distinction must be made between what is unethical and what is illegal..."

3.5.2 International Criminal Police Organization (Interpol) Definition

The International Criminal Police Organization (Interpol) in Computers and Crime: Functionality and Evidence (1995) also identifies that "...confusion exists as to what constitutes a computer crime..." and "...there are many different definitions..."

The problem at present is that all countries have their own penal laws and codes and for that reason it is difficult to prepare a common definition that will suit all countries. In trying to identify various computer related crimes Interpol acknowledges that these crimes can be identified "...where the computer itself is the object of the offence" and "...where a computer is used as a tool or an aid to another crime such as theft or fraud."

3.5.3 Other Definitions

A more comprehensive attempt to define computer crime is found in Computer Crime: A Crimefighters Handbook (Icove, Seger and VonStorch, 1995), International Handbook on Computer Crime (in Sullivan, 1995b) and the 1992 ACARB Profile of Computer Abuse in Australia (Kamay, 1992). The first categorises computer crime according to the type of attack on the system rather than other categories such as, according to who commits the offence or how they were committed. This interpretation identifies, not only, the difficulties encountered in defining computer related crime, but also, the confusion as what is and what is not included within this category of crime.
In the *International Handbook on Computer Crime* (1995) there are three categories that give a broader explanation of the variety of computer related offences. These categories and sub-categories are:

**Category One**

*Computer Related Economic Crimes.*

a. Fraud by computer manipulation, for example, an employee of a business who alters records to disguise the theft of money by that person.

b. Computer espionage and software piracy.

c. Computer sabotage, such as the American use of a virus to disable the Iraqi air defence systems prior to Operation Desert Storm.

d. Theft of services.

e. Unauthorised access to data processing systems and hacking.

f. The computer as a tool for traditional business offences.

**Category Two**

*Computer Related Infringement of Privacy*

a. Use of incorrect data. The alteration of stored information such as that which is kept in Government and non-Government agencies. That information is only valuable while it maintains its reliability and accuracy. Consider the ramifications of altered data held by the Australian Taxation office, the Credit Reference Association or the Department of Social Security.

b. Illegal collection and storage of correct data.
c. Illegal disclosure and misuse of data. Examples being the sale of information from the NSW Police computer systems and the Department of Motor Transport which was highlighted by the ICAC investigation in 1992.

d. Infringements of formalities of privacy laws.

Category Three

Further Abuses

a. Offences against the State and political interests.

b. The extension to offences against personal integrity.

The Australian Computer Abuse (ACARB) Definition

ACARB has produced possibly the simplest approach to defining computer crime in Kamay (1992) in the *1992 ACARB profile of Computer Abuse in Australia*. The principles of this definition are the same as those later embraced by the Organisation for Economic Co-Operation and Development (OECD) back in 1983 and identified in ACARB’s publication when it defined computer crime as “...any illegal, unethical or unauthorised behaviour involving automatic data processing and/or transmission of data.”

ACARB defined computer abuse as “…theft, fraud, embezzlement or damage related to computers…” and it includes;

a. Unauthorised manipulation of computer input and or output;

b. Unauthorised access to the system through terminals or micro-computers;
c. Unauthorised modification or use of application programs, operating systems or computing equipment;

d. Trespass on data processing installation, theft of equipment, files or output;

e. Sabotage of computer installation equipment, files, application programs or operating systems and;

f. Unauthorised data interception.

Essentially computer crime can be viewed as either the computer being the target of the offence, such as the destruction of data or, the means by which the offence is committed such as the unauthorised access to a system for the purpose of the theft, deletion or alteration of data. The purpose of these actions can be for either unethical or criminal reasons. However regardless of these distinctions and the apparent confusion over defining the crime, a new generation of crimes have emerged that have to be successfully dealt with by law enforcement.

Considering the complex nature of the crime and the computing equipment (United Nations, 1995) does the current computing environment lend itself to criminal abuse?

3.6 Security Problems with Computers

The very nature of computing assists criminals according to Kamay (1992) and the Australian Computer Abuse Research Bureau (1992). According to ACARB some of the features that give rise to this susceptibility are:

a. A computer will execute all given instructions no matter how illegal.
b. It is difficult to anticipate what a computer is doing with the data that it holds.

c. Because of the speed of a computer, infiltration of the operation can be carried out equally quickly.

d. Whatever security systems have been implemented, certain persons must have unlimited access to it.

e. Haphazard key presses can be accepted by a computer thereby giving access to the user.

f. Because of a computer's accuracy and speed, the results from the computer are more readily believed than if that same information came from another source.

g. A computer often allows an offender to commit a crime in complete anonymity.

h. If an offender instructs a computer that they are a particular person, by using another person's password or features, it will assume that you are that person and allocate to them all of that person's individual rights.

i. Many persons in upper management are not as computer literate as subordinate staff and, hence they do not understand the intricacies of computer security.

Computers have a crucial role to play in virtually every aspect of our existence in such complicated matters as the dissemination of data, banking and financial transfers of funds, air traffic control, business records and accounting procedures to name but a few. Computers also play a dominant role in areas such as word processing, small business databases and overall office administration which is the playground of the potential fraudster.
We can only imagine the capacity and the horizons for the current and the future development of computer technology. But, with the affordability of personal computers, the simplification of computer languages, the increasing skills of computer users and the availability of information via the Internet it is inevitable that our dependence on computers will only deepen, thereby increasing our vulnerability.

In 1995 a newspaper article Anon (1995) reported that a Federal public servant Peter Mackay, was sentenced to nine months jail after he illegally accessed confidential records at the Attorney General’s Department while employed as that department’s computer programmer. According to this article Mackay removed sensitive material using a number of password-cracking programs and then leaked this information on to the Internet. Mackay’s excuse was his concern for the lack of security of this information and he claimed that it could have quite easily been accessed externally.

On the 12 March 1996 the author was contacted by a person purporting to be Peter Mackay, a former Commonwealth public servant recently gaol for the unauthorised access and theft of confidential data relating to the operations of the Australian Security Intelligence Organisation. This person spoke about his trial and more importantly the lack of knowledge of, not only the Australian Federal Police, but also the presiding judge who he claims, “...made it clear that she did not know the difference between a data file and a program.” Mackay went further to say that when he was in prison “...I met some real criminals and I felt that once computer literacy spread a bit further and software such as Visual Basic and AppleScript became even more powerful and user-friendly, then the honest citizens of cyberspace, who feel comfortable with a password such as ‘secret’ or ‘ozemail’ might have reason to fear these gentlemen, and that the justice system had best pull its socks up ...

As highlighted by Johnston (1991), “The scope of computer related crime is restricted only by the ingenuity of the criminal.”
3.7 Offences

In this section those offences that have been created as a result of the advances in computing technology are identified and defined. Computers and computing technology is well within the financial reach of most citizens and for that reason it comes as no surprise that computers are becoming associated with crime. “Computers are becoming tools for criminals to use in the same way as other devices such as firearms and motor cars.” (Interpol, 1995).

Computing technology has generated new offences such as hacking/cracking, cellular telephone cloning, telecommunications fraud and telephone phreaking. It has also added a new dimension to a number of traditional offences such as embezzlement, credit card fraud, larceny, homicide, paedophilia and the supply of illicit drugs. The basis for this is that the vast majority of criminals, households, businesses and potential victims, possess computing equipment and therefore electronic information and evidence. Electronically stored evidence is becoming more prevalent and therefore criminal investigators will be confronted with a number of technology based issues in the process of securing evidence in the course of any investigation (Christy, 1992).

As personal computers are used in almost every aspect of society, traditional offences such as murder, extortion and drugs could be expected to be absorbed into the realm of the computer merely due to the fact that vital evidence could be stored on a computer and therefore be required to be retrieved and admitted into evidence by investigators.
3.7.1 Hacking or Cracking

Hacking or cracking are terms used where computer systems, such as databases, are accessed, usually from a remote location, without consent and authority and information is either copied, stolen, altered or erased. Interpol defines hacking as “…the action of gaining unauthorised access to a networked computer from a remote source. Access is usually gained by either breaking or by-passing the security features of the computers…”.

An example of the potential for this offence was a physical attack upon staff at the Iranian Embassy in Canberra by terrorists in 1994 and reported by Miranda (1994). An investigation was initiated by the Australian Security Intelligence Organisation (ASIO) and the Defence Signals Directorate (DSD) after it was alleged that a foreign power sabotaged a computer system with the Department of Immigration. Information was received of a possible high-level computer breach that lead to valuable computerised information on the movements of suspected terrorists being erased. Moments before investigators could access this information held on a database at the Department of Immigration that information was accessed and erased.

Databases of confidential information are maintained within both the private and commercial sectors and the value of this information is its accuracy and reliability (Hayward, 1995). If these databases and information were accessed and altered the consequences could be catastrophic (Babin, 1996). For example, if the New South Wales criminal records system (COPS), was compromised and criminal records were either deleted or they were created without basis it could mean that previously law-abiding persons could have a criminal history created about them without their knowledge. Worse still, a habitual criminal could have that person’s criminal history deleted thereby giving that person the status of an honest person. It would be difficult
if not impossible to determine who was a criminal and who was not and this could lead to further complications within the criminal justice system.

3.7.2 Software Theft or Piracy

As the cost of computer hardware continues to decrease, the importance and value of the computer software increases (Coldwell, 1993). Software is the set of instructions that tell a computer what to do and how to do it. It is created and owned by persons who expect the users of their creation to pay through a licensing agreement for that right to do so.

Software theft, which is commonly called software piracy, is defined by Lawrence (1996) as "...the unauthorised use or illegal copying of computer software. This can take many forms such as commercial counterfeiting, deliberate and unauthorised copying by dealers, unlicensed copying and plagiarism by competitors." Morrison (1990) states that there are few individuals who can honestly say that they have never used a program for which the developer has not been properly compensated. Morrison (1990) advises us that in commerce, education and Government departments there is mounting evidence of mass copying of software. Large-scale piracy became a recognisable phenomenon with the demand and availability of affordable personal computers and, ever since, the producers of software have battled to stem the flood of illicit copies of their product which is running into the millions, if not, billions of dollars (Fleming, 1993).

3.7.3 Telecommunications fraud

According to Andrews (1991) telephone fraud is reaching epidemic proportions, with some companies receiving telephone bills for hundreds of thousands of dollars in bogus calls. He states that stolen credit cards and line tapping are old techniques that
have been adapted to new uses which involves cracking into switches and PABX exchanges.

According to Rami Abuhamed, an independent consultant, and until recently executive director of the Communications Fraud Control Association in McLean, Virginia, USA, telecommunications fraud is by far the largest segment of communications fraud. He identified the problem behind this crime by stating, "You have all this equipment just waiting to answer your calls, and it is being run by persons who are not in the business of securing telecommunications."

Mitsubishi International Corp. reported losing $US430,000 in 1991, mostly from calls to Egypt and Pakistan. Procter & Gamble Co. lost $US300,000 in 1988. The New York City Human Resources Administration lost $US529,000 in 1987. And the Secret Service, which investigates such telephone crime, says it is now receiving three to four formal complaints every week, and is adding more telephone specialists Andrews (1991).

Australia, like the rest of the world, has readily embraced the technical revolution within the area of telecommunications. Primarily, telecommunications fraud involves an offence where unauthorised access to computer systems is gained to enable the offender to avoid payment of telephone charges, usually international calls, and to avoid telephone charges in order to gain access to other computer systems to obtain other information. According to the Cellular Telecommunications Industry Association (CTIA) in their publication *Building the Wireless Future* (1996) in the United States of America this type of offence includes;

a. Cellular phone fraud where the computer chip in the cellular phone is re-programmed so that the user may remain anonymous and therefore avoid payment.

b. Toll fraud where free international phone calls are obtained.
c. Cable television fraud where free access is gained to user pay television.

d. PABX fraud

e. Voicemail fraud where access is gained to confidential messages.

The CTIA estimates losses in both the United States of America and Canada to be in the vicinity of $9 billion per year. This report claims that there are close links between telecommunications fraud and other offences such as narcotics trafficking, credit card fraud, money laundering, organised crime, commercial espionage, smuggling and the illegal arms trade. The basis for this claim revolves around the desire by criminals to avoid having their actions monitored and detected by law enforcement agencies who have access to facilities for the interception of cellular and normal phone lines.

3.7.4 Credit Card Fraud

Prior to the year 2000 Olympic Games held in Sydney the United States Secret Service warned Australia that it was a target for a massive international counterfeit credit card operation (Warnock, 1994). They believe that Australia was tested in preparation for the 2000 Olympic games and they also expected an upsurge in the use of counterfeit credit cards with the resulting damaging effects on merchants and card providers.

According to Warnock credit card fraud is primarily committed by the offender using lost or stolen cards, counterfeiting cards embossed with another person’s card details or by manufacturing counterfeit cards with the aid of computer generated algorithms. Offenders also gain unauthorised access to computer systems where credit card numbers and identification numbers are stored. These numbers are then used on counterfeit cards.
The Australian Federal Police (1992) have warned the Australian police community of the availability of the necessary equipment on the international market to commit these crimes. They also believe that because of a forty to fifty per cent reduction in crime in the major source of credit card counterfeiting in Asia, Australia will become a target for credit card fraud.

The Internet again provides a vehicle for the dissemination of the necessary software and information with regard to the creation and generation of credit card numbers and counterfeit cards. There are any number of software such as CMaster4 and Credit Wizard freely and publicly available on the Internet and a quick search will locate these programs in a number of sites. What this software does is generate legitimate and useable credit card numbers either from a single legitimate card or by using supplied bank details. Thousands of legitimate credit card numbers can be generated which can then be stored and encrypted using Pretty Good Privacy (PGP) encryption that is part of this software package.

3.7.5 Other Related Issues to Computer Crime

Paedophilia

According to Verreck (1995) paedophilia is a traditional crime that has embraced computing technology, seeing the benefit in the rapid national and international transmission of data. Paedophiles, by their very nature, are reclusive and prone to congregate in trusted circles. It is a consequence of the availability of mass information utilising the Internet, Bulletin Boards and the World Wide Web that those inner circles now spread globally with the widespread transmission of offensive material such as child pornography. By using electronic mail (e-mail) and an
encryption package such as Pretty Good Privacy (PGP) or encrypted File Transfer Protocols (FTP) a paedophile can receive, transmit, exchange and store securely offensive material utilising a global network of fellow offenders.

Encryption

Encryption was, for centuries, held within the domain of government. This was primarily to protect military and diplomatic communications according to Chantler (1994) and Hayward (1995). The main purpose behind the use of encryption is its ability to be able to send coded messages or material that only the recipient is able to read in the event of the message being intercepted. In the past few decades private enterprise has become an increasingly larger user of cryptography to protect its commercial activities. We have now arrived at the point where individuals are going to become major users of cryptography to protect personal information and finances, and their privacy in general, as they become participants in information infrastructures.

The use of encryption software is not a criminal activity however, like many things, it can be used for either legal or illegal reasons. Legal reasons could be the coded transmission of financial transactions and military traffic and intelligence whereas illegal uses could be the secure communications between criminals such as paedophiles, drug suppliers or anyone who wishes to keep their conversations completely private. It is difficult to decipher PGP based encryption, which is freely available on the Internet for anyone who wishes to download it. When this package is used in conjunction with e-mail software, conversations are virtually impossible to decipher (Icove, 1995).
Criminals are only too aware that telephone intercepts have the potential to compromise and incriminate their activities (Interpol, 1995). As a detective the author saw first hand organised criminals, such as motorcycle gangs, use cellular phone numbers for only a brief period of time before disposing of them to avoid telephone intercepts by law enforcement. Using an encrypted e-mail package reduces the risk of conversations being intercepted on the basis that the interceptor cannot interpret the message thereby rendering it worthless.

Encryption packages have another application that could cause difficulties for investigators, in that they can be used to encrypt data that is held on a hard-drive of a computer. What this means is that potential evidence can be securely stored by an offender with a minimal risk that it can be deciphered and therefore used against them during the course of a prosecution. Only the offender is capable of deciphering the data by using a password. Investigators are then faced with a dilemma. They may have correctly used existing hardware/software for the retrieval of this evidence, but, without the assistance of the offender, readable access to that information is difficult if not impossible.

Police have possibly three plausible options when trying to consider how to overcome the problem of passwords to decrypt data according to Sullivan (1996b). Firstly, the government of the day can legislate to provide a coercive solution. This coercive option would force an offender to disclose the password that would unlock potential evidence. If the offender did not comply with that lawful direction, the person would be arrested and brought before a magistrate who would also issue a formal demand for the disclosure of the password. Punitive measures could then be introduced until the offender complies with those lawful directions much in the same way as Contempt of Court proceedings for not answering questions at a Royal Commission.

The problem with this type of coercive policy is that it would be difficult to distinguish between a person who is deliberately not disclosing the password, and a
person who has genuinely forgotten that password. Some offenders would rather be imprisoned as a person who stood firm against the Police as opposed to being imprisoned as a paedophile or rapist.

The second option is where an offender’s common law right of silence is amended. This could be achieved along the same lines as a government amendment to a person’s right to silence in the United Kingdom (New Scotland Yard, 1996). Previously a person’s chosen silence to questions asked by investigators could not be used as an indication of that person’s guilt and no inference can be drawn as to that person’s guilt or otherwise at court by a person exercising that right of silence. At court a trial judge would instruct the jury accordingly. Due to the amendment to this common law right, an inference can now be drawn from that person’s ability and ensuing reluctance to give a reasonable explanation for their actions.

The third option involves concentrating on the most susceptible aspect of the encryption process. That is, when the individual or offender physically types in the password to either encrypt or decrypt data. This option is only realistic when the individual is identifiable. Surveillance technology is such that a miniature camera, linked to a video recorder, could be installed above the individual’s computer. In the process the suspect can be seen to key the password.

As previously stated computer related crimes are many and varied. A computer can be viewed as either the tool that is used to commit the crime, as in the case of an embezzler or a paedophile, or the computer and data stored within it, being the target of the crime, as stated by Sessions (1991). Considering the latter situation, the criminal use of encryption software can be viewed as an aid to the safe storage of computer data and an impediment to the retrieval of this data or evidence. Criminal investigators should have the ability to foresee evidentiary problems in retrieving electronic evidence and as a result should formulate contingency plans to prepare themselves for such a situation. In the absence of proactive responses for the criminal
use of encryption software, potentially valuable evidence, such as accounting records and financial transactions, could be inaccessible and therefore unavailable to prove or disprove a criminal suspect’s activities.

3.8 Computer Related Fraud

Perhaps the area most affected by the criminal use of encrypted software is computer-related fraud. The generic and historic offence of fraud has long been recognised. However, with the widespread use of computerised and electronic storage rather than the more traditional hardcopy ledgers and journals, computer-related fraud has become a more popular term. Regardless, this crime is primarily a new term for a traditional offence. However it has been expanded to include, generally, those offences which have been created due to advances in computer technology because of the affordability of personal computers, document scanners, easy and cheap access to bulletin boards, local area networks and wide area networks such as the Internet. The current generation of offenders also has access to better and more focused education within the area of computing.

The salient difference between fraud offenders of twenty years ago and now is the offender must alter or erase information from a computer system rather than from a hard-copy ledger or journal. Some of the techniques which enable the offender to commit fraud or to cover the evidence trail are, salami slicing, scavenging, trap doors, logic bombs, trojan horses and viruses. Offences that fall still within this category are the traditional offences such as embezzlement and larceny as either a bailee or a clerk/servant.
3.8.1 Computer Related Fraud Techniques

The previously identified difficulties encountered when investigating fraud are made even more complex, when criminal investigators are confronted with a range of freely available software and techniques that are designed primarily to simplify the commission of an offence or to mask the offender's activities. These evolving tools are available via the Internet that provides a forum for offenders to share information, software tools and utilities to enable others to penetrate systems and subsequently to offend. A major factor when proving or disproving an offender's guilt or otherwise is the availability of evidence. By utilising these software tools and techniques an offender is capable of destroying a computer audit trail making it very difficult to obtain the necessary proof which the various courts demand. ACARB in KAMAY (1996) identifies the following techniques that are used by computer criminals in the process of criminal activity. In order to commit elaborate crimes other than by obvious means, an offender must first obtain access to the target computer and information. Once unauthorised access has been achieved the offender can then attempt to perform a number of procedures depending upon that person's motives and goals. An important component of criminal investigation and fraud prevention is understanding and re-creating the commission of the offence with the ultimate goal of developing methodologies to minimise the risk of fraud. The following methods are but a few in a constantly growing range of software tools that are capable of assisting criminal activity.

On some occasions computer programmers deliberately leave holes in the computer program to enable that person to have unauthorised access to what is believed to be a secure operating system and therefore, access to whatever data that the computer system contains. These holes in the program are commonly called Trap Doors and they also provide unauthorised access to the computer system for would-be offenders.
Scavenging is a term for not only the collection of data that has been carelessly left in waste bins, but also the gathering of information which may have been left in various parts of the computer's memory or left on secondary storage devices such as floppy discs. An offender to access the computer system for illegal purposes can then use this scavenged information, for example passwords. A Trojan Horse is a term for a procedure and a program that involves the introduction of "secret" instructions within a computer program so that unauthorised functions can be performed. It could also be described as a program that performs a devious function that is disguised as a benign program, hence the name. A Mockingbird is a program that captures important data by pretending to be a legitimate application. This illegal process can involve the capturing of individual's passwords that can then be used to access confidential information.

There are many types of software that fall into the category of Password Crackers. Primarily this type of program is designed to by-pass computer security by capturing the passwords of legitimate and authorised users. Password sniffers are programs that monitor and record the name and password of network users as they log in, jeopardising security at a site. Whoever installs the sniffer can then impersonate an authorised user and log in to access restricted documents. An example of this type of password cracker is one titled Gobbler. Once loaded, the software can lay dormant waiting to capture passwords that can then be used for unauthorised access and criminal activity.

Once unauthorised access has been achieved there are a number of options that are available to the offender apart from the blatant theft of data or funds. The following are but a small number of procedures in a large range of freely available programs. Salami Slicing is the fraudulent practice of taking only a thin slice, for example only a few cents, from a large financial transaction and amassing those substantial amounts of money for the benefit of the offender. This manipulation of computer data is a procedure that is common amongst offending members of staff and a typical example
would be slicing a small number of cents from either outgoing or incoming funds. If overlooked these small amounts of money are diverted to the offender's account. Over time this small amount of money sliced from transactions can amount to large losses for the organisation.

A *Logic Bomb* is a term for offensive software that is introduced to a computer system by the offender. This software is often triggered by an action or a command at a predetermined time determined by the offender and the final result associated with the detonation of this bomb is usually the destruction of data. Disgruntled employees often use this technique of destroying data to hide their illegal activities. Another form of offensive software that is designed to destroy data and therefore have the potential for hiding the illegal activities of offenders is the computer *Virus*. Viruses are computer programs that interfere with the normal operation of the computer by making copies of themselves. Viruses may vary from a nuisance to the total destruction of the data held on that computer. A search of the Internet can provide tutorials for the step-by-step generation of viruses.

Criminal Investigators are faced with a challenging, if not daunting situation when potentially damaging computer programs and techniques are introduced into an already complex scenario. This complicated situation is exacerbated even further when the Internet is examined, this time, from the perspective of potential obstacles and difficulties in gaining access to information and evidence.

As the name implies, the Internet is a grid of networked international computers. Historically, the Internet is only a recent innovation coming about in 1969 as a small network of four computers belonging to the research and development arm of the United States Department of Defense. This small network known as *ARPANET* grew into *MILNET* and eventually it developed into the Internet. Soon universities, commercial organisations, government agencies, individuals and research facilities adopted the Internet and according to Babin (1996) it evolved into a facility which
spanned 140 countries with approximately 13,300 networks and approximately 2 million addresses.

In the past few years the Internet has seen a huge increase in the number of World Wide Web (WWW) servers. Today the vast majority of large corporations and virtually every university have their own WWW server and many private individuals have their own home pages. With this growing popularity, the security issues concerning the connection of computer systems with their valuable data to the Internet, how investigators develop proactive responses to electronic commerce, electronic mail security and the investigation and retrieval of evidence within these areas are becoming increasingly important.

Traditionally, criminal investigators have relied upon the interception of potential evidence from conversations intercepted on land-based telephone lines and more recently cellular phones. Consequently, criminals are only too aware that telephone intercepts have the potential to compromise their criminal activities (Sullivan, 1996a). According to Babin (1996) electronic mail (e-mail) is progressively becoming the communication media of choice among the corporate, private and government sectors overshadowing the more traditional hardcopy snail mail alternative. Electronic mail is easily accessible, reliable, fast and economically viable. However, its widespread use amongst the traditional victims of fraud creates further evidentiary problems.

As discussed previously in this chapter, when e-mail is used in conjunction with a Pretty Good Privacy (PGP) based encrypted electronic mail package it makes it extremely difficult to interpret the conversation in the event of a lawful interception. If the interceptor cannot decrypt the message the potential evidence is virtually worthless. Attachments to any e-mail message, such as documents or graphics, can also be encrypted and then disseminated globally thereby creating financial and logistical problems in gathering this evidence. Particular groups, such as paedophile
rings or terrorists who disseminate offensive material within their circles and drug traffickers, have been known to utilise this encryption technology. (Interpol, 1995).

3.9 Summary

The ability or inability of law enforcement to respond to the demands of modern investigations has been exposed, in part, by the rapid advancement in technology. Such developments as the rapid advancements in computing technology, the widespread access to the Internet and powerful software have created a perplexing situation for criminal investigators and law enforcement.

According to Babin (1996), society has changed in the manner of its operation in response to the availability of electronic mail, Internet banking and electronic commerce to name a few. Further to this he believes that the criminal community has also adapted to these changes and they have redeveloped their strategies accordingly. According to Jenner (1995), some of Australia's largest companies have been penetrated by organised crime resulting in the theft of tens of millions of dollars. He states that Australian companies could be losing an average ten per cent of their profits through computer fraud and that the international trend towards collusive fraud is being followed in Australia.

The problems that are confronting traditional law enforcement and by extension, the traditional victims of fraud that are identified by this chapter and are part of the focus of this research, are:

1. Are the traditional methods of criminal investigation able to cope with the demands of current and new developments in technology.

2. Will the needs of the victims of fraud be satisfied and,
3. Can law enforcement adapt and change in line with these demands.

4. More importantly, is it physically possible and economically viable to do so?
Chapter Four

THE INCIDENCE AND COST OF FRAUD.

4.1 Introduction

4.2 The incidence and cost of fraud in Australia

4.3 The Perpetrators of Fraud in Australia

4.4 The United States of America incidence and cost of fraud

4.5 The KPMG Survey

4.6 Summary

It has been established in the previous chapters the history of fraud, the evolution of this crime and what options are available to victims and perpetrators of fraud, and the various influences upon this crime such as advances in computing technology. The physical cost of crime and the economic viability of responding to various crimes are major contributing factors that will be addressed in this chapter. This chapter concentrates on statistical data that identifies the cost of this crime in Australia and globally, the identification of possible offenders of this crime together with their methodologies, and the identification of potential victims of this offence. The purpose of this chapter is to highlight the significance and the impact of this crime and to identify any salient trends.
4.1 Introduction

According to Kamay (1992) Australia, like much of the rest of the world, lacks accurate fraud statistics. The lack of statistics appears to be due mainly to the reluctance of victims to come forward and report the matters to law enforcement bodies. This reluctance on the part of victims gives rise to inaccurate information. The examination of the crime of fraud could therefore be divided into two components. Firstly, scrutiny of reported incidents and therefore available statistics from actual crimes and secondly, research and evaluation of those immeasurable fraud offences and incidents that are not reported to law enforcement and are dealt with internally by the victim. With regard to the latter category, the reasons for the reluctance of victim's to report matters to law enforcement, according to the Association of Certified Fraud Examiners (1996) and Sullivan (1996a), appear, in part, to be due to:

1. A desire to avoid adverse publicity that could affect consumer and shareholder confidence,

2. Possible adverse repercussions against management, and

3. A lack of confidence in the law enforcement to effectively investigate the matter.

It is estimated by ACARB that as little as ten per cent of crimes are actually reported to Police. A survey of businesses and clients conducted by Griffin, Rowe and Associates (Stephens, 1990), an Australian legal firm specialising in fraud, reports that up to twenty-five per cent of the workforce, from the Board level down, are actively seeking opportunities to defraud on a regular basis. This survey also reveals that between two per cent and five per cent of the gross turnover that is stolen each year would be a normal fraud factor; it does give rise to alarming predictions. What happens to the unreported incidents of fraud that varies from seventy-five per cent and
ninety per cent of offences? How are they dealt with and how can this situation of unreported crimes be remedied? It would be fair to say that victims of fraud do not have confidence in the traditional remedies to this crime if the available data, relating to low reporting of fraud offences to law enforcement and the high cost to society in general, are to be believed. These issues will be further examined in later chapters.

Smith (1997b) recognises that police services and the judicial system gather most fraud statistics and that there is a considerable difference between these figures and those offences that are not reported.

4.2 The Incidence and the Cost of Fraud in Australia

Most available statistics relating to the incidence and cost of fraud are obtained from law enforcement but unfortunately these reported incidents only represent the number of fraud cases that are actually reported to the police. As a result the available statistical data might not be seen to be representative of the entire fraud predicament. For example, it could be the case that only certain sectors of the government, who have mandatory reporting rules, make up the majority of those fraud offences that are reported to law enforcement. If this was the case certain identifiable crime trends may not provide a complete picture of the true nature and financial cost of the offence.

The Australian Institute of Criminology in Canberra publishes the most accurate and reliable statistics, with regard to fraud issues. In March 1997 the Australian Institute of Criminology prepared A Statistical Profile of Crime in Australia for the Second National Outlook Symposium. This collection of data was created from only reported crimes to each police service in Australia.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Break, Enter &amp; Steal (Total)</td>
<td>356834</td>
<td>360751</td>
<td>366328</td>
<td>347808</td>
<td>359578</td>
</tr>
<tr>
<td>Break, Enter &amp; Steal (Dwellings)</td>
<td>196156</td>
<td>198178</td>
<td>214480</td>
<td>206499</td>
<td>212139</td>
</tr>
<tr>
<td>Break, Enter &amp; Steal (Other)</td>
<td>160678</td>
<td>162573</td>
<td>151848</td>
<td>141309</td>
<td>147439</td>
</tr>
<tr>
<td>Motor Vehicle Theft</td>
<td>120083</td>
<td>121102</td>
<td>130066</td>
<td>131959</td>
<td>131768</td>
</tr>
<tr>
<td>Stealing</td>
<td>526426</td>
<td>527314</td>
<td>540928</td>
<td>536813</td>
<td>596060</td>
</tr>
<tr>
<td>Arson</td>
<td>8538</td>
<td>8623</td>
<td>9648</td>
<td>9889</td>
<td>11361</td>
</tr>
<tr>
<td>Malicious Damage</td>
<td>178466</td>
<td>196966</td>
<td>188018</td>
<td>210338</td>
<td>227223</td>
</tr>
<tr>
<td>Fraud</td>
<td>111029</td>
<td>110493</td>
<td>74999</td>
<td>80970</td>
<td>86130</td>
</tr>
</tbody>
</table>


Table 2 is an aggregation of crime statistics from all of the State and Territorial law enforcement bodies adapted from police annual reports. It must be remembered that this table highlights only those crimes that have been reported to police from 1991
through to 1996. This table comprises of a number of property offences, namely, three categories of break, enter and steal, motor vehicle theft, stealing, arson, malicious damage and fraud. These crimes are grouped on the basis of loss or damage to property only, as would, for example, the grouping of offences against individuals that includes offences such as murder and rape.

From this table it can be seen that there has been a significant decrease in the number of reported cases of fraud, bottoming out in 1993/94 with a marginal rise up to its 1996 level.

This decrease in reported fraud cases could be due to a number of reasons namely:

1. An effective reactive policy conducted by law enforcement;
2. Movement away from fraud offences by the criminal element, or
3. An increase in the proportion of offences that are not reported to law enforcement.

Considering the results from surveys conducted by KPMG (1997) it is possible that this decrease in reported offences is due to an increase in the proportion of offences that are not reported to law enforcement. What gives support to this possibility is further data from the Australian Institute of Criminology, shown in table 3 that indicates a steady increase in the number of reported fraud cases from 1983, in 1987 and 1988.

This period coincides with a number of high profile corporate prosecutions. From that point onwards there appears to be a steady decline in the number of fraud cases reported to the police. Table 3 also provides an indication that there has been a steady increase in the number of fraud offenders between 1983 and 1992 which is in contrast to the gradual decline in reported matters.
Another significant feature of table two is the fact that all of the offences against property, except fraud, have mandatory reporting to the police, a stipulation of the insurance industry. Whilst a serving police officer I had to provide investigative and reporting services to victims of property offences to enable those persons to submit a claim for the loss with their insurance companies. Perhaps a similar insurance initiative for losses due to fraud would overcome the lack of accurate fraud statistics.

Table 3  Criminal Justice Statistics.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud</td>
<td>64 106</td>
<td>80 878</td>
<td>122 779</td>
<td>118 478</td>
<td>111 029</td>
<td>75 278</td>
</tr>
</tbody>
</table>


If the estimate of as little as ten per cent of fraud related offences are reported to law enforcement, as stated by ACARB, perhaps the only true indication of the extent of fraud will be provided by actual surveys of the persons who are reluctant to report the crimes.

In Australia as with many countries in the world, KPMG regularly conducts fraud surveys of the top corporate organisations. The KPMG (1997) Fraud Awareness Survey was sent to one thousand eight hundred of Australia's largest businesses resulting in six hundred and fifty replies or thirty six per cent. Over sixty per cent thought fraud was an increasing problem with estimates of AUD 5 billion lost to corporate corruption in Australia each year.

Forty three per cent of all organisations indicated that they had experienced some type of fraud in the previous twelve months. This Australian figure is significantly below
survey figures obtained by KPMG with regard to the fraud experience of organisation in countries such as the United States of America and Canada who recorded instances of fraud at seventy seven per cent and sixty one per cent respectively.

Another significant result from the survey was that two thirds of the respondents believed that a contributing factor in the escalating future problem of fraud was the increasing sophistication of white-collar criminals. The manufacturing and financial services industries reported the highest average fraud per occurrence at approximately one-hundred thousand dollars with the survey sample reporting losses in excess of $350 million.

Among the study's other findings:

1. Perceptions of corruption overseas were deterring Australian businesses from dealing with certain countries.

2. Respondents listed Asia, Africa and the Middle East generally and Indonesia, Nigeria and Taiwan specifically as countries with doubtful practices.

3. Countries believed to be the least corrupt were New Zealand, Denmark, Singapore, Finland and Canada.

In a global economy these issues increase the risk of fraud and the general ability of criminal investigators to proactively and reactively respond to fraud in an already complex environment.

4.3 The Perpetrators of Fraud in Australia

In order to effectively develop proactive fraud policies it is essential that high-risk groups are identified and targeted together with an analysis of the legal deterrents, with the ultimate aim of minimising the offence. These high-risk groups and the
sentences that the courts have given them have been highlighted in tables 4 and 5. Again, it must be remembered that the data shown in tables 4 and 5 relate only to reported fraud offences and again for reasons identified earlier in this chapter the extent of the statistical analysis of this data must be considered from this viewpoint. Regardless, tables 4 and 5, published by the Australian Institute of Criminology (1997) and the New South Wales Bureau of Crime Statistics publication Proven Offenders in NSW (1996) respectively, give a breakdown of firstly, the age of offenders and secondly, the sentence that has been given to the offender.

Table 4 is a compilation of data that describes the breakdown of offenders who have been apprehended for committing fraud between 1983 and 1994. A salient feature of this table is the identification of adults as the major high-risk group and a noticeable increase in the numbers and percentage of the population that is in contrast to the decline in the numbers of cases reported to the police as seen in table 2. It comes as no surprise that adults are identified as the high-risk group considering that a significant contributing factor in the commission of fraud is gambling. Perhaps another contributing factor could be the levels of indebtedness within this age group. It is worth considering further research examining the current and future ratios of juvenile to adult offenders when computer related fraud is taken into account, given the level of computer literacy of juveniles.
Table 4  Fraud Offenders

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Persons involved (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Change</td>
</tr>
<tr>
<td>Fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Juvenile</td>
<td>1317</td>
<td>1237</td>
<td>1152</td>
<td>1572</td>
<td>2253</td>
<td>1703</td>
<td>61</td>
</tr>
<tr>
<td>Adult</td>
<td>10719</td>
<td>10731</td>
<td>12302</td>
<td>15979</td>
<td>29509</td>
<td>31635</td>
<td>97</td>
</tr>
</tbody>
</table>


1. Data may include persons identified, arrested, cautioned, proceeded against or charged following the clearance of an offence.

Table 5 New South Wales Court Statistics 1996

<table>
<thead>
<tr>
<th></th>
<th>1.</th>
<th>2.</th>
<th>3.</th>
<th>4.</th>
<th>5.</th>
<th>6.</th>
<th>7.</th>
<th>8.</th>
<th>9.</th>
<th>10.</th>
<th>11.</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Breaking and entering</td>
<td>751</td>
<td>131</td>
<td>333</td>
<td>228</td>
<td>251</td>
<td>52</td>
<td>97</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1886</td>
</tr>
<tr>
<td>Fraud</td>
<td>173</td>
<td>65</td>
<td>293</td>
<td>179</td>
<td>528</td>
<td>169</td>
<td>1566</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td>3099</td>
</tr>
<tr>
<td>Larceny by shop stealing</td>
<td>214</td>
<td>40</td>
<td>138</td>
<td>166</td>
<td>253</td>
<td>349</td>
<td>2140</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3611</td>
</tr>
<tr>
<td>Other larceny</td>
<td>540</td>
<td>93</td>
<td>399</td>
<td>396</td>
<td>688</td>
<td>497</td>
<td>2444</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5444</td>
</tr>
<tr>
<td>Unlawful possession</td>
<td>284</td>
<td>49</td>
<td>157</td>
<td>159</td>
<td>286</td>
<td>102</td>
<td>987</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2099</td>
</tr>
<tr>
<td>Vehicle theft</td>
<td>380</td>
<td>82</td>
<td>183</td>
<td>117</td>
<td>185</td>
<td>37</td>
<td>152</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1153</td>
</tr>
</tbody>
</table>

Source: New South Wales Bureau of Crime Statistics and Research

Key


Table 5 compares the punishment of fraud offenders with similar property offenders who have committed offences of dishonesty within the state of New South Wales in 1996. Apart from the offence of fraud there are five other property offences. Utilising
the Detective's Education Programme (New South Wales Police Service, 1994), for a brief summary of these offences and categories they are:

1. *Break, enter and steal.* This offence usually involves the illegal entry into premises and the theft of property from either private or commercial premises.

2. *Fraud.*

3. *Larceny by shop stealing.* This offence is commonly known as shoplifting and it usually involves stealing from retail premises.

4. *Other larceny* involves all other theft of property that does not include violence.

5. As the name implies *unlawful possession* involves possessing property without lawful excuse.


These six property offences have been broken down into eleven categories according to the sentence imposed upon the offender. These categories are:

- Category one is *imprisonment* and it is a sentence that involves permanent incarceration in prison facility for a specified period for adult offenders.

- Category two is *detention in a juvenile institution* and it is a sentence that involves permanent incarceration in prison facility for a specified period for juvenile offenders.

- Category three is *periodic detention* and it involves temporary or periodic incarceration, usually for a specified number of days per week, rather than permanent imprisonment.
• Category four is a sentence of a *community service order*. This sentence usually involves the offender performing a service of benefit for the community for a specified number of hours in total.

• Category five is a sentence of *recognizance with supervision* and it is commonly called a good behaviour bond. With this type of recognizance the offender is monitored by a person appointed by the court.

• Category six, *recognizance without supervision*, is a sentence the same as category five with the only difference being the absence of supervision.

• Category seven is a penalty of a *fine* only.

• Category eight is a penalty of *licence disqualification* and it involves the disqualification of an offender's drivers licence usually in association with another offence.

• Category nine is an order, by the court, for the payment of compensation to the victim of the crime.

• Category ten is a penalty where the offender is sentenced to remain in the court until it is next adjourned or more formally stated, until the *rising of the court*. It is commonly used in juvenile cases.

• Category eleven is a situation where the offender is found guilty of the offence however due to certain circumstances there is *no conviction recorded* and the offender is released.

An examination of table 5 shows a disproportionate number of fraud offenders given custodial sentences together with an unusually high number of non-custodial sentences. Of the 3,099 reported fraud offences only 173 offenders, or approximately 5.5% of the population, were given terms of imprisonment. This figure was the lowest proportion of the six property crimes followed by shoplifting with 5.9% of offenders
receiving a term of imprisonment. The other crimes, in order of the percentage of offenders receiving a custodial sentence were, other larceny 9.9%, unlawful possession 13.5%, vehicles theft 32.9% and break, enter and steal 39.8%.

Table 5 highlights that the preferred punishment of fraud offenders in New South Wales is by way of fine and recognizance with supervision. Over fifty per cent of offenders received only a fine while shoplifting was the only crime that exceeded this proportion where over fifty nine per cent of offenders were fined for their actions. Over seventeen per cent of offenders were placed on recognizance with supervision, the highest proportion.

If imprisonment is designed as the ultimate deterrent to potential offenders or criminals re-offending, there seems to be more importance given to deterring shoplifting by the judicial system rather than fraud. Furthermore, if fraud offenders are released after acts of dishonesty, into their own unsupervised recognizance there seems to be very little in the way of a positive deterrent for offenders or, more importantly, satisfaction for the victims. This issue could shed light on the reason why victims of fraud are not reporting the matters to law enforcement. Perhaps only 14 compensation orders from 3,099 crimes being made by the courts is a further reason for victims of fraud seeing the current judicial solution as unsuitable for their requirements.

4.4 The international incidence and cost of fraud

The examination of the incidence of fraud generally and computer fraud, in particular in the previous section concentrated on data and crime statistics from the state of New South Wales. The results from this data are believed to be typical of law enforcement
and the judicial system Australia-wide. This section compares these Australian responses, where possible, with similar international data in order to determine whether or not the identifiable Australian trends are specific to just Australia or whether the patterns that have emerged in this country are in fact global.

In 1996 the Association of Certified Fraud Examiners (ACFE), an American based association of investigators, compiled the *Report to the Nation on Occupational Fraud and Abuse (1996)*. This report claims the research undertaken by the ACFE to be the largest privately funded study ever conducted on the subject of occupational fraud and abuse. The research analysed two thousand six hundred actual cases of fraud and abuse in the United States totalling $15US billion from four perspectives namely;

1. The cost of occupational fraud and abuse;

2. The Victims;

3. The Perpetrators and;

4. The Methodologies used to commit the crime.

**The Cost of Occupational Fraud and Abuse**

The two and a half-year survey found that:

1. The average organisation in the United States of America loses more than $US9 a day per employee to fraud and abuse;

2. The average organisation loses about six per cent of its total annual revenue to fraud and abuse committed by its own employees;

3. Fraud and abuse cost United States organisations more than $400 billion annually;
4. The median loss per case by males is about $185,000 and by females about $48,000.

The Victims

The victims in this report are organisations and not persons. The salient features are:

1. The most costly abuses occurred in organisations with less than one hundred employees;
2. The education industry experienced the lowest median losses, and
3. The highest median losses occurred in the real estate financing sector.

The Perpetrators

The report gathered personal information on employees, managers and executives who committed occupational fraud and abuses. The findings indicate;

1. The typical perpetrator was a college educated white male;
2. Men committed nearly three fourths of the offences;
3. Median losses caused by men were nearly four times those caused by women;
4. Losses caused by managers were four times those caused by employees and;
5. Median losses caused by executives were sixteen times those of their employees.
The Methodologies

These occupational fraud and abuses were divided into three main categories on the basis that most common offences fall within these three groups. These categories are:

1. Asset misappropriation
2. Fraudulent Statements
3. Bribery and Corruption

Summary

While the similarities between the Australian and the United States surveys are no way conclusive, there are a number of identifiable similar findings between this survey and those conducted by the New South Wales Bureau of Statistics, the Australian Institute of Criminology and the author, highlighted in tables 4, 5, 6 and 7. These are that the financing sector is identified as the most likely victim, males being identified as the most typical perpetrator and females being the least likely group to offend. Perhaps examining the offence of fraud from a global perspective could reinforce these similarities.

4.5 The KPMG Survey

According to KPMG, the forecast for fraud and corporate honesty is pessimistic with more than half the companies responding to an international fraud survey believing that global fraud will be an increasing problem (KPMG, 1996).

KPMG conducted an International Fraud Survey, which looked at nearly four thousand mostly large companies in eighteen countries in North America, Europe,
Australasia, Africa and Asia. However, while the global outlook is gloomy, in
Australia and New Zealand respondents were more optimistic with the majority
believing the level of fraud would stay the same. At the other end of the scale, eighty
four per cent of respondents from Africa and eighty per cent from Hong Kong expect
fraud to increase.

KPMG believe that the reasons for the various attitudes are due to regional
differences. They state that in North America and in Africa, respondents appeared to
feel that the rise in white-collar crime was directly related to worsening economic
pressures. In other parts of the world such as Hong Kong, the Middle East and Asia,
Europe and Australasia, a weakening of society's values was the prime reason given.
A third reason commonly given was the increasing sophistication of criminals.

The survey revealed those companies worldwide believes and is aware that fraud is a
serious problem. Over half the respondents indicated that they were aware of at least
one occurrence of fraud in their organisation in the past year. This awareness was
highest in Africa, where seventy nine per cent of respondents were aware of fraud in
their organisations. In Australia, forty three per cent of respondents indicated they had
experienced some type of fraud in the past twelve months.

Worldwide, KPMG found that the most common types of fraud by employees and
company management were kickbacks, purchase of items for personal use,
falsification of financial statements and misappropriation of cash. Common fraud by
external persons included false representation, patent infringement, false invoice and
secret payments such as bribes and commissions.

KPMG found the most common forms of management fraud were expense account,
purchase for personal use, and theft of inventory. With employees the most common
forms were theft of inventory, petty cash and purchase for personal use. Theft of
inventory, false invoices and cheque forgery was most common for external fraud. In
the international survey, fraud detection was mainly through internal accounting controls and specific investigation by management.

One of the recommendations arising out of the KPMG survey was that companies should examine the kinds of risks to which they are exposed, and make sure that their internal control procedures are effective. The importance of fraud prevention was emphasised and proactive measures such as training courses in fraud prevention and detection, increased budgets for internal audit, staff rotation policies, increased focus of senior management on the problem and investigative reviews were identified.

KPMG highlighted the fact that many companies failed to recognise or ignored what they term *red flags* that often imply the existence of fraud. These include:

1. Staff living above their means
2. Staff propensity to gamble
3. Dubious accounting entries always adjusted when queried
4. Warnings by external auditors
5. Repetitive inventory shortages
6. Complaints from customers

The salient feature of this survey and report is the fact that the commercial sector has become active within the area of fraud. It could be argued that they have assumed some of the responsibility for the investigation and mitigation of fraud, possibly stemming from issues such as non-reporting of offences, and a lack of confidence in law enforcement and the judicial system as a remedy. By extension this places them either in direct competition to the traditional option of law enforcement agencies or a viable alternative and supplement to traditional criminal investigation.
4.6 Summary

This chapter concentrated on statistical data that identifies the impact and cost of this crime in Australia, the United States of America and globally as well as the identification of possible offenders of this crime together with their methodologies and the identification of potential victims of this offence. The tabulated data relating to Australian, United States and global fraud offences portrays a trend away from the traditional responses to fraud, namely, law enforcement. Tables 4 and 5 portray what appears to be a decline in the number of fraud offences. Table 6, which depicts similar data from the reported fraud cases in the United Kingdom, shows a similar trend.

<table>
<thead>
<tr>
<th>Table 6</th>
<th>Recorded Crime/Notifiable offences in the United Kingdom from June 1993 to June 1997</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud and Forgery</td>
<td>167</td>
</tr>
</tbody>
</table>

Source: Home Office Research and Statistics Directorate United Kingdom

Table 6 identifies the reported cases of fraud in the United Kingdom from June 1993 to June 1997. The noticeable decline in the number of fraud cases reported to law enforcement is comparable to the Australian data compiled by the Australian Institute
of Criminology. Perhaps the non-reporting of fraud offences is not typical of the Australian environment but more accurately an international trend.

If the research undertaken by ACARB, revealing that as little as ten per cent of offences are reported to law enforcement, is accepted and, therefore, the data relates only to possibly a small percentage of the overall crime, perhaps the only method of gauging the full extent of fraud is by way of anonymous questionnaire and survey. It is difficult to establish the true extent of fraud from victims of fraud who are reluctant to publicise the fact that they have been affected by this crime. This practice would negate the problems of exposing an organisation's inadequacies, possible shareholder backlash and drop in consumer confidence, issues which have been identified as reasons for non-reporting of offences. In order to obtain a clearer picture of the total issues in responding to fraud it is necessary to measure the public cost of providing the services of law enforcement.
Chapter Five - THE COST OF POLICING FRAUD

5.1 Introduction

5.2 The Cost of policing and the current success of reactive measures

5.3 The Sullivan Report

5.4 Investigative Issues to Consider

5.5 The level of computer skills within the New South Wales Police Service

5.6 New South Wales Police officers attitudes to computer related crime

5.7 The requirements for the retrieval of computer based evidence

5.8 Issues to consider with search warrants.

5.9 Basic steps to consider for the search and seizure of evidence.

5.10 Summary

The previous chapters have established a number of fraud-related issues such as:

- The evolution and social cost of the crime,
- the effects that advances in computing technology have had on this offence,
- the changing face of fraud,
- the new challenges facing law enforcement investigators when investigating new and traditional types of crimes, and
- the types of persons who commit fraud and upon what types of victim.

This chapter examines the financial cost of policing to the community and issues that will question the ability of law enforcement to investigate these types of crime, such as the methodologies that should be considered for the successful search and seizure of computer based evidence.
5.1 Introduction

It is reasonable to ask whether or not the tax payer funded law enforcement bodies, such as the New South Wales Police Service, are minimising and preventing crime in general, as a measure by the success or otherwise of current investigative procedures. Most law enforcement agencies are financed by taxes raised from the public sector or, more importantly, from potential victims of the crime. It should be questioned, specifically in the area of fraud, whether or not the money is being spent to the satisfaction of these victims.

In light of the new investigative challenges that confront criminal investigators that were highlighted in previous chapters, the ability of law enforcement to satisfy the requirements of computer-based investigations must be determined. In order to determine this, the computer literacy and attitudes of law enforcement investigators of the New South Wales Police Service towards the investigation of computer-related offences are examined. After establishing the attitudes of these police together with their level of computer literacy, this chapter then identifies a number of investigative issues involving computers. These are the retrieval of computer-based evidence, the execution of search warrants relating to computing equipment and changes to standard operating procedures for the search and seizure of potential evidence. These routine investigative issues challenge further the capabilities and financial viability of traditional law enforcement.

5.2 The Cost of Policing and the Current Success of Reactive Measures

The predicament that victims of fraud face has been highlighted in a statement made by the New South Wales Police Assistant Commissioner Jeff Jarratt in Seymour (1997) where he says “...the level of fraud is so high police can no longer deal with
the huge number of cases coming across their desks”. He goes further to say “...white collar crime is estimated to have risen by twenty five per cent in the 1995/96 financial year, with New South Wales Police investigating cases valued at $189 million in 1996”.

Table 7 1994-95 Total Police Expenditure in ($'000)

<table>
<thead>
<tr>
<th></th>
<th>NSW</th>
<th>VIC</th>
<th>QLD</th>
<th>WA</th>
<th>SA</th>
<th>TAS</th>
<th>NT</th>
<th>ACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salaries</td>
<td>860910</td>
<td>672249</td>
<td>378509</td>
<td>237306</td>
<td>213999</td>
<td>59160</td>
<td>50961</td>
<td>40715</td>
</tr>
<tr>
<td>Capital Expend</td>
<td>40553</td>
<td>33286</td>
<td>36553</td>
<td>10212</td>
<td>20942</td>
<td>2076</td>
<td>4215</td>
<td>8020</td>
</tr>
<tr>
<td>Total Expend</td>
<td>110093</td>
<td>869839</td>
<td>480895</td>
<td>308299</td>
<td>274944</td>
<td>73178</td>
<td>64743</td>
<td>56279</td>
</tr>
</tbody>
</table>

Table 8 Size of Police Forces 1994-1995

<table>
<thead>
<tr>
<th></th>
<th>NSW</th>
<th>VIC</th>
<th>QLD</th>
<th>WA</th>
<th>SA</th>
<th>TAS</th>
<th>NT</th>
<th>ACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uniform</td>
<td>10645</td>
<td>9078</td>
<td>5340</td>
<td>3662</td>
<td>3616</td>
<td>768</td>
<td>664</td>
<td>533</td>
</tr>
<tr>
<td>Non-uniform</td>
<td>2425</td>
<td>938</td>
<td>950</td>
<td>565</td>
<td>0</td>
<td>304</td>
<td>92</td>
<td>128</td>
</tr>
<tr>
<td>Civilian</td>
<td>2449</td>
<td>1814</td>
<td>1742</td>
<td>849</td>
<td>564</td>
<td>309</td>
<td>192</td>
<td>62</td>
</tr>
<tr>
<td>Other</td>
<td>666</td>
<td>429</td>
<td>188</td>
<td>179</td>
<td>95</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TOTAL</td>
<td>16185</td>
<td>12259</td>
<td>8220</td>
<td>5255</td>
<td>4276</td>
<td>1381</td>
<td>948</td>
<td>723</td>
</tr>
</tbody>
</table>

Sources: Australian Institute of Criminology in a Statistical Profile of Crime in Australia

According to Mukherjee, Carcach, and Higgins (1997) the cost of policing fraud in Australia between 1994 and 1995 was $3,229,100,000 with New South Wales costing in excess of $1.1 billion alone. The individual cost of providing this public service is identified in Table 7. During that same period the Australian Institute of Criminology has identified the size of the individual police forces and these figures are represented in Table 8. It could be argued that this cost and the current strength of each police service would have risen in the years since these figures were published.
Has the public funding of fraud investigations been effective and are the Australian Police Services and more particularly the New South Wales Police Service, too conservative and unwilling to adapt and change to meet new demands in criminal investigation? Recommendations have been made to the New South Wales Police Service suggesting changes to the ways in which criminal investigations are undertaken brought on by the advent of increases in computer technology.


In November 1995, the author was given the task of researching various aspects of computer-related crime that included the retrieval of computer-based evidence for and on behalf of the New South Wales Police Service. The purpose of this research was to explore possible changes to the current methodologies caused by advances in technology. In June 1996 the Sullivan Report was submitted to the State Commander of the New South Wales Police Service and some of the recommendations that arose from this report were:

1. The use of artificial intelligence and computer technology to aid with investigations;

2. Stronger links with the commercial sectors of industry and academia for the formation of a multi-skilled team of computer related crime investigators;

3. The shared financial burden of investigating computer related crime between the public and private sectors;

4. Computer related crime data and intelligence gathering;

5. Various degrees of training of all police with regard to computer crime awareness and;
6. The creation of a dedicated computer crime unit.

With that in mind, this initiative should be viewed as keeping all Police up to date on best practices, which in this case, involves the retrieval and analysis of evidence and the investigation of computer related crime.

At the time of that report the only section within the New South Wales Police Service that had an initiative within the area of computer related crime was the Computer Based Evidence (CBE) Section of the Special Technical Investigation Branch (STIB) based at Zetland. However, it was recognised that CBE was only to be an interim response to this crime. Furthermore, this report emphasised that these recommendations were not just the creation of a dedicated computer crime unit, but more importantly, the education of all Police so that they have the ability to recognise, appreciate, respond and investigate technical crimes. This initiative would have to be implemented with a goal to achieve similar results to the effective introduction of the Breathalyzer technology and the Statewide effect on drink driving, rather than a limited response which could only selectively investigate particular crimes at best.

Sullivan recommended the role of CBE as a technical support unit, providing backup to investigating Police if and when problems arose that were outside of the technical capabilities of the investigators. This role was preferable to CBE carrying the sole responsibility of the retrieval, analysis and investigation of computer related crime for the entire State. If a select technical group was solely responsible for the retrieval and analysis of computer based evidence the State response could be minimal unless there were sufficient numbers of available staff suitably located around the State. This situation would have stretched or even exhausted limited resources.

Some of the problems that Sullivan identified in having one group solely responsible for the retrieval of data as seen and experienced by Scotland Yard are:
1. Technical staff is not available 24 hours per day 7 days per week as is investigative staff;

2. Some operations fall outside of the working hours of technical staff and this may necessitate the use of costly consultants, and

3. Some investigations are sudden and they require an immediate response.

Sullivan identified a number of advantages with having investigating Police shouldering the responsibility of retrieving and analysing their own computer-based evidence namely:

1. The officer in charge of investigating a matter would have the ability to identify all potential exhibits whereas someone who only performs an analysis function would not have that appreciation;

2. The degree of service provided to the business community would be extensive;

3. The training of Police and in particular, criminal investigators was being overhauled at that time and therefore to include suitable training modules would have been timely and cost effective;

4. Technical specialists, such as those attached to CBE, could then perform duties in line with their skills rather than have them attend to matters that could be performed by non-technical persons.

One aspect of the Sullivan Report was implemented, namely the New South Wales Police Working Party on Computer Based Evidence. Perhaps this response could be linked to the attitudes of police identified later in this previous chapter where it was found that police rated the investigation of computer related crime as insignificant when compared to the investigation of crimes of similar impact.
The remainder of the recommendations made by Sullivan has yet to be implemented on the basis of the findings by the aforementioned Working Party. These findings concluded that "...the general consensus appears to be that these matters (computer crimes) come to the attention of police rarely..." and "...there are insufficient numbers of electronic based crimes to warrant training of police personnel generally" (New South Wales Police Service, 1996).

Perhaps the only way that these issues can be resolved is by asking the potential victims of fraud and technology based crimes whether or not they have been affected by any of the previously defined offences and where they believe current crime trends will lead. These potential victims should also be questioned with regard to any possible deficiencies in the traditional investigative methodologies that may effect their decision as to whether or not to report the crime to the police or deal with the matter in an alternative way.

In order to learn about these issues, senior executives from both the government and commercial sectors, as well as police were questioned by way of self-completing questionnaire and personal interview.

5.4 Investigative Issues to Consider

In this section the investigative skills that criminal investigators should possess when attempting to investigate crimes that involve new technology, such as computers, are highlighted and discussed, again from a financial viability perspective. These necessary skills that investigators should possess involve:

1. The application and execution of search warrants relating to computing equipment;

2. The ability to retrieve and analyse computer based evidence;
3. A necessary standard of computer literacy, and

4. A positive attitude towards the investigation of these offences.

In order to examine these issues the investigative procedures of criminal investigators attached to the New South Wales Police Service have been scrutinised in relation to:

1. The level of computer expertise already in existence within the New South Wales Police Service;

2. The attitude of these police towards investigating computer related offences, and

3. The requirements of investigating these crimes.

5.5 The Level of Computer Skills within the New South Wales Police

In June, 1996 a working party on computer-based evidence was formed by the largest law enforcement body in Australia, the New South Wales Police Service, to determine the user requirements in all aspects of computer related crime. This working party was formed on the recommendation of the Sullivan Report (1996) so that investigative issues relative to computer related crime could be examined with the view to establishing a permanent investigative response team. The recommendations of this working party were reported to the Field Training Directorate of the police service and it is this section that has the responsibility for initiating training schemes for police across the State (New South Wales Police Service, 1996).

As a result this working party in conjunction with the Investigative Skills Training Unit distributed a survey to specialist units and conducted a telephone survey with operational detectives from patrols. (New South Wales Police Service, 1996. According to the survey documents, its objective was to determine investigative
frequencies, incident types, skilling needs, computer retrieval skills, information analysis skills, prosecution rates and skills training.

This document revealed that the survey results suggest that there is insufficient electronic based crime in New South Wales to warrant an education package for the majority of police personnel. It is the opinion of the New South Wales Police Service that "...the general consensus appears to be that these matters come to the attention of police rarely and personnel trained at the Special Technical Investigation Branch (STIB) are presently providing assistance. However investigators are experiencing delays as there are few STIB personnel trained in data evidence gathering."

This report states that in the twelve months up to the 16 August 1996 only a small number of specialists and detectives had investigated matters requiring the retrieval of computer based evidence. The spokesperson for this working party then states that "...there are insufficient numbers of electronic based crimes to warrant training of police personnel generally. It should be noted that one patrol claimed to have investigated twenty to thirty telephone frauds requiring the execution of over four hundred search warrants. Expert retrieval of the data was supplied by Telstra and analysed by the investigators, there being no need for internal expert evidence."

The author of this report then recommends that it is unnecessary to train all uniform police and detectives with a computer crime awareness programme on the basis that there is presently insufficient computer crime coming to the attention of the police. Some of the significant features of this computer based crime survey conducted by the New South Wales Police Service are:

1. One hundred per cent of detectives and one hundred per cent of specialists state they do not have the necessary skills to retrieve or analyse electronic data based evidence.
In the past year to August 1996 eighteen per cent of detectives and twenty seven per cent of specialists have investigated one to two matters of computer related crime.

Four per cent of detectives and four per cent of specialists have investigated hacking/cracking.

No detective or specialist has investigated any incidents of cellular telephone cloning, malicious software, credit card software offences or telephone phreaking.

Nine per cent of detectives and eighteen per cent of specialists have investigated fraud offences where a computer is the tool by which the crime is committed.

Thirteen per cent of detectives and thirty six per cent of specialists have investigated other incidents concerning telephone fraud.

No detectives and eighteen per cent of specialists have investigated paedophilia matters.

5.6 New South Wales Police officers Attitudes to Computer Related Crime

In 1995 research was undertaken to establish the attitudes of police and university undergraduates towards a number of similar computer related and non-computer related offences (Sullivan, 1995a). The reasoning for the selection of these two groups was done on the basis that:

1. Police academy students will eventually be this country's future investigators of crime, and
2. University undergraduates from a faculty of business would eventually be involved in business practice therefore placing them in a position to determine the course of action should an offence occur.

The attitudes of these groups towards financial offences and computer related crimes were surveyed to gauge their attitudes towards offences such as:

1. Computer fraud;
2. Credit card fraud, and
3. Hacking or unauthorised access to a computer system.

The findings from this research are highlighted in tables 9, 10 and 11. Table 9 illustrates that police criminal investigators from the New South Wales Police Service believe that computer related fraud is insignificant when compared with a number of similar offences by giving it the worst and most insignificant ranking of greater than ten. This same attitude is depicted in table twelve where credit card fraud is also considered to be insignificant with a ranking of greater than ten. Perhaps the only exception to this overall attitude of insignificance of technically related offences is depicted in table thirteen. This table shows the responses from police when asked whether or not hacking into computer systems is insignificant as a crime. The majority of respondents considered this to be an offence however the question still remains as to whether or not police feel adept at investigating crimes of this nature.
Table 9

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Respondents’ categories</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>University Respondents</td>
<td>Police Academy Respondents</td>
</tr>
<tr>
<td>1-5</td>
<td>10 (5.71)</td>
<td>29 (5.69)</td>
</tr>
<tr>
<td>6-10</td>
<td>59 (33.72)</td>
<td>172 (33.73)</td>
</tr>
<tr>
<td>&gt;10</td>
<td>106 (66.57)</td>
<td>309 (60.59)</td>
</tr>
<tr>
<td>Totals</td>
<td>175 (100)</td>
<td>510 (100)</td>
</tr>
</tbody>
</table>

Table 10

RESPONDENTS' RANKING OF CREDIT CARD FRAUD AGAINST OTHER OFFENCES

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Respondents' categories</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>University</td>
<td>Police Academy</td>
</tr>
<tr>
<td></td>
<td>Respondents</td>
<td>Respondents</td>
</tr>
<tr>
<td>1-5</td>
<td>13 (7.43)</td>
<td>10 (1.96)</td>
</tr>
<tr>
<td>6-10</td>
<td>51 (29.14)</td>
<td>150 (29.41)</td>
</tr>
<tr>
<td>&gt;10</td>
<td>111 (63.43)</td>
<td>350 (68.63)</td>
</tr>
<tr>
<td>Totals</td>
<td>175 (100)</td>
<td>510 (100)</td>
</tr>
</tbody>
</table>

Table 11

<table>
<thead>
<tr>
<th>Acceptance</th>
<th>Respondents' categories</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>University Respondents</td>
<td>Police Academy Respondents</td>
</tr>
<tr>
<td>Acceptable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>112</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>(64.00)</td>
<td>(4.31)</td>
</tr>
<tr>
<td>Not acceptable</td>
<td>12</td>
<td>423</td>
</tr>
<tr>
<td></td>
<td>(6.86)</td>
<td>(82.94)</td>
</tr>
<tr>
<td>Don't know</td>
<td>51</td>
<td>65</td>
</tr>
<tr>
<td></td>
<td>(29.14)</td>
<td>(12.75)</td>
</tr>
<tr>
<td>Totals</td>
<td>175</td>
<td>510</td>
</tr>
<tr>
<td></td>
<td>(100)</td>
<td>(100)</td>
</tr>
</tbody>
</table>

The overall results of this survey indicate that;

- Detectives and police generally as well as university undergraduates consider the investigation of computer related crimes to be of lesser importance than the investigation of other offences that have far less financial and social impact.

This attitude coincides with the results from the survey conducted by the New South Wales Working party on Computer Crime. (New South Wales Police Service, 1996 and Sullivan, 1995).

It is a standard operating procedure within the New South Wales Police Service that criminal investigators should investigate a number of simultaneous investigations in order to achieve maximum results. From the author’s experience as a criminal investigator, rarely if ever, does an investigator have just one investigation at a time. Investigators therefore must give priority to their inquiries. The ramifications of this attitude towards computer related offences could mean that investigations of that nature will be given little importance and priority.

5.7 The Requirements for the Retrieval of Computer Based Evidence

Within the Detective Education Programme at the New South Wales Police Academy police are taught that in all criminal investigations and subsequent prosecutions the most important component in an investigation is evidence. It is this evidence that either proves or disproves a person’s innocence or guilt and therefore the integrity of this evidence must be maintained at all costs. (New South Wales Police, 1994)

According to Sullivan (1996b) the advances in computing technology have brought with them certain complications with regard to the gathering of electronic evidence. Sullivan identifies the fact that with the widespread use of computers both in business and domestically, evidence is now stored on computers rather than in hard-copy
documents. The traditional evidence gathering methods of obtaining a search warrant and seizing evidence by virtue of that warrant have been complicated by such issues as:

1. How does a criminal investigator physically seize electronic evidence;

2. How is the integrity of that evidence maintained so that when it is produced at court it can be established that this evidence is an exact duplicate of the original document;

3. How does an investigator prove that the evidence has not been tampered with;

4. What right does an investigator have to take information that may also be stored electronically on that computer but is irrelevant to the investigation and;

5. What are the legal ramifications of taking a computer system totally when that person may rely upon it to earn a living.

The answer to these questions is the electronic evidence must be retrieved from the computer using universally recognised standard operating procedures that abide by the laws of evidence.

The effective retrieval of evidence is an essential part of criminal investigation regardless of the offence. It has added a new perspective to a number of traditional offences such as homicide, paedophilia and the supply of illicit drugs merely by the vast majority of households and businesses or, potential victims, possessing computing equipment which is capable of storing possible evidence.

According to Sullivan there appear to be two ways of approaching the retrieval and analysis of evidence from computers. One view would be that of technicians who believe that the retrieval of computer based evidence should be left within their control as the standard operating procedures are too complicated.
On the other side of the coin are the non-technical persons. With the present levels of user-friendly technology, the retrieval and analysis of computer based evidence can be achieved on a macro, or large scale, rather than on a micro, or small scale, by using only trained personnel conversant with the operation of the machinery and not its dynamics.

5.8 Issues to consider with search warrants.

Apart from the physical retrieval of evidence, search warrants would have to be one of the most important issues within an investigation regardless of whether or not the offence is computer related. If a search warrant is not obtained in total accordance with current legislation and executed effectively, all other procedures that follow could be jeopardised and, as a consequence, all of the evidence seized in accordance with that search warrant could be deemed inadmissible at court.

Other important issues that should be considered when obtaining a search warrant is the information sworn by police and accepted by the issuing Chamber Magistrate could be later deemed to have been too broad and non-specific. Later scrutiny could reveal that the application and its contents were merely a fishing expedition that hoped to net relevant information and evidence during the course of a mass collection of information. The Detectives Education Programme (1995) emphasises focusing upon individual points of evidence and seizing only evidence that was stipulated in the search warrant.

With that in mind, it is imperative that the wording of the information, in support of an application for a search warrant, should specify all of the potential exhibits. According to the Computer Crime Units of Thames Valley Police (1996), West Mercia Constabulary (1996) and New Scotland Yard (1996) in the United Kingdom,
in most applications for search warrants in order to avoid the exclusion of evidence, it is necessary to highlight the following items when a search involves a computer:-

1. Computer(s) and peripheral attachments.

2. Media, upon which that information is recorded by the computer, such as floppy discs, cartridges, optical discs, tape and the like.

3. Modem.

4. Documents detailing the methods of unauthorised access to computer and such systems.

One possible legislative problem that may need consideration relates to the earlier issue of *fishing expeditions*, which can be remedied by law or rectified by procedures. The current technology allows for a disc image to be created of the *entire* hard drive of a personal computer. At this point in time there isn’t any current capacity for selective imaging. In other words, investigating Police could seize information that they are not lawfully entitled to seize.

An example could be a search warrant executed at a medical practitioner’s surgery relating to medical records for a specific person, which is stored with other patient’s information on a personal computer. The current technology only allows for all of the data to be retrieved, that is, all patients’ medical records. Apart from specific legislation, the only possible solution to this problem could be the culling of unrelated and irrelevant information at some stage of the investigation or judicial process by a delegated authority.
5.9 Basic steps to consider for the search and seizure of evidence

No two searches for evidence are the same and with that in mind it is extremely difficult to formulate standard procedures or methodologies for all types of searches. Most of the innovative issues relative to the investigation procedures for computer related crime have emanated from the United Kingdom and for that reason various Police agencies have been approached for their views with regard to operating procedures. According to information from the computer crime units of West Mercia Constabulary manual (1996), Thames Valley Police manual (1996), and New Scotland Yard manual (1996) some basic steps can be taken to ensure a successful seizure of evidence, such as:

1. Prior to an application to a Chamber Magistrate for a search warrant, investigating Police should already possess a quantity of information with regard to the suspect and the premises to be searched. In addition to that information and well before any search warrant is executed, further intelligence should be gathered with regard to telephone connections and whether or not there is evidence that the suspect could be connected to the outside world via Internet or a bulletin board.

2. As with all search teams, delegate specific duties to individuals such as photographer or video operator, exhibit handler, draftsperson and searchers.

3. Once the suspect premises have been entered ensure that cellular phones are kept at a distance, no unauthorised person touches the computer or the power and the keyboard or alters any function that the computer may be performing. This is to counter any possible booby traps.

4. Photograph, sketch or video tape all of the connected equipment and cables together with a scene of the room.
5. If possible tag each piece of equipment and record exactly how it is connected to corresponding equipment.

6. Tag all of the cables and record how they were connected. This is vital for later evidentiary and analytical purposes.

7. Record any visible messages that may appear on the screen.

At this point of the search it must be determined:-

a) When the equipment can be imaged on-site but it cannot be taken from the premises.

This option covers the situation where an image is taken of the offender’s hard drive however, the machine is vital for the survival of a business for example, and therefore it must be left at the premises due to legal complications and possible litigation. The Master copy of the offender’s computer must be correctly certified and sealed in an evidence bag and this procedure should stop allegations of evidence tampering. A second copy of the hard drive can be imaged and it should be regarded as a working copy for investigating Police. If legal representatives wish to examine these exhibits arrangements can be made to do so at a Police Station or law office, much in the same manner as ordinary exhibits.

or

b) When the system can be imaged on-site and taken from the premises.

This is the preferred option. Not only is the evidence retrieved and certified in an appropriate manner as highlighted in option a), but, all of the offender’s equipment including hardware and software, can be taken and stored as an exhibit and possibly forfeited to the Crown at a later stage. To be able to seize the equipment it must not
be connected with any financial or business activity other than the criminal actions of the offender.

or

c) When the system cannot be imaged on-site and it can be taken from the premises for further analyses.

As previously pointed out, not all computers can be imaged utilising the current technology. Therefore, there will be occasions when the imaging process will not suffice and the machine will have to be seized in accordance with a search warrant and taken for further analyses by specialists. The conditions for seizure are the same as in option b) and therefore, after imaging analyses, it may be subject to a forfeiture order.

or

d) When the equipment cannot be imaged on-site and it cannot be taken from the premises.

An example of this situation would be a networked machine using Linux and also utilised by a business. If and when this scenario arises, specialists would be required to attend to retrieve the evidence.

8. All evidence should then be documented and stored.
Available equipment for the Retrieval of Computer Based Evidence.

Again, depending upon which school of thought one adheres to, there are several hardware/software packages and purely software that is available for the purpose of disc imaging personal computers. At the moment the major options in this field for selection are:

1. Flightserver.
2. Dibs.

Flightserver

This disc imaging hardware/software is manufactured in the United Kingdom by Data Recovery S & S International PLC. It is currently on the market for around $A30,000.00 depending upon the model and specifications and it is a machine which requires a skilled technician to operate. This machine does not appear to be widely used by either law enforcement or statutory bodies. The advantages of Flightserver are:

1. An unlimited capacity for storage of recovered data.
2. Retrievals and searches can be done on-site.
3. It is a complete hardware and software package that does not require any further development of storage media.
4. Flightserver can image more than five machines simultaneously producing efficient use of time on-site.
The disadvantages of Flightserver are:-

1. Even though Flightserver is transportable it is large and requires more than one person to transport it and operate it.

2. The storage media is by way of a Compact Disc (CD) writer that has a reputation for accuracy when used in a stable environment however, it also has a reputation for being fragile and prone to malfunction if mishandled.

3. A high level of technical expertise is required to operate this equipment.

4. It is an expensive piece of equipment.

5. Limited use by law enforcement and statutory bodies means limited exposure to possible legal challenges, in both the civil and/or criminal jurisdictions.

Dibs (Disc Imaging Backup System)

Computer Forensics Ltd manufactures this hardware/software package in the United Kingdom. It is currently on the market for around $A15,000.00 and it is a machine that requires little training to operate by non-technical persons. This equipment is used by almost one half of UK Police Forces as well as statutory bodies such as the British Inland Revenue.

The advantages of Dibs are:-

1. The entire retrieval unit is small enough to be transported by one person.

2. The operation of the equipment is simple enough for non-technical persons to disc image potential evidence.

3. Retrievals and searches can be done on-site.
4. It is a complete hardware and software package that does not require any further development of storage media.

5. The storage media is by way of optical drive and optical disc that are both hardy pieces of equipment. Other storage media are also available.

The disadvantages of Dibs are:-

1. It is an expensive piece of equipment, around $A15,000.00 per unit.

2. Dibs currently has the ability to disc image only Windows and Macintosh-based machines.

3. Optical drive technology is slower than hard drive technology. This means that as hard drives become larger and larger multiple optical discs are required for storage.

SafeBack

Unlike Flightserver and Dibs that are a combination of storage media (hardware) and software, SafeBack is software only. It was developed at the request of the Criminal Investigation Division of the United States Internal Revenue Service and as it is only software it sells at a reasonable price of $US200.00 per copy. The advantages of SafeBack are:-

1. The software is relatively cheap at $US200.00.

2. It is extensively used in the United States by hundreds of law enforcement agencies as well as government agencies such as the Internal Revenue Service (IRS), Federal Bureau of Investigation (FBI), Air Force Office of Special Investigations, Drug Enforcement Agency (DEA) and many others.
The disadvantages of SafeBack are:-

1. It is only software without any storage facility. The responsibility for the development of that storage facility lies with the purchaser. What must also be kept in mind is the need for simplicity.

Once suitable equipment for the retrieval of computer based evidence is selected, training programmes can then be implemented involving those standard operating procedures for the retrieval equipment, on a 3 tiered basis namely Uniformed Police, Criminal Investigators and Specialist Criminal Investigators.

Summary

This chapter has identified:

1. The high cost of policing to the public;

2. The acceptance of the inadequate level of computer literacy within the New South Wales Police Service;

3. The attitude of criminal investigators towards the investigation of computer related offences is cause of concern as they have identified these offences as insignificant when compared with crimes of a similar nature but with far less financial impact;

4. An examination of the criminal investigation of computer based crimes requires a moderate standard of skills in order to physically retrieve potential evidence and it is doubtful whether criminal investigators will possess these skills considering the attitudes of both investigators and the police training directorate, and
5. An examination of the standard operating procedures for the application and the execution of search warrants in relation to electronic evidence identified the need for specialist training that the New South Wales Police Service appears reluctant to provide.

These issues may provide an explanation for the apparent reluctance of victims to report fraud offences however, in order to establish this possibility a survey of fraud victims is required.
Chapter Six  

THE QUESTIONNAIRES AND INTERVIEWS

6.1  Introduction

6.2  The Survey

6.3  The Questionnaires

6.4  Analysis of fraud offenders

Now that the scene has been set describing the various responses and issues relative to fraud this chapter focuses on the questioning of the potential victims of the crime, the investigators of fraud and actual offenders to establish the effectiveness or otherwise of the current fraud investigative responses.
6.1 Introduction

The purpose of this chapter is to provide information with regard to;

1. The objectives of the survey, the questionnaires and the analysis of the case studies, and

2. The issues that were addressed by these surveys;

The observations conducted in the previous chapters have generated a number of questions relating to the attitudes of firstly, law enforcement, particularly the New South Wales Police Service, towards:

1. White-collar crime and financial offences in general;

2. Emerging criminal offences generated by advances in computing technology and;

3. Proactive fraud issues as opposed to purely reactive responses.

Secondly, the commercial and government sectors of the community are surveyed with regard to their attitudes towards:

1. The effectiveness of the current reactive response;

2. The incidence and cost of fraud within their organisations;

3. Offender details, and

4. The needs of the organisation with regard to solutions to fraud.

To determine the attitudes and methodologies of both the police and the victims of fraud it was decided first to evaluate the police responses by way of a self-completing questionnaire and second to obtain the responses from the corporate sector by way of
personal interview. Finally actual fraud cases were analysed to identify actual offender and victim details as well as sentences imposed by the courts for comparative purposes.

In previous chapters it was indicated that the victims of fraud are reluctant to report offences of fraud to law enforcement for a number of reasons that are addressed in the survey questionnaire. For that reason it was decided to approach senior executives within the government and commercial sectors personally to assure these person that their responses would be kept strictly confidential.

6.2 The Survey

The populations for these surveys are the police and the executives in the commercial and governments sectors. The police component of the survey can be further divided into two categories according to the subject of the survey, namely:

1. Attitudes to fraud, and

2. Attitudes to fraud prevention as a component of the Detectives Education Programme for criminal investigators at the New South Wales Police Academy.

The sample size for the survey on attitudes to fraud at the New South Wales Police Academy at Goulburn, New South Wales was five hundred and ten respondents comprising of student police officers and detectives (See Appendix 2). These respondents were temporarily studying at the Police Academy at the time of this survey.

The sample size for the survey, on attitudes to fraud prevention as a part of the Detectives Education Programme, was fifty-one respondents consisting of experienced criminal investigators selected a random from around the State of New South Wales.
Every police station within the State, that had criminal investigators on staff, was sent a self-completing questionnaire (See Appendix 3).

The sample size for the survey of senior executives from the commercial and government sectors was thirty respondents. These respondents were selected randomly and unlike the police respondents, they were each interviewed personally from a pre-determined schedule of questions (See Appendix 1).

Part of this study was undertaken only at the New South Wales Police Academy from recently recruited student police officers and experienced detectives. This institution has its own distinct culture that may have permeated through to the detectives and may have done so with the student police officers. This culture may have influenced the responses from the student police officers in particular, whose academic achievement and behaviour has an effect upon their graduation.

The sample of detectives considering the inclusion of fraud prevention methodologies was comparatively small when compared to the large number of respondents from previous questionnaire. This survey amounted to only fifty-one respondents. Greater confidence could be placed in the findings and conclusions with a larger sample however, considering that every detective's office in the State of New South Wales was canvassed the author has obtained the maximum number of responses achievable.

The sample size of only thirty respondents from the ranks of senior executives from the commercial and government sectors was also comparatively small. Only large corporations and senior executives were interviewed and considering the availability of these persons and their heavy schedules thirty respondents was seen as a realistic and achievable sample.

The questionnaire used for the survey of decision-makers within the corporate and government sectors included a combination of twenty-three questions. Question one was designed to determine the position of the interviewee within the corporation. The
purpose behind this question was to ensure that this person was in a senior position and in a decision-making role which was a prerequisite.

Questions two and three were intended to identify the nature and structure of the corporation so that high-risk industries could be identified. Questions four through to seven established any details of fraud inflicted upon the organisation and this included the cost of fraud to the organisation, the frequency of any offences, the method of discovery and the recovery of any stolen money, if any.

Questions eight through to ten targeted offender details such as employment status and position in the hope of determining the significance of either internal or external fraud risks.

Question eleven and twelve confronted the issue of a small percentage of fraud matters being reported to law enforcement by asking whether or not frauds were reported to the police and if so, why was it reported to the police.

The remainder of the survey focused upon perceptions and attitudes of senior executives to a range of issues that include;

1. The motivations not to report fraud offences to the police;

2. The most important issues when confronted with a fraud offence;

3. Solutions when faced with a fraud offence;

4. Future perceptions of fraud in Australia and the area of concern;

5. Fraud prevention, and

6. Solutions to fraud.
6.3 The Questionnaire

Two questionnaires were developed targeting the New South Wales Police Service with the aims of determining the objectives of this research, namely the attitudes of police to firstly, white-collar crime and secondly to crime prevention. The police respondents were chosen at random and the New South Wales Police Academy at Goulburn was chosen on the basis that large numbers of police from all across the State of New South Wales were studying there temporarily.

The first self-completing questionnaire comprised of fourteen questions and five-hundred-ten respondents at the New South Wales Police Academy at Goulburn completed it. Questions one through twelve were developed in order to determine whether sex, age, educational standard and marital status had any impact upon the responses provided by the police.

The main feature of this questionnaire is question thirteen that asks the respondent to prioritise fifteen offences. The most serious offence, in the opinion of the respondent, was to be given the score of "1" with the least serious offence being given the score of "15". Most of the offences are of a similar nature apart from the crimes of murder, domestic violence and rape. These three serious crimes are violent and emotional when compared with the remaining crimes. It is a clear indication of a respondent's attitude and attention to detail within this questionnaire when the scores for these three serious offences are analysed. They would be given very low scores if the respondent's viewed the offences objectively and not hastily. Police quite often have a number of simultaneous investigations and subsequently it is the intention of this question to determine the attitudes of police with regard to white-collar crimes in the context of priority.

The second self-completing questionnaire comprised of six questions and detectives from forty police stations from around the State of New South Wales completed the
questionnaire. These respondents participated voluntarily and anonymously.
Questions one through four established the rank of the respondents together with the
level of experience and the length of service.

The main feature of this questionnaire is question five that asks the respondent to
prioritise fifteen possible subjects that could be included within the Detective's
Education Programme at the New South Wales Police Academy. The most important
subject, in the opinion of the respondent, was to be given the score of "1" with the
least important subject being given the score of "15". Most of the subjects are of a
similar nature. The intention of this question was to determine the attitudes of
detectives towards proactive or preventative measures in reducing crime. Traditionally
law enforcement has relied upon predominantly reactive measures and it is the aim of
this question to ascertain the acceptance or otherwise of alternative methods.

6.4 The analysis of convicted fraud offenders

In 1995, as a Visiting Research Fellow of the New South Wales Police Academy, I
retrieved a sample of twenty-eight case studies from the New South Wales Police
Criminal Histories computer database. The criteria for this search were based on those
fraudulent crimes that involved the use of a computer as the tool to facilitate the crime
or, the computer was the actual target of the crime. Between January 1992 and
January 1994, only 28 crimes met these criteria. These 28 reported crimes were then
examined to study:

1. The types of persons who commit fraud;

2. The sentence given to offenders by the courts upon conviction, and

3. Details with regard to the victims of this crime.
All of this data was collated whilst maintaining strict confidentiality over the identity and personal details of the offenders. Only sex, age, employment status, compensation orders and the sentence handed down to each offender were identified and then tabulated into tables 36 and 37. As with the tables examined previously in this chapter the details relate to those persons who have been convicted by the courts only in relation to cases that have been reported to the police and therefore the results and trends must be considered with that in mind.
Chapter Seven  THE RESULTS FROM THE SURVEY AND THE QUESTIONNAIRES

7.1 Introduction

7.2 The Results of the Survey of Potential Victims of Fraud

7.3 The Results Regarding Attitudes to White Collar Crime

7.4 The Results Regarding Attitudes to Crime Prevention

7.5 The Results from the analysis of fraud offenders

7.6 Summary

This chapter examines the results from the various questionnaires and surveys conducted with police investigators from the New South Wales Police Service and potential victims of fraud from both the government and commercial sectors. The questions asked of each of these respondents are described and the results stemming from these questions are displayed.
7.1 Introduction

The previous chapters have set the scene describing;

1. The complexity of the various types of fraud;
2. The cost and incidence of fraud;
3. The ability and attitudes of criminal investigators;
4. The effect of advances of computing technology and;
5. Offender and victim details.

Both police and non-police respondents have been questioned with regard to;

1. White-collar crime and financial offences in general;
2. Emerging criminal offences generated by advances in computing technology and;
3. Proactive fraud issues as opposed to purely reactive responses;
4. The effectiveness of the current reactive response;
5. The incidence and cost of fraud within their organisations;
6. Offender details and;
7. The needs of the organisation with regard to solutions to fraud.

This chapter deals with the various responses emanating from these surveys.
7.2 The Results from the Survey of Potential Victims of Fraud

Question One

The significance of this question is to ensure that the respondent holds a decision making position. It was essential to this research that the person questioned is capable of implementing fraud-related issues.

Table 12 The position held by the respondent

<table>
<thead>
<tr>
<th>Position</th>
<th>Percentage</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Executive Officer</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>Chief Financial Officer</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>Senior Manager</td>
<td>21</td>
<td>6</td>
</tr>
<tr>
<td>Middle Management</td>
<td>47</td>
<td>14</td>
</tr>
<tr>
<td>Audit</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Other</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>

Questions Two and Three

This question identifies the sector from which the respondent works, either the government or commercial areas and secondly which industry they represent. Of these decision-makers twenty-one per cent were associated with the Manufacturing industry however the majority of respondents, almost thirty-seven per cent, were employed within the government sector. The remaining industries represented were:
• Education 3 %
• Service 13 %
• Finance 3 %
• Insurance 7 %
• Retail 3 %
• Other 3 %

Subsequently, the proportion of government organisations dominated with forty-seven percent followed by privately owned companies with twenty-three percent representation, publicly owned companies with seventeen percent and other organisations comprising of thirteen percent of the population.

**Question Four**

Question four concentrated upon the number of known incidents of fraud that the companies have experienced in the past five years. The frequency of these frauds are highlighted in Table 13 which shows that the most frequent number of incidents is between one and five crimes and that this classification attracted thirty-seven per cent of interviewees responses. Twenty-seven percent of respondents indicated that they had not incurred any incidents of fraud while nine percent of respondents revealed that they had suffered between six and twenty crimes. The most significant response is twenty-seven percent of respondents indicated that they had incurred more than twenty crimes.
Question Five

Following on from the frequency of these offences, the respondents were asked to approximate the total loss in connection with these frauds. These losses are highlighted in Table 14. Of the thirty initial respondents, eight of those indicated that they had not encountered any fraud in the past five years thereby restricting this sample to twenty-two respondents.

Of those respondents thirty-two per cent indicated that they had average losses between $10,000 and $100,000 and another thirty-two percent indicated losses between $100,000 and $1 million.

Table 13 The Number of Known Incidents of Fraud in the Past Five Years

<table>
<thead>
<tr>
<th>Classification of Offences</th>
<th>Percentage</th>
<th>Number of responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>27</td>
<td>8</td>
</tr>
<tr>
<td>1 - 5</td>
<td>37</td>
<td>11</td>
</tr>
<tr>
<td>6 - 10</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>11 - 20</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>More than 20</td>
<td>27</td>
<td>8</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>
Question Six

Almost forty-one percent of respondents who had incurred losses due to fraud indicated that none of the stolen monies was recovered. Of the remainder of the respondents;

- Twenty-three percent indicated that they had recovered a quarter of the stolen money;

- Eighteen percent had recovered half of the stolen money;

- Four percent had recovered three-quarters, and

- Fourteen percent had recovered all of the money stolen from their organisation.

Table 14  The Approximate total Loss Associated with these Frauds

<table>
<thead>
<tr>
<th>Categories of Loss</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than $10,000</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>Between $10,000 &amp; $100,000</td>
<td>32</td>
<td>7</td>
</tr>
<tr>
<td>Between $100,000 &amp; $1 million</td>
<td>32</td>
<td>7</td>
</tr>
<tr>
<td>Between $1 million &amp; $2 million</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>More than $2 million</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Don't Know</td>
<td>18</td>
<td>4</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>22</td>
</tr>
</tbody>
</table>
Question Seven

Of the remaining twenty-two respondents who had experienced fraud in the past five years, this question asks how the fraud was discovered and the responses obtained are highlighted in Table 15.

When asked how the fraud was discovered thirty-six per cent of respondents indicated that the fraud was found accidentally closely followed by thirty-two per cent of responses indicating that internal audit had found the fraud. No crimes were detected by external audit, investigations uncovered fourteen percent, and whistleblowers found nine percent and other methods detecting nine percent.

Table 15  How the Fraud was Discovered

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Audit</td>
<td>32</td>
<td>7</td>
</tr>
<tr>
<td>External Audit</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Whistleblowers</td>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>Accidentally</td>
<td>36</td>
<td>8</td>
</tr>
<tr>
<td>Investigation</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td>Other</td>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>22</td>
</tr>
</tbody>
</table>

Question Eight

Table 16 highlights the responses for the question whether or not the fraud offender was an employee of the organisation.
The majority of the interviewees, eighty-seven per cent or nineteen out of the twenty-two respondents, indicated that the person responsible for the fraud was an employee as opposed to only fourteen percent being non-employees.

<table>
<thead>
<tr>
<th>Offender Status</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>86</td>
<td>19</td>
</tr>
<tr>
<td>Non-Employee</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>22</td>
</tr>
</tbody>
</table>

Questions Nine and Ten

These questions follow on from the previous question with regard to whether or not the person or persons responsible for the fraud were employees or external persons. The question seeks to classify the position held be the employee at the time of the fraudulent offence.

Forty-five percent of offenders were employed within the clerical or administration sections of the organisation with middle management being responsible for ten percent, sales two percent, senior management twenty-seven percent and other sections fourteen percent.
Table 17  Fraud Offenders Classified by Employment Type

<table>
<thead>
<tr>
<th>Employment Type</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clerical/Administration</td>
<td>45</td>
<td>10</td>
</tr>
<tr>
<td>Middle Management</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>Sales</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Senior Management</td>
<td>27</td>
<td>6</td>
</tr>
<tr>
<td>Other</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>22</td>
</tr>
</tbody>
</table>

Question Eleven

This question is perhaps one of the salient features of this survey as it broaches the subject of whether or not losses due to fraud were reported to the police. Table 18 highlights the responses from these interviewees. Sixty-eight percent of cases were reported to the police and thirty-two percent were not.

Table 18  Whether or not Victims of Fraud Reported the Matter to Police

<table>
<thead>
<tr>
<th>Was the Fraud Reported</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>68</td>
<td>15</td>
</tr>
<tr>
<td>No</td>
<td>32</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>22</td>
</tr>
</tbody>
</table>
Question Twelve

This question asks of the thirty persons interviewed what would be necessary to motivate that person to report a fraud offence to the Police. The responses given by these persons are identified in Table 19. Sixty-four percent of respondents indicated that it was a compulsory policy to report offences while thirteen percent indicated that they would be motivated to report the offence on the basis of having the person punished. Thirteen percent reported the matter on the basis of it being the only course of action known to them and ten percent were motivated by other matters.

Table 19  The Motivation to Report a Fraud to Police

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>To have the Offender Punished</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>Compulsory Policy</td>
<td>64</td>
<td>19</td>
</tr>
<tr>
<td>The Only Known Course of Action</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>Other</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>

Question Thirteen

Table 20 highlights the responses to the question that asks the interviewees to identify the motivation that would deter them from reporting the matter to the police. An overwhelming seventy-seven percent of respondents indicated that the adverse publicity for the organisation would be the prime motivation not to report the matter.
Of the ten options available to the respondents only six attained any score. These were a lack of confidence in the judicial system which scored three percent, lengthy court appearances three percent, loss of control over the investigation seven percent, loss of control over confidentiality three percent and other motivations seven percent. Others such as a possible shareholder backlash, possible dismissal, lack of confidence in the remedies offered by courts and poor sentences did not achieve a score.

Table 20 The Motivation to Not Report a Fraud to Police

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>A desire not to expose your business to possibly adverse publicity</td>
<td>77</td>
<td>23</td>
</tr>
<tr>
<td>A desire not to risk possible shareholder backlash</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>A lack of confidence in the criminal Justice System</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>A desire not to become involved in lengthy court proceedings</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Loss of Control over the outcome of the investigation</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>Loss of Control over the confidentiality of the investigation</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>A desire not to risk dismissal for being held responsible for the fraud</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>A lack of confidence in the remedies offered by the civil courts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>A lack of confidence in the sentences given to offenders in the criminal courts</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>
Question Fourteen

Table 21 highlights the responses to the question that asks the interviewees to identify the most important issue if a fraud had occurred within that organisation. The range of options included both criminal and civil sanctions. However forty-seven per cent of respondents chose the removal of the cause of the problem as their preferred option.

This was closely followed by twenty-seven per cent of responses that considered that the recovery of stolen funds as the most important issues if a fraud had occurred within their organisation.

Table 21 The Most Important Issue if a Fraud occurred within the Organisation

<table>
<thead>
<tr>
<th>Issue</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Criminal Punishment of the offender</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>The Resignation or Dismissal of the employee</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>The Recovery of Stolen funds</td>
<td>27</td>
<td>8</td>
</tr>
<tr>
<td>The Civil Punishment of the offender</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>The Reputation of the Business</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>The Removal of the Cause of the Problem</td>
<td>47</td>
<td>14</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>

Question Fifteen

Table 22 highlights the responses provided by the interviewees to the question that asks these persons to identify the most appropriate course of action if a fraud had
occurred within that organisation. Forty-three per cent of interviewees elected, as the response most appropriate for their organisations to, "Automatically report the matter to the police and therefore have the matter dealt with in the criminal courts" if their organisation was a victim of fraud. This was closely followed by thirty-three per cent of responses that chose to "Legally dismiss the offender and pursue a negotiated compensation". Other options such as the pursuit of a civil remedy and allowing the offender to resign with benefits scored poorly with scores of three percent and zero respectively. The "other" scored higher with twenty percent of responses.

Table 22  The Most Appropriate course of Action if a Fraud occurred within the Organisation

<table>
<thead>
<tr>
<th>Course of Action</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically report the matter to the police and therefore have the matter dealt with in the criminal courts</td>
<td>43</td>
<td>13</td>
</tr>
<tr>
<td>Legally dismiss the offender and pursue a negotiated settlement</td>
<td>34</td>
<td>10</td>
</tr>
<tr>
<td>Allow the offender to resign with benefits</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Pursue a civil remedy</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Other</td>
<td>20</td>
<td>6</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>

Question Sixteen

This question focuses upon the perception of the interviewees towards the future threat of fraud by asking the respondent whether or not in their opinion fraud will increase over the next five years in Australia. Table 23 highlights the responses provided.
Eighty per cent of respondents believed that fraud would increase over the next five years in Australia while only twenty percent of respondents believed that fraud would not increase over that same period.

Table 23  Will fraud will increase over the next five years in Australia

<table>
<thead>
<tr>
<th>Will Fraud Increase</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>80</td>
<td>24</td>
</tr>
<tr>
<td>No</td>
<td>20</td>
<td>6</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>

Question Seventeen

This question follows on from the previous perception of the future of fraud. The interviewees were asked the reason for this increase in the commission of this offence, as highlighted in Table 24.

Thirty-seven percent of respondents indicated that deficiencies in fraud prevention programmes would be responsible for this perceived increase in fraud while thirty percent of respondents believed that a lack of internal controls would be the cause. Twenty percent of respondents indicated that they did not know what would be the cause for this perceived increase in fraud while thirteen percent believed that increases in financial pressures on individuals was the likely cause.
Table 24  The Reason behind this Perceived Increase in Fraud

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deficiencies in fraud prevention programmes</td>
<td>37</td>
<td>11</td>
</tr>
<tr>
<td>Increase financial pressures on individuals</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>Lack of internal controls</td>
<td>30</td>
<td>9</td>
</tr>
<tr>
<td>Don't know</td>
<td>20</td>
<td>6</td>
</tr>
<tr>
<td>Other</td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>

**Question Eighteen**

Again following on from questions sixteen and seventeen the interviewees were asked the area where the interviewee believes that this increase in fraud will occur as highlighted in Table 25. Sixty-seven per cent of respondents believed that the area of growth would be computer fraud followed by twenty percent believing that growth to be in the area of employee fraud with management fraud attracting only ten percent of responses. Three percent of responses stated that they did not know where this increase would come from.
Table 25  Perceived Areas where this Increase in Fraud will Occur

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embezzlement by Employees</td>
<td>20</td>
<td>6</td>
</tr>
<tr>
<td>Management Fraud</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>Computer Fraud</td>
<td>67</td>
<td>20</td>
</tr>
<tr>
<td>Don't Know</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>

Question Nineteen

Question nineteen asks whether or not there is a formal reporting framework for fraud to be communicated to the persons responsible for the necessary fraud prevention controls as identified in Table 26.

Fifty-seven per cent of respondents indicated that such a framework exists within their organisation while forty-three percent did not.

Table 26  The Existence of Fraud Reporting Framework

<table>
<thead>
<tr>
<th>Existence</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>57</td>
<td>17</td>
</tr>
<tr>
<td>No</td>
<td>43</td>
<td>13</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>
Question Twenty

Question twenty asks whether or not the respondent’s organisation has a fraud prevention programme as identified in Table 27. Forty-seven per cent of respondents indicated that such as programme exists. However of these interviewees, over sixty-four percent are employed within the government sector.

Of the fifty-three per cent who indicated that they do not have a fraud prevention programme less than two percent were from the government.

Table 27  The Existence of Fraud Prevention Programmes

<table>
<thead>
<tr>
<th>Existence</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>47</td>
<td>14</td>
</tr>
<tr>
<td>No</td>
<td>53</td>
<td>16</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>

Question Twenty-One

Question twenty-one questions the adequacy or otherwise of the fraud prevention programmes as identified in Table 28. Of those persons who indicated in question twenty that their organisations have a fraud prevention programme only seven percent believed that this programme adequately addresses that organisation’s exposure to fraud risk while ninety-three percent believed that their fraud prevention programme was inadequate.
Table 28  The Adequacy of these Fraud Prevention Programmes

<table>
<thead>
<tr>
<th>Adequate</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>No</td>
<td>93</td>
<td>13</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>14</td>
</tr>
</tbody>
</table>

Question Twenty-two

Question twenty-two asks whether or not the Board of Directors takes an interest in the development and execution of fraud prevention policies as identified in Table 29. Considering the results of questions twenty and twenty-one it comes as no surprise that sixty per cent of respondents indicate that their Boards of Directors do not take an active interest in the development and execution of fraud prevention policies.

Over fifty-eight percent of respondents who indicated in the positive again came from the government sector.

Table 29  Interest Shown by the Board of Directors re Fraud Prevention

<table>
<thead>
<tr>
<th>Interest</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>40</td>
<td>12</td>
</tr>
<tr>
<td>No</td>
<td>60</td>
<td>18</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>
Question 23

This question asks the respondents to identify their preferred course of action if their organisation was a victim of fraud. Their responses are highlighted in Table 30. Fifty per cent of the respondents indicated that their preferred course of action, if their organisation was a victim of fraud, was an investigation that would gather evidence and then hand the matter over to the police for criminal prosecution and punishment. Over forty-six percent of respondents who chose this option were again employed within the government sector however a high number of persons from the commercial sector, over fifty-three percent, do lend support for this option.

Thirty percent of respondents chose the option for an investigation that would gather evidence and then hand the matter over to a solicitor for a negotiated settlement and the dismissal of the offender, three percent preferred a civil investigation and a civil remedy and seventeen percent preferred another option.
Table 30  Preferred Course of Action in the event of Fraud

<table>
<thead>
<tr>
<th>Course of Action</th>
<th>Percentage</th>
<th>Number of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>An investigation that would gather evidence and then hand the matter over to the police for criminal prosecution and punishment</td>
<td>50</td>
<td>15</td>
</tr>
<tr>
<td>An investigation that would gather evidence and then hand the matter over to a solicitor for a civil prosecution</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>An investigation that would gather evidence and then hand the matter over to a solicitor for a negotiated settlement and the dismissal of the offender</td>
<td>30</td>
<td>9</td>
</tr>
<tr>
<td>Other</td>
<td>17</td>
<td>5</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>30</td>
</tr>
</tbody>
</table>

Summary

The overall results of the survey of potential victims of fraud from within the government and commercial sectors are highlighted in Tables 31 and 32. They have been highlighted separately to indicate the significant differences based upon the government’s policy of compulsory reporting of offences to police and compulsory fraud prevention programmes.
<table>
<thead>
<tr>
<th>Issue</th>
<th>Finding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most represented position in survey</td>
<td>Middle Manager</td>
</tr>
<tr>
<td>Most represented industry</td>
<td>Government sector</td>
</tr>
<tr>
<td>Most represented number of frauds</td>
<td>1 - 5</td>
</tr>
<tr>
<td>Most common loss to fraud</td>
<td>Both $10,000 to $100,000 &amp; $100,000 to $1 million</td>
</tr>
<tr>
<td>Most common amount recovered</td>
<td>None</td>
</tr>
<tr>
<td>Most common method of discovery</td>
<td>By Accident</td>
</tr>
<tr>
<td>Most common offender</td>
<td>Employee</td>
</tr>
<tr>
<td>Most common position held</td>
<td>Clerical/Administration</td>
</tr>
<tr>
<td>Reporting or non-reporting to police</td>
<td>Report to Police</td>
</tr>
<tr>
<td>Most common motivation to report</td>
<td>Compulsory policy</td>
</tr>
<tr>
<td>Most common motivation not to report</td>
<td>A desire not to expose the business to possibly adverse publicity</td>
</tr>
<tr>
<td>Most important issue</td>
<td>The removal of the cause of the problem</td>
</tr>
<tr>
<td>Most appropriate course of action</td>
<td>Report the matter to the Police</td>
</tr>
<tr>
<td>Most common perception of future fraud</td>
<td>It will increase over the next 5 years</td>
</tr>
<tr>
<td>Most common area for this increase</td>
<td>Computer Fraud</td>
</tr>
<tr>
<td>Most common cause for this increase</td>
<td>Deficiencies in fraud prevention</td>
</tr>
<tr>
<td>Adequate communications of fraud</td>
<td>The presence of fraud reporting framework</td>
</tr>
<tr>
<td>Fraud prevention present</td>
<td>No</td>
</tr>
<tr>
<td>Adequacy of current fraud prevention</td>
<td>Not adequate</td>
</tr>
<tr>
<td>Board interest in fraud prevention</td>
<td>No</td>
</tr>
<tr>
<td>Preferred course of action</td>
<td>An investigation that would gather evidence and hand the matter over to the police</td>
</tr>
</tbody>
</table>
Table 32  The Overall Results from the Survey Classified by Industry

<table>
<thead>
<tr>
<th>Issue</th>
<th>Govt</th>
<th>Commercial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most represented position in survey</td>
<td>Mid.Management</td>
<td>Mid.Management</td>
</tr>
<tr>
<td>Industry Representation</td>
<td>11</td>
<td>19</td>
</tr>
<tr>
<td>Most represented number of frauds</td>
<td>More than 20</td>
<td>1-5</td>
</tr>
<tr>
<td>Most common loss to fraud</td>
<td>$100,000 - $1 mill</td>
<td>$10,000 - $100,000</td>
</tr>
<tr>
<td>Most common amount recovered</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Most common method of discovery</td>
<td>Accidentally</td>
<td>Accidentally</td>
</tr>
<tr>
<td>Most common offender</td>
<td>Employee</td>
<td>Employee</td>
</tr>
<tr>
<td>Most common position held</td>
<td>Clerical/Admin</td>
<td>Senior Management</td>
</tr>
<tr>
<td>Reporting or non-reporting to police</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Most common motivation to report</td>
<td>Compulsory policy</td>
<td>Compulsory policy</td>
</tr>
<tr>
<td>Most common motivation not to report</td>
<td>To avoid adverse publicity</td>
<td>To avoid adverse publicity</td>
</tr>
<tr>
<td>Most important issue</td>
<td>Removal of cause</td>
<td>Removal of cause</td>
</tr>
<tr>
<td>Most appropriate course of action</td>
<td>Report to Police</td>
<td>Negotiated settlement</td>
</tr>
<tr>
<td>Most common perception of future fraud</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Most common area for this increase</td>
<td>Computer Fraud</td>
<td>Computer Fraud</td>
</tr>
<tr>
<td>Most common cause for this increase</td>
<td>Lack of Fraud Prev.</td>
<td>Lack of Fraud Prev</td>
</tr>
<tr>
<td>Adequate communications of fraud</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Fraud prevention present</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Adequacy of current fraud prevention</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Board interest in fraud prevention</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Preferred course of action</td>
<td>Police</td>
<td>Solicitor</td>
</tr>
</tbody>
</table>
7.3 The Results Regarding Attitudes to White Collar Crime

The previous survey of decision-makers in the commercial and government sectors has provided insight into the possible reasons for the non-reporting of crimes to police as well as highlighting the difference between what victims of fraud require and the solutions that law enforcement provide. The result of the questionnaire reported within this section tests the attitudes of both detectives and student police officers towards investigating white-collar crime and its significance when compared to offences of a similar nature and importance.

The overall sample was broken down into two categories, the first being detectives and the latter being student police officers. The basis for this division is that detectives are experienced police officers with a number of years police service. Student police officers on the other hand are recent recruits to the police service from a variety of vocations and therefore are likely not to be as institutionalised as detectives.
Table 33  Classification of Offences According to Perceived Seriousness by Detectives

<table>
<thead>
<tr>
<th>Crime</th>
<th>1 - 5</th>
<th>6 - 10</th>
<th>Greater than 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Murder</td>
<td>28</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rape</td>
<td>28</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Domestic Violence</td>
<td>12</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Drug Offences</td>
<td>20</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>Stealing</td>
<td>11</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td>Break &amp; Enter</td>
<td>20</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Shoplifting</td>
<td>16</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Traffic Offences</td>
<td>16</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Malicious Damage</td>
<td>11</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td>Drunk Driving</td>
<td>12</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>Embezzlement</td>
<td>10</td>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>3</td>
<td>24</td>
<td>1</td>
</tr>
<tr>
<td>Computer Fraud</td>
<td>9</td>
<td>15</td>
<td>4</td>
</tr>
<tr>
<td>White Collar</td>
<td>16</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>Arson</td>
<td>20</td>
<td>7</td>
<td>1</td>
</tr>
</tbody>
</table>

Results from survey of Detectives

Table 33 highlights the responses from detectives and the main features of their responses are:

1. The most serious of the fifteen crimes were considered to be murder, rape and domestic violence;
2. The least serious of the offences with the highest score in the category of greater than ten were traffic offences and shoplifting;

3. The crimes with the highest scores within the six to ten category were firstly credit card fraud with an overall score of twenty-four, embezzlement with a score of seventeen and computer fraud with a score of fifteen. White collar crime ranked next with a score of ten;

4. In the category of one to five the three offences with the worst scores were credit card fraud with a score of three, computer fraud with a score of nine and embezzlement with a score of ten. White-collar crime ranked with shoplifting and traffic offences with a score of sixteen, and

5. Overall three out of the four financial offences achieved the worst scores in the one to five category where the most serious offences are recognised.

The data generated by this questionnaire and table 33 was also tested using the chi-squared test and more specifically, the association between two sets of attributes namely crime and ranking (See Appendix 4). The null hypothesis for this test draws the assumption that there is no association between these attributes. However, in all cases the null hypothesis can be rejected at 0.05 confidence level. From this we can deduce that there is a strong relationship between the two attributes. Therefore the null hypothesis is rejected, as there is strong evidence that there is an association between crime and ranking.
Table 34  Classification of Offences According to Perceived Seriousness by Student Police Officers

<table>
<thead>
<tr>
<th>Crime</th>
<th>1 - 5</th>
<th>6 - 10</th>
<th>Greater than 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Murder</td>
<td>478</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Rape</td>
<td>474</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Domestic Violence</td>
<td>379</td>
<td>82</td>
<td>21</td>
</tr>
<tr>
<td>Drug Offences</td>
<td>271</td>
<td>149</td>
<td>62</td>
</tr>
<tr>
<td>Stealing</td>
<td>52</td>
<td>280</td>
<td>150</td>
</tr>
<tr>
<td>Break &amp; Enter</td>
<td>106</td>
<td>306</td>
<td>70</td>
</tr>
<tr>
<td>Shoplifting</td>
<td>21</td>
<td>100</td>
<td>361</td>
</tr>
<tr>
<td>Traffic Offences</td>
<td>21</td>
<td>94</td>
<td>366</td>
</tr>
<tr>
<td>Malicious Damage</td>
<td>101</td>
<td>266</td>
<td>115</td>
</tr>
<tr>
<td>Drunk Driving</td>
<td>268</td>
<td>158</td>
<td>56</td>
</tr>
<tr>
<td>Embezzlement</td>
<td>39</td>
<td>219</td>
<td>224</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>22</td>
<td>126</td>
<td>334</td>
</tr>
<tr>
<td>Computer Fraud</td>
<td>36</td>
<td>157</td>
<td>289</td>
</tr>
<tr>
<td>White Collar</td>
<td>65</td>
<td>200</td>
<td>217</td>
</tr>
<tr>
<td>Arson</td>
<td>227</td>
<td>223</td>
<td>32</td>
</tr>
</tbody>
</table>

Results from the Survey of Student Police Officers

The significant features of the results from this questionnaire are;
1. As expected the most serious of the fifteen crimes are murder, rape and domestic violence;

2. As with the responses from the detectives, student police indicated that the most insignificant of the offences, those with the highest number of responses within the category of greater than ten were traffic offences and shoplifting. These offences scored three hundred and sixty-six responses and three-hundred and sixty-one responses respectively;

3. The student police officers placed financial offences predominantly within the greater than ten category with scores only slightly better than traffic offences and shoplifting. Credit card fraud attracted three hundred and thirty four responses, computer fraud received two hundred and eighty-nine responses, embezzlement two hundred and twenty-four and white-collar crime two hundred and seventeen;

4. This same situation was also reflected in the category of one to five. The financial offences of credit card fraud, computer fraud, and embezzlement were placed behind traffic offences and shoplifting respectively with white-collar crime in sixth position behind stealing.

The data generated by this questionnaire and table 34 was also tested using the chi-squared test and more specifically, the association between two sets of attributes namely crime and ranking (See Appendix 5). The null hypothesis for this test draws the assumption that there is no association between these attributes. However, in all cases the null hypothesis can be rejected at 0.05 confidence level. From this we can deduce that there is a strong relationship between the two attributes. Therefore the null hypothesis is rejected, as there is strong evidence that there is an association between crime and ranking.
7.4 The Results Regarding Attitudes to Crime Prevention

This survey asked the criminal investigators to identify those issues that they believed should or should not be included within the training of future detectives from the standpoint of the significance or otherwise of fraud prevention programmes. Twenty-nine police stations across the State of New South Wales that had criminal investigators attached to their station responded with fifty-one individual responses.

Questions one through to four identify the rank structure of the population that comprises of:

- Two Inspectors;
- Eleven Sergeants;
- Twenty-five Senior Constables;
- Ten Constables First Class and;
- Three Constables.

The main focus of this questionnaire is question five which asks the respondent to categorised fifteen potential subjects with the most important issue to be given the score of "1" and the least important subject to be given the score of "15". The results of that questionnaire are highlighted in Table 35.
Table 35  Responses from Detectives re possible subjects for Detectives Training

<table>
<thead>
<tr>
<th>Subject</th>
<th>1 - 5</th>
<th>6 - 10</th>
<th>&gt; 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laws of Evidence</td>
<td>50</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Psychology</td>
<td>2</td>
<td>17</td>
<td>32</td>
</tr>
<tr>
<td>Crime Scenes</td>
<td>48</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Ethics Training</td>
<td>2</td>
<td>14</td>
<td>35</td>
</tr>
<tr>
<td>Powers of Arrest</td>
<td>44</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>Supervision</td>
<td>5</td>
<td>33</td>
<td>13</td>
</tr>
<tr>
<td>Use of Firearms</td>
<td>21</td>
<td>19</td>
<td>11</td>
</tr>
<tr>
<td>Multi-culturalism</td>
<td>0</td>
<td>5</td>
<td>46</td>
</tr>
<tr>
<td>Team Spirit building</td>
<td>6</td>
<td>19</td>
<td>26</td>
</tr>
<tr>
<td>Officer Survival</td>
<td>19</td>
<td>27</td>
<td>5</td>
</tr>
<tr>
<td>Health</td>
<td>3</td>
<td>22</td>
<td>26</td>
</tr>
<tr>
<td>Role Play</td>
<td>3</td>
<td>26</td>
<td>22</td>
</tr>
<tr>
<td>Acts of Parliament</td>
<td>38</td>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td>Crime Prevention</td>
<td>5</td>
<td>28</td>
<td>18</td>
</tr>
<tr>
<td>Guest lecturers</td>
<td>10</td>
<td>27</td>
<td>14</td>
</tr>
</tbody>
</table>

The subjects that rated poorly with criminal investigators with regard to their inclusion within the training of future detectives are;

1. Psychology with a score of thirty-two responses in the greater than ten category and only two responses in the most important category of one to five;
2. Ethics training with a score of thirty-five responses in the greater than ten category and only two responses in the most important category of one to five and;

3. Multi-culturalism with a score of forty-six responses out of a possible fifty-one in the greater than ten category and no responses in the most important category of one to five.

Other main features of the results from this questionnaire are;

1. Laws of Evidence, Crime Scenes and Powers of Arrest were the most supported responses in the category of one to five;

2. Within the category of six to ten, which indicates moderate support, the most favoured possible subject was Supervision;

3. The next most favoured response behind supervision within this same category was Crime Prevention and;

4. Crime Prevention was favoured ahead of such possible subjects as Officer Survival, Health and Team Spirit Building.

The data generated by this questionnaire and table 35 was also tested using the chi-squared test and more specifically, the association between two sets of attributes namely crime and ranking (See Appendix 6). The null hypothesis for this test draws the assumption that there is no association between these attributes. However, in all cases the null hypothesis can be rejected at 0.05 confidence level. From this we can deduce that there is a strong relationship between the two attributes. Therefore the null hypothesis is rejected, as there is strong evidence that there is an association between crime and ranking.
7.5 The Results from the analysis of fraud offenders

The criteria for this search were based on those fraudulent crimes that involved the use of a computer as the tool to facilitate the crime or, the computer was the actual target of the crime. These figures, while limited in number, are actual cases of persons arrested rather than projections taken from surveys or questionnaires. The results from this analysis will be compared to the results from the survey and questionnaires in order to identify trends. Between January 1992 and January 1994, only 28 crimes met these criteria. These 28 reported crimes were then examined to study:

1. The types of persons who commit fraud;

2. The sentence given to offenders by the courts upon conviction.

3. Details with regard to the victims of this crime, and

4. Industry or victim details.

The results from this analysis are highlighted in Table 36 and Table 37.
Table 36  Sentences given to Arrested Computer Fraud Offenders

<table>
<thead>
<tr>
<th>Sentence</th>
<th>Percentage</th>
<th>Number of Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recognizance</td>
<td>39</td>
<td>11</td>
</tr>
<tr>
<td>Fine</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>Imprisonment</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>556A where the Offence is Proven but Dismissed</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>Community Service Order</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>Periodic Detention</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>Unknown</td>
<td>18</td>
<td>5</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>28</td>
</tr>
</tbody>
</table>

**Source:** New South Wales Criminal Histories Computer System

The results from this analysis of table 36 indicate that:

- Only three percent of persons arrested received a term of imprisonment.
- Eleven percent of offenders received only a fine for their actions.
- Eleven percent of offenders received a community service order or section 556A.
- Seven percent of offenders received periodic detention.

- Eighteen percent of sentences were unknown.

Other significant results from the sample of computer fraud offences include:

- Of the twenty-eight cases retrieved nineteen involved males and nine involved females;

- The most common age group for the females was between thirty-one and thirty-nine;

- The most common age group for the males was between forty and forty-nine;

- Twenty-seven out of the twenty-eight offenders were employees of the victim, and

- Twenty-one out of the twenty-eight victims did not receive compensation.

- Twenty-two out of the twenty-eight offenders did not have a previous criminal record;

- No female had a previous criminal history;

- Only six males did not have a criminal history;

- Twenty-three out of the twenty-eight offenders did not have a criminal history;

- No female had a previous criminal history for committing fraud, and

- Only fourteen males did not have a previous criminal history for committing fraud.
Table 37  Victim Details based on Industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
<th>Number of Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking</td>
<td>29</td>
<td>8</td>
</tr>
<tr>
<td>Insurance</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Hospitality</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Government</td>
<td>11</td>
<td>3</td>
</tr>
<tr>
<td>Retail</td>
<td>22</td>
<td>6</td>
</tr>
<tr>
<td>Other</td>
<td>18</td>
<td>5</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>28</td>
</tr>
</tbody>
</table>

Source: New South Wales Criminal Histories Computer System

- Twenty-nine percent of offenders were employed within the banking system
- The retail industry had twenty-two percent of offenders
- The government and insurance sectors attracted eleven percent of offenders
- The hospital industry with six percent of offenders
- The manufacturing industry with three percent of offenders, and
• Other Industries had eighteen percent of offenders.

7.6 Summary

The results from these surveys provide a possible explanation for the non-reporting of fraud offences by victims of crime and the ramifications of these results will be discussed in the following chapter.
Chapter Eight  
THE DISCUSSION OF THE RESULTS FROM THE SURVEY AND THE QUESTIONNAIRES

8.1 Introduction

8.2 Discussion of the results of the survey of potential victims of fraud

8.3 Discussion of the results regarding attitudes to white-collar crime

8.2 Discussion of the results regarding attitudes to crime prevention

8.3 Discussion of the results of the analysis of fraud offenders

8.6 Summary

This chapter discusses the results from the various questionnaires and surveys conducted with police investigators from the New South Wales Police Service and potential victims of fraud from both the government and commercial sectors. The questions asked of each of these respondents are described and the results stemming from these questions are scrutinised.
8.1 Introduction

The previous chapter has provided the results of the surveys and questionnaires involving respondents from:

1. Government departments;
2. The commercial sector;
3. Experienced criminal investigators;
4. Student Police Officers and;
5. Statewide Police Stations.

The results from those surveys and questionnaires will now be discussed in light of the requirements of victims of fraud, the incidence and responses to fraud, the implementation of fraud prevention programmes and the various attitudes of police officers to fraud and fraud prevention.

8.2 Discussion of the results of the Survey of Potential Victims of Fraud

Question One

Table 12 in the previous chapter identifies the position held by the respondent. The significance of this question is to ensure that the respondent holds a decision making position. It was essential to this research that the person questioned is capable of implementing fraud-related issues. In this case the vast majority of persons interviewed are capable of this with the remainder in a position where their opinion is capable of influencing such a decision.
Questions Two and Three

Questions two and three required firstly, an indication from the respondents of the sector of the government or commercial areas that these persons represented and secondly the ownership of the organisation. The need to establish the sector and the ownership of the organisation was based upon the knowledge that within government organisations certain reporting procedures for criminal offences and fraud prevention are mandatory unlike commercial entities where it is by choice (Commonwealth Law Enforcement Board 1996). The results from these questions indicate that the large proportions of companies, forty-seven percent, are government entities. Consequently this large proportion from the government sector has impacted upon some of the final results namely, the reporting of fraud offences to law enforcement due to the compulsory reporting policies.

Nonetheless, the sample contains a broad spectrum of companies that includes the manufacturing industry, which was identified by research conducted by the Association of Certified Fraud Examiners as a high-risk industry. This industry is well represented with twenty-one percent of the population. Publicly and privately owned corporations were also well represented with forty percent thereby providing this sample with the full spectrum of candidates which was required for this research.

Question Four

Question four concentrated upon the number of known incidents of fraud that the companies have experienced in the past five years. The most salient feature of these results is the fact that seventy-three per cent of interviewees indicated that they had incurred incidents of fraud over the past five years. It is also worth noting that a large proportion of respondents, twenty-seven per cent, indicated that they had incurred over twenty incidents of fraud in that same period of time with seven out of eight of these respondents coming from the government sector. As previously stated the policy of mandatory reporting of crimes to police would have impacted upon this statistic.
Twenty-seven percent of the population surveyed indicated that they had not incurred any fraud during that period. This may be in part due to the implementation of fraud prevention policies or as suggested by Kamay (1992) these companies may have chosen not to report these crimes for a variety of corporate and financial reasons.

Nonetheless the results from this question across the spectrum of both government and commercial corporations reveal that the crime of fraud has been committed upon and present in some of Australia’s largest corporations.

**Question Five**

Following on from the frequency of these offences, the respondents were asked to approximate the total loss in connection with these frauds. Only ten percent of those respondents who admitted being affected by fraud indicated that they had losses due to this crime of less than ten thousand dollars. This loss is comparable and consistent with the findings of research conducted by KPMG (1995) where the average fraud amounted to less than $10,000. However, thirty-two percent of respondents stated that they had losses between ten thousand dollars and one hundred thousand dollars and that same percentage of respondents indicated that they had losses between one hundred thousand dollars and one million dollars. Considering the small sample of respondents these figures are quite substantial giving credibility to the fact that average losses to fraud are considerably larger than believed (KPMG 1997).

**Question Six**

This question asked those twenty-two respondents who admitted being affected by fraud whether or not any of the money that was lost to this crime was actually recovered. The majority of these respondents, forty-one percent, indicated that they had recovered none of the money lost to fraud while twenty-three percent recovered a
quarter of the money, eighteen percent recovered half, four percent recovered three-quarters and fourteen percent recovered all of the money.

This result sheds some light on a response to question fourteen where twenty-seven per cent of respondents, which was the second highest score, indicated that the recovery of stolen funds was one of the most important issues for an organisation that had been a victim of fraud.

It is worth mentioning that the primary function of law enforcement and more particularly of criminal investigators, is to apprehend criminal offenders and bring them before a Justice to be dealt with according to law. A criminal investigation does not include seeking stolen funds nor does it include securing the offender's assets pending a claim for compensation by the victim. As a detective and criminal investigator with the New South Wales Police Service for over fifteen years the attitude of the police is typically depicted in the statement that I have heard said to victims of crime on many an occasion that "...we are not debt collectors".

This issue of compensation by the criminal courts is worthy of mention and it will be scrutinised in further detail in the next chapter of recommendations in the dissection of fifty case studies taken from the New South Wales Police criminal histories computers. The incidence and amounts of compensation will also be examined as well as the overall needs of victims of fraud.

Overall the responses to this question being a poor recovery of money lost to fraud, at the very least, shed some light on a possible reason why victims of fraud may not report the matter to police unless of course it is mandatory.

**Question Seven**

Of the remaining twenty-two respondents who had experienced fraud in the past five years, this question asks how the fraud was discovered. The highest score was thirty-
six percent of respondents who stated that they discovered the crime by accident. This was followed by internal audit attaining a score of thirty-two percent, external audit found no offences, an investigation uncovered fourteen percent of offences and other methods and whistleblowers found nine percent each. The fact that the majority of the frauds were only discovered by accident coincides with the responses in question twenty-one where the interviewees were asked "...do you believe that the fraud prevention programme adequately addresses your organisation's exposure to fraud risk". Twenty-nine out of the thirty interviewees, or ninety-seven per cent, indicated that the organisation's fraud prevention programme was inadequate.

Therefore, a logical starting point in the minimisation of fraud is the development of suitable fraud prevention, detection and deterrence programmes that are examined further in the following chapter. This point is further aided by the relatively high score of nine percent of offences uncovered by whistleblowers and fourteen percent revealed by investigations which is but one part of the fraud prevention programme.

The fact that external audit uncovered no offences coincides and supports issues raised in chapter nine as to its lack of effectiveness in uncovering fraud (Sullivan, 1999).

**Question Eight**

As shown in Table 16, eighty percent of respondents indicated that the fraud offender was an employee and only fourteen percent were external to the organisation. The high score highlighting the offender as an employee coincides with the findings of the Association of Certified Fraud Examiners (1996) as well as KPMG (1995) and the examination of the case studies from the New South Wales Police. Again this issue strengthens the case for fraud prevention programmes within an organisation and this matter will be examined in the following chapter.
Questions Nine and Ten

This question seeks to classify the position held by the employee at the time of the fraudulent offence. Forty-five percent of respondents had offenders employed within the clerical or administration sections of the organisation with middle management being responsible for ten percent, sales two percent, senior management twenty-seven percent and other sections fourteen percent.

There were two separate issues that arose from the results from this question. A person holding a clerical or administrative position committed forty-five percent of offences. In the absence of fraud prevention programmes it is difficult to monitor or stop a person who control such responsibilities as payments and receipts. I believe the most alarming statistic is the score of ten percent for middle management and twenty-seven percent for senior management. These are the persons who are usually responsible for the authorisation and implementation of fraud prevention strategies. If this group of persons are also responsible for committing a large proportion of offences it is presumably very unlikely that they would implement policies that could see them caught offending.

Fortunately there are still company officers that are in senior decision-making positions to these persons. Staff employed within high-risk areas could then be targeted with concentrated efforts to offer alternatives to theft and at the same time rigid controls and procedures could be implemented to make it more difficult for persons to offend.
Question Eleven

This question is perhaps one of the salient features of this survey as it broaches the subject of whether or not the twenty-two respondents who incurred losses due to fraud reported the matter to the police.

As evidenced by Table 19, the large proportion of respondents from the government sector in this survey has impacted upon these results. As with most government departments it is compulsory that each and every illegal activity is to be reported to the police. Therefore, the issue of reporting the fraud to law enforcement was not done so as a matter of choice based on the requirements of the organisation but compulsory.

The significant feature of these responses were the fifteen responses or sixty-eight percent, that indicated that the fraud was reported to the police, nine of those respondents were employed within the government sector. Of the seven responses or thirty-two percent, that indicated that the fraud was not reported to the police, no government sectors were represented.

Question Twelve

This question asks of the thirty persons interviewed what would be necessary to motivate that person to report a fraud offence to the Police. Sixty-four percent of respondents indicated that it was a compulsory policy to report offences while thirteen percent indicated that they would be motivated to report the offence on the basis of having the person punished. Thirteen percent reported the matter on the basis of it being the only course of action known to them and ten percent were motivated by other matters.

This result is yet another area where the large proportion of respondents from the government sector in this survey has impacted upon the results. As with most government departments it is compulsory that each and every illegal activity is to be
reported to the police. Therefore, the issue of compulsory policy being the motivation behind reporting the fraud to law enforcement was again done so based on the requirements of the organisation and not as a matter of choice.

**Question Thirteen**

Table 20 highlights the responses to the question that asks the interviewees to identify the motivation that would deter them from reporting the matter to the police. Of the ten choices on offer to the respondents the vast majority, seventy-seven per cent, opted for "A desire not to expose your business to possibly adverse publicity". The bulk of these responses came from the private sector however nine interviewees from the government sector also believed this to be the best option.

Of the ten options available to the respondents only six attained any score. These were a lack of confidence in the judicial system which scored three percent, lengthy court appearances three percent, loss of control over the investigation seven percent, loss of control over confidentiality three percent and other motivations seven percent. Others such as a possible shareholder backlash, possible dismissal, lack of confidence in the remedies offered by courts and poor sentences did not achieve a score.

A strong response to avoid bad publicity for the business also reinforces reasons why corporations have not been reporting fraud offences to the police.

**Question Fourteen**

This question asks the interviewees to identify the most important issue if a fraud had occurred within their organisation. The options available to the interviewees ranged from civil and criminal remedies to in-house solutions. The result from this question indicates that an in-house and confidential solution to the problem is the preferred
option with forty-seven percent of respondents identified the removal of the cause of the problem as their most favoured option. This response falls in line with a previous response that the reputation of the organisation is paramount in the minds of the respondents as does the next most favoured response being the recovery of stolen funds with twenty-seven percent of respondents preferring this response. The selection of "the removal of the cause of the problem" could provide some insight possibly into the non-reporting of matters to the police. Both criminal and civil sanctions were overlooked in favour of this option and are seen to be more of an overt solution to the problem of fraud, bringing attention to the exploits of the organisation.

**Question Fifteen**

This question asks the interviewees to identify the most appropriate course of action if a fraud had occurred within that organisation. Forty-three per cent of interviewees elected, as the response most appropriate for their organisations to, "automatically report the matter to the police and therefore have the matter dealt with in the criminal courts" if their organisation was a victim of fraud. This result is in stark contrast to the responses provided in question fourteen. Again, almost half of the respondents were employed within the government sector and therefore it is possible that this response could have been swayed by the compulsory policy to report all frauds.

The next most popular response was to "legally dismiss the offender and pursue a negotiated compensation". All bar one of the respondents who chose this option were from the private sector that lends credence to the proposition that the obligatory reporting of offences within the government sector has influenced the outcome. This result also supports the most favoured responses to question fourteen being the in-house and confidential solution to the offence rather than an action that may bring adverse publicity on the organisation.
Question Sixteen

This question focuses upon the perception of the interviewees towards the future threat of fraud by asking the respondent whether or not in their opinion fraud will increase over the next five years in Australia.

The fact that eighty per cent of respondents believe that fraud will increase over the next five years in Australia coincides with similar results from both KPMG (1995) and the Association of Certified Fraud Examiners (1996). This result is unusual considering the responses in question twenty-one where the vast majority of persons believed that their current fraud prevention programmes were inadequate. This result prompts the question, if respondents believe that frequency of fraud will increase over the next five years in this country why then don’t their respective organisations have suitable protection such as internal controls and fraud prevention policies? Perhaps this attitude should warrant further research.

Question Seventeen

This question follows on from the previous perception of the future of fraud and it asks the interviewees the reason why they believe that there will be an increase in the commission of this fraud over the next five years in Australia.

Thirty-seven percent of respondents indicated that deficiencies in fraud prevention programmes would be responsible for this perceived increase in fraud while thirty percent of respondents believed that a lack of internal controls would be the cause. Twenty percent of respondents indicated that they did not know what would be the cause for this perceived increase in fraud while thirteen percent believed that increases in financial pressures on individuals was the likely cause.

Overall sixty-seven per cent of respondents believe that this increase in fraud will be attributed to the lack of internal controls and fraud prevention programmes. This result
prompts an interesting question. Does the fact that thirty-seven percent of offenders are in a decision-making position within the organisation, as identified in question nine, have any impact on the fact that preventative policies are not in place even though they are recognised as a cause for a perceived increase in the future? The results from this question appears to provide support that these effective controls are not wanted, perhaps motivated by nefarious reasons.

Another disturbing result from this question is that twenty percent of respondents did not know what would be the cause of a perceived increase in fraud in the future. Again, as decision-makers, it is the responsibility of these persons to operate the organisation optimally and to have no ideas regarding the cause and potential solutions possibly explains why employees are the prime group of offenders.

Question Eighteen

Again following on from questions sixteen and seventeen the interviewees were asked the area where the interviewee believes that this increase in fraud will occur. Sixty-seven per cent of respondents believed that the area of growth would be computer fraud.

This perception corresponds with the Computer Crime and Security Survey (1997) that states "...Australian industry is subject to a significant level of computer security incidents at a rate comparable to the United States". They go further to state "...there is a direct correlation between our increasing dependence on sophisticated information technologies and a growing level of vulnerability to electronic attack".

This perception contradicts the findings of the New South Wales Police Working Party on Computer Based Evidence (1996). This working party took the view that "...it is unnecessary to train all uniform police, let alone detectives, with a computer
crime awareness programme, as there is presently insufficient computer crime coming to the attention of police. From my fourteen years experience, twelve in investigation, I state categorically that the requirement for computer retrieval of evidence is rare."

If the law enforcement agencies are to realistically compete and ultimately overcome the criminal element with regard to these emerging issues perhaps they may have to re-think their position with regard to technology based issues.

**Question Nineteen**

Question nineteen asks whether or not there is a formal reporting framework for fraud to be communicated to the persons responsible for the necessary fraud prevention controls.

Fifty-seven per cent of respondents indicated that such a framework exists within their organisation however over fifty-eight percent of these respondents were again from the government sector and with compulsory fraud prevention policies in place it explains the high proportion of responses and therefore downgrades the significance of this score.

Forty-three percent of respondents indicated that they did not have the necessary reporting framework in place however only fifteen percent of those respondents were employed within the government sector. This gives rise to the fact that the necessary reporting procedures for fraud offences within the commercial sector is low and it is questionable whether or not the government sector would follow suit if not for compulsory policies.
Question Twenty

Question twenty asks whether or not the respondent’s organisation has a fraud prevention programme. Forty-seven per cent of respondents indicated that such a programme exists however of these interviewees, sixty-four percent are employed within the government sector. Of the fifty-three per cent who indicated that they do not have a fraud prevention programme less than two percent were from the government leaving the commercial sector well behind in appreciating the significance of fraud prevention. This result gives the impression that the government sectors have a far greater appreciation and acceptance of the relevance of fraud issues than the organisations within the commercial or private sector.

Question Twenty-One

Question twenty-one questions the adequacy or otherwise of those interviewees who have fraud prevention programmes as identified in Table 28. Of those fourteen persons who indicated in question twenty that their organisations have a fraud prevention programme only one person believed that this programme adequately addresses that organisation's exposure to fraud risk.

Not surprisingly this person was employed within the government sector. The significant feature of this result is that eighty-nine per cent of the government-employed respondents believe that the fraud prevention policies adopted by their organisations are inadequate. We are therefore left with a situation where fifty-three per cent of the interviewees do not have a fraud prevention policy and of the forty-seven per cent that do, eighty-nine per cent of those persons believe that their programmes are inadequate.

The responses from this question cast some doubt over the responses to the previous question.
Question Twenty-two

Question twenty-two asks whether or not the Board of Directors takes an interest in the development and execution of fraud prevention policies. Considering the results of questions twenty and twenty-one it comes as no surprise that sixty per cent of respondents indicate that their Boards of Directors does not take an active interest in the development and execution of fraud prevention policies. This result supports the responses to a number of previous questions where there seems to be a reluctance on the part of senior management to implement strategies to minimise the impact of fraud and that there is a large percentage of senior management who have committed the offences. Over fifty-eight percent of the respondents who indicated in the positive again came from the government sector again emphasising the poor participation of the commercial sector.

Question Twenty-three

This question asks the respondents to identify their preferred course of action if their organisation was a victim of fraud. Fifty per cent of the respondents indicated that their preferred course of action, if their organisation was a victim of fraud, was an investigation that would gather evidence and then hand the matter over to the police for criminal prosecution and punishment. Over forty-six percent of respondents who chose this option were again employed within the government sector however a high number of persons from the commercial sector, over fifty-three percent, do lend support for this option. It does support the notion that the commercial sector prefers that the police deal with fraud however there are other influencing factors that go against this desire. It could be based on the fact that the costs of having the police investigate the matter is borne by the government whereas other forms of investigation are borne by the victim.
Of the thirty-percent of respondents who chose the option for an investigation that would gather evidence and then hand the matter over to a solicitor for a negotiated settlement and the dismissal of the offender, all but one of the respondents were from the commercial sector lending support for issues such as control over the outcome and the exposure to the organisation.

Summary

The overall results of the survey of potential victims of fraud from within the government and commercial sectors are highlighted in Tables 33 and 34 in the previous chapter. This division has been based upon the influence that compulsory reporting of offences to police and compulsory fraud prevention strategies has had on the responses provided by the respondents. This distinction is highlighted in Table 32 and in the process it provides a more accurate summary of both the government and commercial sectors attitudes to the offence of fraud and the implementation of strategies that may be implemented to minimize its effect.

The differences between these two groups are:

1. The most common incidence of fraud in the government sector is “More than Twenty” while in the commercial sector it is one to five offences;

2. The average loss in the government sector is $100,000 to $1 million whereas in the commercial sector the average loss is $10,000 to $100,000;

3. Both sectors recognise that no stolen monies have been recovered;

4. The most common methods of discovery is by accident within both sectors;
5. The most common offender is still the employee however this person is in a clerical or administrative position within the government sector whereas this person is a senior manager within the commercial sector;

6. The government interviewees have reported these frauds to the police whereas the persons within the commercial sector have not;

7. The most appropriate course of action if a fraud existed within the government sector is to report the matter to the police whereas within the commercial sector it is to investigate the matter and then negotiate a settlement with a solicitor;

8. Both agree that fraud will increase over the next five years within the area of computer fraud and due to deficiencies in fraud prevention;

9. The government respondents indicate that they have a fraud reporting framework whereas the commercial sector respondents do not;

10. The government respondents indicate that they have fraud prevention programmes whereas the commercial sector respondents do not;

11. Both agree that the current fraud prevention programmes are inadequate and;

12. The preferred course of action if a fraud was incurred by the government organisation is to conduct an investigation that would gather evidence and then hand the matter over to the police whereas the commercial sector respondents prefer an investigation that would gather evidence and then hand the matter over to a solicitor.

The results from this survey of both commercial and government decision-makers indicates that even though victims of fraud would prefer to report crimes to the police they are reluctant to do so on the basis that the requirements of the victims are not
satisfied by the services that are provided by law enforcement and the judicial system. Also, regardless of the industry classification both groups identify the need for fraud prevention programmes in light of their belief that fraud will escalate over the next five years and at the same time they identify the inadequacies of those existing programmes to combat fraud.

8.3 Discussion of the Results Regarding Attitudes to White Collar Crime

The previous survey of decision-makers in the commercial and government sectors has provided insight into the possible reasons for the non-reporting of crimes to police as well as highlighting the difference between what victims of fraud require and the solutions that law enforcement provide. This questionnaire tests the attitudes of both detectives and student police officers towards investigating white-collar crime and its significance when compared to offences of a similar nature and importance.

Discussion of the survey of Detectives

Table 33 in the previous chapter highlights the responses from detectives and the main features of their responses are;

1. The most serious of the fifteen crimes are murder, rape and domestic violence that indicates that the respondents gave serious attention to the classification of crimes;

2. The worst of the offences with the highest score in the category of greater than ten were traffic offences and shoplifting;
3. The crimes with the highest scores within the six to ten category were firstly computer fraud with an overall score of twenty-four, embezzlement with a score of seventeen and computer fraud with a score of fifteen. White-collar crime ranked next with a score of ten;

4. In the category of one to five the three offences with the worst scores were credit card fraud with a score of only three, computer-related fraud with a score of nine and embezzlement with a score of ten. White-collar crime ranked with shoplifting and traffic offences with a score of sixteen and;

5. Overall three out of the four financial offences achieved the worst scores in the one to five category where the most serious offences are recognised.

Credit card fraud, computer fraud and embezzlement scored worse than offences such as shoplifting, malicious damage (vandalism) and traffic offences while white-collar crime was ranked on par with shoplifting and traffic offences. These crimes have far less social impact and monetary impact than financially based crime. As a former criminal investigator I can establish that experienced criminal investigators have a number of criminal investigations running simultaneously which compels them to prioritise these investigations in order of importance. The results of this questionnaire indicate that criminal investigators believe that the various forms of fraud are as significant and as important as investigating shoplifters and therefore it would be safe to assume that fraud offences would rate lowly in the order of attention and seriousness in the mind of the investigator. Perhaps this attitude could have impacted on the responses given by the victims of fraud.

8.4 Discussion from the Survey of Student Police Officers

The significant features of the results from this questionnaire are;
1. As expected the most serious of the fifteen crimes are murder, rape and domestic violence that indicates that these respondents, as with detectives, gave serious attention to the classification of crimes;

2. As with the responses from the detectives, student police indicated that the most insignificant of the offences, those with the highest number of responses within the category of greater than ten were traffic offences and shoplifting. These offences scored three hundred and sixty-six responses and three-hundred and sixty-one responses respectively;

3. Within the detective's responses the financial offences were placed in the mid range category of six to ten category. Unlike the detectives, the student police officers placed these financial offences predominantly within the greater than ten category with scores only slightly better than traffic offences and shoplifting. Credit card fraud attracted three hundred and thirty four responses, computer fraud received two hundred and eighty-nine responses, embezzlement two hundred and twenty-four and white-collar crime two hundred and seventeen;

4. This same situation was also reflected in the category of one to five. The financial offences of credit card fraud, computer fraud, and embezzlement were placed behind traffic offences and shoplifting respectively with white-collar crime in sixth position behind stealing.

Summary

The results from this questionnaire are not conducive for an effective investigation when you consider that the various forms of fraud are seen as significant as:

- Traffic offences that could include, for example, receiving a Traffic Infringement Notice for not using your indicator when turning a corner;
• Shoplifting or shop-stealing which is the theft of low value goods from a department store, and

• The offence of malicious damage (vandalism) that could be writing graffiti on a wall, costing probably hundreds of dollars to repair, that was seen to be more serious than financial offences, that could have values in excess of millions of dollars, that have a far greater impact on society.

The present situation for the criminal investigation of fraud seems grim considering the experienced detective’s low priority to investigating the crime and the future of the investigation of fraud is also not a promising one when you consider the criminal investigators of the future, current student police officers, believe that the most insignificant offences in their eyes, after traffic offences and shoplifting are credit card fraud, computer fraud, embezzlement, stealing and white-collar crime.

8.5 Discussion of the Results Regarding Attitudes to Crime Prevention

In Chapter two the benefits of fraud prevention were discussed in publications such as the Commonwealth Law Enforcement Board (1996), KPMG (1997) and the United Nations (1995). According to these documents fraud prevention is as an integral part of the various responses to fraud. Traditional law enforcement is predominantly a reactive one however the assessment of the attitudes of criminal investigators towards the utilisation of fraud preventative policies is warranted.

This survey asked the criminal investigators to identify those issues that they believed should or should not be included within the training of future detectives. Twenty-nine police stations across the State of New South Wales that had criminal investigators attached to their station responded with fifty-one individual responses.
The preliminary questions in this survey, one through to four identify the rank and experience of the respondent thereby determining that the responses have been given by a person who is in a position to possibly influence the content of any training programmes. The main focus of this questionnaire is question five which asks the respondent to categorised fifteen potential subjects with the most important issue to be given the score of "1" and the least important subject to be given the score of "15". All of these potential subjects are considered to be of equal importance however Laws of Evidence, Crime Scenes and Powers of Arrest according to the Detectives Education Programme (1995) are the bread and butter of police and therefore they should be considered the three most important issues and score consequently in the top three. The results of that questionnaire are highlighted in Table 35. Accordingly most of the various options for inclusion within any proposed training courses were identified as you would expect with subjects such as powers of arrest and laws, supervision, officer survival and laws of evidence attaining high scores. While subjects such as psychology and multi-culturalism rated poorly.

The most significant result from this survey was these senior ranking police rated the importance of Crime Prevention ahead of other possible subjects as Officer Survival, Health and Team Spirit Building.

Unlike computer related crime issues, police and experienced criminal investigators have shown support for the inclusion of crime prevention within the Detectives Education Programme and therefore a level of acceptance of this issue as a tool for the reduction of crime. The question remains however as to how law enforcement can approach this principle of crime prevention and more specifically, fraud prevention considering that the main thrust of the current law enforcement response is based upon reacting to crime rather than attempting to prevent it.
8.6 Discussion of the results of the analysis of fraud offenders

There are a number of similarities when comparing the results highlighted in table 36 for computer fraud offenders, with those of table 5 for fraud offenders. The preference by the judicial system to punish convicted offenders by way of releasing that person into their own recognizance has continued. Table 36 identifies that 11 of the 28, or 39%, convicted offenders were sentenced in this manner. Furthermore only 3 of the cases attracted a custodial sentence thereby strengthening the trend identified in table 5. Again, these figures could explain the reasoning behind victims of fraud not reporting the crime to law enforcement to have the matter dealt with within the judicial system.

The large proportion of offenders, thirty-nine percent received a recognizance that allows the offender to be released, on most occasions unsupervised. That person must be of good behaviour for a period of time specified by the court and in that time should the person re-offend they would be recalled before the same magistrate or judge for a review of their previous sentence.

Eleven percent of offenders received only a fine for their actions that are self-explanatory while eleven percent of offenders received a community service order or section 556A. A community service order is an order by the magistrate or judge directing the offender to undertake a certain number of hours towards working on community projects such as cleaning cemeteries. A 556A is a situation with the offence is proven but due to the offender’s background and character or the circumstances of the offence the presiding magistrate or judge releases the offender with no punishment.

Seven percent of offenders received periodic detention. This sentence involves a certain number of hours where the offender must be incarcerated, usually for a
weekend, so that the offender can continue with employment. Eighteen percent of sentences were unknown.

The effectiveness or otherwise of the judicial system as a deterrent and a system of punishment of offenders is under suspicion if the data from table 36 is typical. Ninety-seven percent of all persons arrested received non-custodial sentences, in other words they walked conditionally free. Considering that fraud usually involves the theft of large sums of money, the crime and the punishment seem to be polarised and there seems to be little, if any, deterrent for would-be offenders. The scrutiny of the data displayed in these tables together with tables 4, 5 and 6 even though limited by way of reporting procedures, does provide an explanation for the reasons why the victims of fraud in New South Wales have chosen not to adhere to the traditional remedies through law enforcement and the judicial system.

Further analysis of this offender data reinforces the findings in chapter 8.2 from the survey of potential victims of fraud. In accordance with the survey the victim employed twenty-seven out of twenty-eight offenders and more importantly twenty-one out of a possible twenty-eight victims did not receive any compensation. From a fraud prevention viewpoint no female had a criminal history with only six males having no prior convictions. With that in mind it is interesting that persons within the age groups of, males forty to forty-nine and females thirty to thirty-nine, decide to offend in the middle stages of their lives. These figures compare with those in the survey conducted by the Association of Certified Fraud Examiners (1996) who identified male employees as the most likely group of persons to offend. Perhaps it could be indebtedness however, the sociological reasons for supposedly honest persons offending could be examined in further research.

The examination of this sample of offenders generates a number of questions namely:
1. What is the motivating force behind a female between thirty-one and thirty-nine, without any history of either fraudulent offences or any form of criminal background, to steal from her employer?

2. What is a more suitable approach to rectifying the losses caused by fraud when you consider that of the twenty-eight victims only seven of those were awarded any form of compensation?

3. Is the current criminal justice system effectively deterring would-be offenders from committing fraud when you consider that only one offender out of twenty-eight was given a custodial sentence and the majority of the remainder were given varying periods of good behaviour bonds?

The figures contained in table 37 also compare with the finding of the survey conducted by KPMG (1996) who found that the industries most likely to incur fraud are the banking and retail industries. In the case of table 37 twenty-nine percent of offenders were employed within the banking system with the next most vulnerable industry being retail with twenty-two percent of offenders. The government and insurance sectors were next with eleven percent of offenders followed by the hospital industry with six percent and the manufacturing industry with three percent. Other industries had eighteen percent of offences. While the sample of this survey is restricted by the availability of reported crimes it is nonetheless credible considering that unauthorised computer intrusions for financial gain would tend to concentrate on cash rewards and therefore favour the banking sector.

In order to effectively develop proactive computer fraud policies it is essential that high-risk industry groups and individuals are identified and targeted with the aim of minimising the offence.
8.7 Summary

The results from these surveys provide a possible explanation for the non-reporting of fraud offences by victims of crime and the declining incidence of fraud as identified in table 4. These are:

- Reported fraud offences and the resulting statistics relate to mostly government institutions where a compulsory reporting scheme is implemented,

- Dissatisfaction with the traditional solutions for fraud by victims of the crime,

- The needs of those victims of fraud varying from those offered by traditional law enforcement such as the recovery of stolen funds,

- A perceived lack of punishment of fraud offenders,

- Lack of compensation,

- Victims believing the future areas of risk to be computer related fraud,

- Doubts over the ability of law enforcement to be sufficiently skilled within the area of computer related fraud to be able to combat this emerging crime,

- Doubts over the desire of law enforcement to be responsible for this emerging crime and,

- Whether the cost of investigating this crime should be the responsibility of the taxpayer.

In order to address this situation an alternative to the current system of investigating and resolving fraud offences is required.
Chapter Nine  IMPLICATIONS OF THIS STUDY AND CONCLUSIONS

9.1 Introduction

9.2 An Alternative to the Current Investigation Methodologies

9.3 Conclusions

9.4 Further research

Previous chapters have established that the current and traditional responses for investigating fraud are not totally addressing the needs of the victims of this crime. This chapter discusses alternative measures that can be utilised to more effectively minimise the effects of fraud and to maximise fraud prevention policies. This chapter also provides a summary of the previous chapters, their implications and any future requirements for further research.
9.1 Introduction

In chapter one the goals of this research were identified and they were:

1. To examine the incidence, impact and changing nature of fraud,

2. To determine the attitudes of police investigators towards the investigation of fraud,

3. To determine the attitudes of police investigators towards the significance of the investigation of computer-related crimes,

4. To determine the needs of stakeholders compared with the service that is provided in the course of traditional criminal investigation, and

5. To seek alternatives to the current investigation methodologies.

In accordance with these goals the research has established that:

**Research Goal 1. To examine the incidence, impact and changing nature of fraud.**

An examination of fraud statistics has been undertaken in order to identify any trends in the reporting of fraud to law enforcement. These statistics were scrutinised to identify particular patterns of offenders and susceptibilities. A summary of the findings is;

- Fraud is an evolving crime and more recently the nature of the crime has been altered and impacted due to the advances in computing technology. See chapter 2 and 3.
• New offences have been created in accordance with these advances and the nature of traditional offences has also been altered. See chapter 2 and 3.

• The majority of fraud offences are not being reported to law enforcement. See chapter 2 and 7;

• Statistics indicate that fraud offences are on the decline. See chapter 4.

• Those offences that are reported appear to have been done so due to compulsory reporting rules. See chapter 7.

• The true cost and incidence of fraud can only be estimated due to the lack of reliable statistics. See chapter 4.

• The non-reporting of fraud offences appears due to dissatisfaction with the current solutions offered by traditional law enforcement. See chapter 7.

• The taxpayer carries the burden and social cost of investigating criminal offences. See chapters 4 and 5.

**Research Goal 2. To determine the attitudes of police investigators towards the investigation of fraud,**

It was identified in chapter one that a vital part of the complete package of responses toward the mitigation of fraud and white-collar crime in general is the reactive or investigative response. It was therefore necessary that the significance of investigating fraud offences was measured in order to determine the priority that criminal investigators give to investigating fraud offences when faced with managing multiple investigations. This research revealed:

• Criminal investigators perceive financial offences as less important than similar offences. See chapter 7;
Research Goal 3. To determine the attitudes of police investigators towards the significance the investigation of computer-related crimes

- The New South Wales Police Service does not recognise computer-related crimes as extensive. See chapter 5.

- The New South Wales Police Service does not warrant the training of all criminal investigators in the areas of computer-related crime in accordance with the above point. See chapter 5.

- New South Wales Police criminal investigators perceive computer-related offences as less significant than offences of a similar nature with far less financial and social impact. See chapter 7;

- Police appear not to have the widespread, necessary skills and training in the area of technical crimes. See chapter 4;

- The current investigative responses do not appear to be effective for responding to computer related crimes. See chapter 4;

Research Goal 4. To determine the needs of stakeholders compared with the service that is provided in the course of traditional criminal investigation

- Potential victims of fraud prefer to report matters to the police. See chapter 7;

- The services provided by law enforcement differ from those required by the potential victims of this crime. See chapter 7

- Potential victims of fraud require services that are currently outside of those provided by law enforcement. See chapter 7.
Research Goal 5. To seek alternatives to the current investigation methodologies

- Detectives consider fraud prevention training as a relevant issue for training future criminal investigators. See chapter 7.

- The New South Wales Police Service currently has a taxpayer-funded budget that is not effectively providing the level of service to the victims of fraud. See chapter 7.

Summary of the current situation

The New South Wales Police Service, like most other law enforcement agencies, is designed primarily for the reactive investigation of crimes, the apprehension of offenders and the public presentation of evidence at court for a hearing to determine the guilt or otherwise of that offender (New South Wales Police, 1995). As seen by the results identified in previous chapters and those of the survey of convicted offenders in chapter 7 and 8 this level of service provided by law enforcement does not satisfy the requirements of the victims of fraud. The results from the survey of convicted offenders highlights:-

- Only seven cases out of total of twenty-eight received some form of compensation.

- Only one offender received a term of imprisonment as a deterrent with the remainder receiving non-custodial sentences

- The public exposure of the circumstances of the offence and therefore the victim.

Further results from chapter 7 indicate that the victims of fraud;

- Still prefer to report matters to law enforcement,
• Do not seek public exposure of the circumstances and

• See the return of stolen funds as a priority.

According to this research the current solutions for the offence of fraud appear to be in conflict with those demanded by the victims and considering the above points it is arguable as to whether or not the individual and current traditional investigative procedures will ever successfully address the demands of victims of fraud.

In the process of addressing research goal 5 it is intended, by suggesting an alternative approach, the needs of the victims of fraud will be more adequately satisfied. At the same time those issues that are not present in current investigative methodologies will also be addressed together with an alternative to the current process of taxpayer-funded policing.

9.2 An Alternative to the Current Investigation Methodologies

In light of the identified the current strengths and weaknesses of traditional investigative procedures and in order to counteract the shortfalls highlighted identified by this research an alternative to the current methods of investigating fraud has been developed and highlighted in the following model.
The Model explained

It is the recommendation of the author that a combined and permanent multi-skilled joint task force be created between the commercial sector and law enforcement similar in nature to that of Task Force Choke that was formed in response to allegations of insurance fraud emanating from the earthquake in Newcastle in 1989. The stakeholders or potential victims within the commercial sector would initially fund this task force and they would also provide those skilled persons who are currently unavailable to law enforcement, such as lawyers, accountants and computer
specialists. The stakeholders would also provide access to specialist academics and university computing facilities. On the other hand law enforcement would provide skilled detectives as well as their investigative expertise to the task force. As a result the benefits to the commercial sector would be a reactive response in accordance with their desires identified in the survey rather than a piecemeal response that they currently possess. Law enforcement would benefit by obtaining accurate reporting statistics that could be used to target high-risk industries and groups. Overall there would be higher level of satisfaction and service on the part of the victims.

I see the greatest benefit of this innovative model being reaped by the taxpayer and victims of other crimes. Currently the police budget is being thinly stretched across a broad spectrum of crimes. If the major responsibility for funding and responding to fraud is given to this task force it would be reasonable to believe that the funds previously allocated to fraud could be re-directed to perhaps crimes of violence thereby providing a better response to those crimes. With greater resources those crimes could be concentrated upon with the ultimate goal of a reduction in offences.

Unlike traditional reactive policing the joint task force could utilise the accurate and up-to-date fraud statistics to provide fraud risk assessments and to implement fraud prevention programmes for the commercial sector and perhaps the government sector. This would provide some funding for the task force with the eventual aim that ventures of this nature would enable the task force to be self funding and more adaptive to further changes in technology.

It is still essential that the police maintain a response to fraud independent of the task force. For that reason, detectives on a patrol basis would still investigate minor fraud offences.

All those high-risk industries identified in chapter 5 and 7 such as the retail sector, banking and finance, together with insurance would be included within this task force.
The initial advantages of a combined task force of this nature are:

1. The cross-pollination of methodologies through the use of industry-specific and police specialists,

2. The creation of a fraud database that may provide industry-specific data and record incidents of fraud. This information has a number of uses from targeting potential fraud offenders in the process of fraud prevention programmes through to monitoring the incidence of fraud and therefore the success or otherwise of combined fraud programmes,

3. The financial burden of investigating fraud offences is no longer the sole responsibility of the taxpayer with part of the financial responsibility shifting to the victims of the crime. It is possible that public funding could be diverted from fraud to other areas of crime,

4. The cost of training police, particularly within the technical areas of computing, could be the responsibility of the commercial sector. This public funding could also be diverted to other areas of crime,

5. The availability of specialist human resources and equipment that may have previously been unavailable to law enforcement due to the scale of state-wide policing could also be the responsibility of the victims of fraud.

The above advantages solve a number of procedural issues identified in this research such as the lack of accurate data and the requirements for investigating complex and technical crimes. In order to address the problems identified in chapter 7 such as the importance placed upon the recovery of stolen funds a task force such as this would have to collaborate with task force lawyers in order to firstly, attempt to recover funds through compensation in the criminal courts or secondly and preferably, pursue the matter civilly through lawyers. Rather than having a limited number of reactive options at their disposal, as is the situation with traditional law enforcement, the task
force should be able to choose from a range of solutions to the offence and therefore
be given some latitude in decision-making. Corruption and the misuse of this latitude
could pose a problem however with the necessary reporting procedures and checks
implemented in the course of any prevention programme, those risks could be
minimised.

These choices should include:

- The traditional arrest of the offender and the subsequent criminal proceedings,

- The use of civil proceedings with a view to the recovery of stolen funds,

- An investigation with a negotiated settlement with a view to the recovery of
  stolen funds and the legal dismissal of the offender, and

- The ability to liaise with various industries to assist or to implement
  comprehensive fraud preventative and deterrence policies;

Control, confidentiality and discretion can be maintained on behalf of the victim in the
course of the investigation.
Fraud Prevention Programmes

According to detectives and victims of fraud in chapter 7 an important component in the overall package of responses to fraud includes fraud prevention. Both the Commonwealth Law Enforcement Board (1996) and Arthur Andersen (1996) believe that both the public and private sectors are under increasing competitive, regulatory and shareholder pressure to assess and manage their business risks more effectively. In the past investigators and management have used their skills and resources to investigate financial frauds and illegal acts after they have happened. While this reactive ability continues to be important, it seems to be a situation where investigators are throwing scarce resources into an area of crime in an attempt to cope with the volume of fraud offences. The logical starting point is to adopt preventative policies that are designed to minimise such problems and therefore avoid serious damage to their organisation’s reputation and shareholder wealth.

The proposed joint task force would also focus on fraud prevention together with overall business risks with the view to improving the corporation’s business performance by enhancing their processes to prevent, deter and detect fraud and reduce damage to the company’s reputation and by minimising the commission of the offence. Effective fraud prevention programmes are designed to counteract situations similar to those that were identified and highlighted in chapter 7 and 8 where a survey of convicted fraud offenders was examined. That survey highlighted twenty-two out of the twenty-eight offenders did not have a previous criminal record with no female having a previous criminal history and only six males with a criminal history and twenty-seven out of the possible twenty-eight offenders were employees of the victim.

With that available information it is possible to formulate fraud prevention strategies aimed directly at an organisation’s employees and more specifically male employees. Assuming that these persons were essentially good persons, what were the pressures
that forced them to commit crime? Was it drugs or gambling or lifestyle? If it was any of these influences fraud prevention strategies could target financial problems that employees may face, thereby reducing the risk of theft and subsequent reactive solutions.

**The Implementation of Fraud Prevention Strategies**

In the surveys conducted by KPMG (1997) and the Association of Certified Fraud Examiners (1996) which are highlighted in chapter four, there are a number of high-risk commercial industries, such as finance and manufacturing that are identified and considered susceptible to fraud. With this knowledge the first stage in a fraud prevention methodology would be to assess the fraud risks specifically applicable to that industry or organisation by having an intimate knowledge of the workings of that organisation.

Armed with this information it is possible to then determine the resources appropriate to allocate to the task of reducing the risk of fraud to an acceptable level. At the same time expenditure on fraud prevention measures is monitored to determine that it is adequate but not excessive and is focused on the areas of greatest exposure. It involves an:

1. **Evaluation of the organisation's specific business risks from fraud**;
2. **Identification of industry-specific and country-specific risks which merit attention**;
3. **The development of formal anti-fraud policies and reporting procedures and**;
4. A full business low-level review that involves an examination of the operations of the organisation to highlight “weak areas” to minimise the risk of fraudulent activity and an assessment of the level of computer security; Preventative programmes will not stop all persons offending. They are designed to offer an alternative to good persons who offend for whatever pressure they are experiencing, such as gambling or drug addictions or lifestyle problems and to act as impediments to make it difficult for persons to offend. Regardless of the success of fraud prevention procedures it is still necessary to have an investigative response and standard operating procedures in place to cover those situations where a person deliberately sets out to offend. If a conspiracy of employees consciously and deliberately set out to commit fraud there is very little that could stop them from doing so regardless of the effectiveness of an organisation’s controls. For that reason part of the fraud model must include a reactive response.

A Current Commercial Alternative

Since 1992 in the United States of America, Price Waterhouse has doubled its forensic ranks to 500; Coopers & Lybrand has increased its forensic staff more than fivefold to 380. Membership in the premier financial sleuthing organization, the Association of Certified Fraud Examiners in Austin, Texas, has more than tripled to 15,000 since 1991; about one-third are forensic accountants (McDonald, 1996).

In recent years, forensic accountants have been called in to unravel a string of high-profile cases, including the Daiwa Bank Ltd., Barings Bank and Bank of Credit & Commerce International scandals. Forensic accountants at KPMG Peat Marwick, Arthur Andersen and Price Waterhouse have scoured Swiss bank accounts for assets deposited by victims of Nazi persecution. Mounting pressure on accounting firms to
fight white-collar crime more aggressively is a major factor behind burgeoning demand for forensic accountants and investigators.

A distinct disadvantage in using predominantly commercial consultants is again the lack of available statistics that can be utilised for the development of fraud prevention policies. With a large number of independent and competitive consultants providing separate responses for victims it would be difficult if not impossible to amass combined statistics.

Regardless of the current effectiveness of law enforcement it has been indicated by this research that victims of fraud still desire certain incidents of fraud to be resolved by criminal prosecution. By creating a task force that utilises a combination of commercial sector and law enforcement specialists it provides a broader response rather than only those provided by commercial consultants.

9.3 Conclusions

Not all victims of fraud wish to have the offender arrested and prosecuted though the criminal courts. As earlier indicated in chapter seven most organisations, eighty per cent, are concerned about the impact that publicising a fraud may have on the reputation of the company. Other concerns which deter victims from reporting fraud also include:

1. A possible fall in the share price of publicly listed companies as seen in the recent losses by a large Australian company after a high level management dispute wiped six billion dollars off the share price of the company;

2. A fall in consumer confidence and market loss and;

3. Possible dismissal for being held responsible for the fraud.
In order to provide a service to the potential victims of fraud and to overcome the shortfalls that have been highlighted by this research, traditional law enforcement or more particularly the government of the day, should concede that their present system of responding to fraud does not satisfy the needs of the victims who need:-

1. A flexible and adaptive investigation methodology that can keep pace with changing social, legal and commercial issues;

2. Suitably skilled and trained investigators who can effectively deal with ongoing complex financial and technical issues;

3. Effective financial, human and organisational support and resources;

4. Effective professional liaisons and;

5. The ability to implement comprehensive preventative and deterrence policies

Combining the talents of the commercial sector with those of law enforcement can only provide the level of service those victims of fraud demand. In doing so such a combined response should effectively address the evolving nature and the financial and social costs of this constantly evolving crime.

Traditional law enforcement is the first line of defence in the war against crime and it is stretched to its extreme. With added pressures such as further rapid advancements in computing technology, there will be even further demands on limited resources available to law enforcement and the judicial system in the not too distant future.

Research has revealed that anything up to 90% of fraud offences are not reported to law enforcement and perhaps one of the reasons for this could be dissatisfaction with the current solutions offered by law enforcement. The police cannot be everywhere. More so than ever, law enforcement agencies require the cooperation and assistance of the community in order to control crime. This is especially the case in the climate of accountability and fiscal austerity.
There is now a viable alternative and support to law enforcement that achieves the same results by responding to the needs of stakeholders while operating with confidentiality, discretion and within the control of the client. Private companies have formed multi-skilled team of fraud specialists and these teams include lawyers, investigators, risk managers and computer crime specialists who have the necessary resources, experience and industry credibility to protect, prevent and respond to fraud and illegal acts. By combining these resources with those of law enforcement it should provide a formidable response to this crime while having the added benefit of reducing the financial strain on the public purse.

The model that has been proposed by this research is primarily the privatisation of an historical part of a law enforcement function. I see this as the evolution of fraud investigation and prevention. Law enforcement must adapt to its circumstances and in doing so it must be flexible to change or the service that it provides will be nothing but a flag waving exercise.

9.4 Further Research

Following on from the findings of this thesis further research should be undertaken in order to determine the reasons for the attitudes of both detectives and student police officers towards complex and serious financial offences as well as their resistance to issues of multi-culturalism and ethics training. These surveys of the police sector were undertaken prior to the Wood Royal Commission and perhaps the attitude towards ethics may have altered since corruption was exposed however the Wood Royal Commission did not touch on issues of racism or ignorance of other cultures.

Further areas to be scrutinised should be the success or otherwise of the commercial sector in solving serious and complex fraud issues. It should be ascertained whether or
not some of the responses to fraud from within the commercial sector are just a matter of revenue raising with the major issues still swept under the carpet and unresolved.

The never ending cycle of researching technical security issues as a deterrent to would-be intruders must be an on-going project in order to just keep pace with criminals. No sooner do we create supposedly secure environments than they are violated and even though this issue could be compared to a dog chasing its tail, while there are persons who would take advantage of weakness in existence it is imperative that we follow this course of action.

Perhaps the most important area of research that should be considered further is the role of the judiciary as a deterrent to fraud. Many questions arise from this research such as:

1. Are the sentences handed down by the Courts in relation to fraud offenders merely an indication of a trend towards leniency by the Courts or is it only particular to fraud offenders?

2. Should the criminal justice system lean more towards compensating victims of financial offences rather than merely punishing the offender?

3. For complex frauds should the criminal justice system dispense with juries who could not be expected to understand the intricacies of these crimes and opt for a panel of specialist judges?

Most importantly as society commences a new millenium the general community should feel comfortable knowing that the use of taxpayer funds and the system for the investigation of fraud should more than adequately address the current and future problems that are associated with fraud. The question is whether or not the decision-makers will confront this issue and deal with it accordingly.
BIBLIOGRAPHIES AND REFERENCES


COMPLEX COMMERCIAL FRAUD CONFERENCE. (1991): Australian Institute of Criminology, Canberra A.C.T.


HOMER OFFICE RESEARCH AND STATISTICS DIRECTORATE - UK. (1997):
http://www.homeoffice.gov.uk/rsd/xcrime2.htm


Accountancy Books; The Institute of Chartered Accountants in England and Wales. UK.


INTERNATIONAL CRIMINAL POLICE ORGANIZATION: (1995): Interpol:


Page 15 June 27.


November 19 page 36.

KPMG (1996): International Fraud Report April. KPMG.

KPMG (1997): 1997 Fraud Survey. KPMG


NEW SOUTH WALES CRIMES ACT (1901): New South Wales Government


THAMES VALLEY POLICE. (1996): Computer Crime Unit


Appendix 1  1997 Fraud and Computer Related Crime Survey

The responses provided for this survey are strictly confidential. At no stage can or will the participants be identified. Thank you for taking the time to complete this survey.

1  What position do you currently hold?
   a  Chief Executive Officer
   b  Chief Financial Officer
   c  Senior Management/Director
   d  Middle Management
   e  Audit
   f  Other

2  Which industry category best describes your business operation?
   a  Education
   b  Service provider
   c  Financial sector
   d  Manufacturing
   e  Insurance
   f  Government
   g  Retail
   h  Other

3  Is your business:
   a  A publicly owned company
   b  A privately owned company
   c  A government/statutory body
   d  Other

4  In the past five years, approximately how many known incidents of fraud has your company suffered? If none please go to question 12:
5 What was the approximate total loss associated with this fraud:
   a Less than $10,000
   b Between $10,000 & $100,000
   c Between $100,000 & $1 million
   d Between $1 million & $2 million
   e More than $2 million
   f Don't Know

6 How much of this was recovered:
   a None
   b 25%
   c 50%
   d 75%
   e 100%

7 How was the fraud discovered:
   a Internal Audit
   b External Audit
   c Whistleblowers programme
   d Accidentally
   e Investigation
   f Other
8 Was the offender in this case an employee?
Y/N

9 If yes to the above, what type of employee?
   a  Clerical/administration
   b  Middle management
   c  Sales
   d  Other
   e  Senior Management

10 If your response to Q9 was "no" was the offender in:
   a  Sales
   b  Clerical/administration
   c  Middle Management
   d  Senior Management
   e  Other

11 Was the matter reported to the Police?
Y/N

12 If a fraud occurred within your organisation, which of the following would be your motivation to report the matter to the Police?
   a  To have the offender punished
   b  Compulsory policy
   c  The only known course of action
   d  Other
8 Was the offender in this case an employee?
   Y/N

9 If yes to the above, what type of employee?
   a  Clerical/administration
   b  Middle management
   c  Sales
   d  Other
   e  Senior Management

10 If your response to Q9 was "no" was the offender in:
   a  Sales
   b  Clerical/administration
   c  Middle Management
   d  Senior Management
   e  Other

11 Was the matter reported to the Police?
   Y/N

12 If a fraud occurred within your organisation, which of the following would be your motivation to report the matter to the Police?
   a  To have the offender punished
   b  Compulsory policy
   c  The only known course of action
   d  Other
13 Again, if a fraud occurred within your organisation, which of the following would be your motivation NOT to report the matter to the Police? Please rank the following responses with the main reason you did would not report the matter to the Police given the ranking of “1” and the least the ranking of “10”:  

 a  A desire not to expose your business to possibly adverse publicity  
 b  A desire not to risk possible shareholder backlash  
 c  A lack of confidence in the criminal justice system  
 d  A desire not to become involved in lengthy Court proceedings  
 e  Loss of control over the outcome of the investigation  
 f  Loss of control over the confidentiality of the investigation  
 g  A desire not to risk dismissal for being held responsible for the fraud  
 h  A lack of confidence in the remedies offered by the civil courts  
 i  A lack of confidence in the sentences given to offenders in the Criminal Courts.  
 j  Other

14 Again, if a fraud occurred within your organisation, which ONE of the following issues would you feel is the MOST important:  

 a  The criminal punishment of the offender ie imprisonment, community service, bond etc  
 b  The resignation or dismissal of the employee from the company  
 c  The recovery of stolen funds  
 d  The civil punishment of the offender ie litigation  
 e  The reputation of the business  
 f  The removal of the cause of the problem

15 Again, if your company was a victim of fraud today, which ONE of the following issues would you feel is the MOST appropriate for your organisation:  

 a  Automatically report the matter to the Police and therefore have the matter dealt with in the criminal courts  
 b  Legally dismiss the offender and pursue a negotiated compensation  
 c  Allow the offender to resign with benefits  
 d  Pursue a civil remedy  
 e  Other
In your opinion, will the incident of fraud increase over the next five years in Australia:
Y/N/Don't Know

If you answered yes, what do you think this increase will be attributed to:

a. Deficiencies in fraud prevention programmes
b. Increased financial pressures on individuals
c. Lack of internal controls
d. Don't Know

If you think the incidence of fraud will increase, in what areas do you think this will occur:

a. Embezzlement by employees
b. Management fraud ie kickbacks
c. Computer fraud
d. Don't Know

Does your organisation have a formal reporting framework for fraudulent activity to be communicated to those responsible for establishing fraud prevention controls:
Y/N/Don't Know

Does your organisation have a fraud prevention/deterrence programme?
Y/N/Don't Know

If yes, do you believe that the fraud prevention programme adequately addresses your organisation's exposure to fraud risk:
Y/N/Don't Know

Does your Board of Directors take an active interest in the development and execution of fraud prevention policies:
Y/N/Don't Know
23 Which ONE of the following courses of action would you consider if your company was a victim of fraud:

a An investigation that would gather evidence and then hand the matter over to the Police for criminal prosecution and punishment

b An investigation that would gather evidence and then hand the matter over to a solicitor for a civil prosecution

c An investigation that would gather evidence and then hand the matter over to a solicitor for a negotiated settlement and the dismissal of the offender

d Other
Appendix 2    CONFIDENTIAL QUESTIONNAIRE

Please would you complete the following confidential and anonymous questionnaire.
The results will be analysed and published in the Australian Police Journal. (Circle answers as required.) THANK YOU FOR YOUR PARTICIPATION.

1. What rank are you?..................................................................................................................

2. What sex are you? Male/Female

3. What age are you? 20-29, 30-39, 40-49, 50-65,
Other?........................................

4. What is your current marital status? Married/Unmarried

5. In which country were you born?..........................................................................................

6. Did you complete your HSC? Yes/No

7. Do you have a Degree? Yes/No

8. If "yes", which
Degree?...................................................................................................................

9. If so, in which specialty was your undergraduate study?............................................

10. In which section are you now employed?...........................................................................

11. How long have you been employed there?........................................................................

12. What was your earlier occupation?....................................................................................
13. Please number from 1 -15, what you consider to be the 15 most serious offences. (Give the most serious offence the score of "1".)

Arson
Breaking and entering
Computer Fraud
Credit Card Fraud
Domestic Violence
Drug Offences
Drunk Driving
Embezzlement
Malicious Damage
Murder
Rape
Shoplifting
Stealing
Traffic Offences
White Collar Crime

14. Do you believe that hacking into computer systems is acceptable? Yes/ No/ Don't Know
Appendix 3

CONFIDENTIAL QUESTIONNAIRE

There has been considerable debate over the content of the Detective's Education Programme. Here is your opportunity to anonymously voice your opinion as to what you believe should or should not be included within the programme and what should be emphasised. It must be stressed that your responses are strictly confidential.

1. What rank are you? Sgt........S/C........Cst 1/c........Cst........

2. Are you designated? Partially through your course.............., Yet to start

3. How many years of service do you have? 0-5......,6-10......, 11-15......,16-20......,

   More than 20 years......

4. Do you have criminal investigation experience at Patrol level......, Region level......, Task Force level......, State level......

5. Please number from 1 to 15 these issues giving what you consider to be the most important issue the ranking of "1" and the least important issue the ranking of "15".

   Laws of Evidence
   Psychology
   Crime Scenes
   Ethics training
   Powers of Arrest
   Supervision
   Use of Firearms
   Multiculturalism
Team Spirit Building
Officer Survival
Health
Role Play
Acts of Parliament
Crime Prevention
Guest Lecturers

6. Please finish these questions with one word answers.

I would like to see more...........................................within the D.E.P

Please fax your response to eaglenet 67416 or mail it to Gosford D.O for the attention of Detective Senior Constable Paul Sullivan. THANK YOU FOR YOUR PARTICIPATION.
### Appendix 4  The Statistical Analysis of the classification of offences according to perceived seriousness by Detectives

Contingency Table from Table 33.

<table>
<thead>
<tr>
<th>Crime</th>
<th>Expected Frequencies</th>
<th>Relative Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Murder</td>
<td>15.466667</td>
<td>10.156322</td>
</tr>
<tr>
<td>Rape</td>
<td>15.466667</td>
<td>10.156322</td>
</tr>
<tr>
<td>Domestic V</td>
<td>15.466667</td>
<td>7.770115</td>
</tr>
<tr>
<td>Drug Offenses</td>
<td>15.466667</td>
<td>1.3287356</td>
</tr>
<tr>
<td>Stealing</td>
<td>15.466667</td>
<td>1.2899425</td>
</tr>
<tr>
<td>Break &amp; En.</td>
<td>15.466667</td>
<td>1.3287356</td>
</tr>
<tr>
<td>Shoplifting</td>
<td>15.466667</td>
<td>0.0183908</td>
</tr>
<tr>
<td>Traffic Offr.</td>
<td>15.466667</td>
<td>0.0183908</td>
</tr>
<tr>
<td>Malicious Int.</td>
<td>15.466667</td>
<td>1.2899425</td>
</tr>
<tr>
<td>Drunk Driv.</td>
<td>15.466667</td>
<td>0.7770115</td>
</tr>
<tr>
<td>Embezzlement</td>
<td>15.466667</td>
<td>1.9321839</td>
</tr>
<tr>
<td>Credit Card</td>
<td>15.466667</td>
<td>10.048563</td>
</tr>
<tr>
<td>Computer Off.</td>
<td>15.466667</td>
<td>2.7073756</td>
</tr>
<tr>
<td>White collar</td>
<td>15.466667</td>
<td>0.0183908</td>
</tr>
<tr>
<td>Arson</td>
<td>15.466667</td>
<td>1.3287356</td>
</tr>
</tbody>
</table>

Total 232 147 41 420 232 147 41 43.172414 64.734694 45.707317

Chi-squared = 153.61442, with 28 degrees of freedom.
Critical value at 0.005 level is 50.994.
Appendix 5  The Statistical Analysis of the classification of offences according to perceived seriousness by Student Police Officers

<table>
<thead>
<tr>
<th>Crime</th>
<th>Ranking</th>
<th>1-5</th>
<th>6-10</th>
<th>&lt;10</th>
<th>Total</th>
<th>Expected Frequencies</th>
<th>Relative Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Murder</td>
<td></td>
<td>478</td>
<td>1</td>
<td>3</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>553.27854 155.69482 147.67983</td>
</tr>
<tr>
<td>Rape</td>
<td></td>
<td>474</td>
<td>4</td>
<td>4</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>538.96913 149.78994 145.7254</td>
</tr>
<tr>
<td>Domestic Violence</td>
<td></td>
<td>379</td>
<td>82</td>
<td>21</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>254.22035 36.329513 114.49194</td>
</tr>
<tr>
<td>Drug Offences</td>
<td></td>
<td>271</td>
<td>149</td>
<td>62</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>58.949166 0.4787264 54.643828</td>
</tr>
<tr>
<td>Stealing</td>
<td></td>
<td>52</td>
<td>280</td>
<td>150</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>82.531834 94.871286 0.0853621</td>
</tr>
<tr>
<td>Break &amp; Enter</td>
<td></td>
<td>106</td>
<td>306</td>
<td>70</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>24.517107 139.492177 45.517877</td>
</tr>
<tr>
<td>Shoplifting</td>
<td></td>
<td>21</td>
<td>100</td>
<td>361</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>131.2739 21.104652 279.94791</td>
</tr>
<tr>
<td>Malicious Damage</td>
<td></td>
<td>101</td>
<td>266</td>
<td>115</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>28.453493 74.395963 9.7095994</td>
</tr>
<tr>
<td>Drunk Driving</td>
<td></td>
<td>268</td>
<td>158</td>
<td>56</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>55.475817 0.0006154 62.035091</td>
</tr>
<tr>
<td>Embezzlement</td>
<td></td>
<td>39</td>
<td>219</td>
<td>224</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>101.60115 23.838792 32.242732</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td></td>
<td>22</td>
<td>126</td>
<td>334</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>129.52582 6.3679959 211.79684</td>
</tr>
<tr>
<td>Computer Fraud</td>
<td></td>
<td>36</td>
<td>157</td>
<td>289</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>106.28297 0.0030059 119.30255</td>
</tr>
<tr>
<td>Arson</td>
<td></td>
<td>227</td>
<td>223</td>
<td>32</td>
<td>482</td>
<td>170.69028 157.68848 153.62125</td>
<td>18.576249 27.050772 96.286992</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>2560</td>
<td>2365</td>
<td>2304</td>
<td>7229</td>
<td>2280.0233 766.28378 1640.7180</td>
<td>4687.0251</td>
</tr>
</tbody>
</table>

Chi-squared = 4687, with 28 degrees of freedom.
Critical value at 0.005 level is 50.994.
Appendix 6  The Statistical Analysis of the responses from Detectives regarding possible subjects for detective training.

<table>
<thead>
<tr>
<th>Crime</th>
<th>Ranking</th>
<th>Expected Frequencies</th>
<th>Relative Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Murder</td>
<td>1-5</td>
<td>17.066667 17.133333 16.8</td>
<td>63.551042 15.191699 16.8</td>
</tr>
<tr>
<td>Rape</td>
<td>2</td>
<td>17.066667 17.133333 16.8</td>
<td>13.301042 0.0010376 13.752381</td>
</tr>
<tr>
<td>Domestic V</td>
<td>48</td>
<td>17.066667 17.133333 16.8</td>
<td>56.066667 11.658625 16.8</td>
</tr>
<tr>
<td>Drug Offense</td>
<td>2</td>
<td>17.066667 17.133333 16.8</td>
<td>13.301042 0.573022 19.716667</td>
</tr>
<tr>
<td>Stealing</td>
<td>44</td>
<td>17.066667 17.133333 16.8</td>
<td>42.340417 5.992255 16.8</td>
</tr>
<tr>
<td>Break &amp; En</td>
<td>5</td>
<td>17.066667 17.133333 16.8</td>
<td>8.5315104 14.693645 0.859238</td>
</tr>
<tr>
<td>Shoplifting</td>
<td>21</td>
<td>17.066667 17.133333 16.8</td>
<td>0.9065104 0.2033722 2.002381</td>
</tr>
<tr>
<td>Traffic Off</td>
<td>0</td>
<td>17.066667 17.133333 16.8</td>
<td>17.066667 8.592477 50.752381</td>
</tr>
<tr>
<td>Malicious L</td>
<td>6</td>
<td>17.066667 17.133333 16.8</td>
<td>7.1760417 0.2033722 5.0380952</td>
</tr>
<tr>
<td>Drunk Driv</td>
<td>19</td>
<td>17.066667 17.133333 16.8</td>
<td>0.2190104 5.6819715 8.2889052</td>
</tr>
<tr>
<td>Embezzlement</td>
<td>3</td>
<td>17.066667 17.133333 16.8</td>
<td>11.59401 1.3823606 5.0380952</td>
</tr>
<tr>
<td>Credit Card</td>
<td>3</td>
<td>17.066667 17.133333 16.8</td>
<td>11.59401 4.5885863 1.6095238</td>
</tr>
<tr>
<td>Computer F</td>
<td>38</td>
<td>17.066667 17.133333 16.8</td>
<td>25.676042 3.8609298 9.752381</td>
</tr>
<tr>
<td>White collar</td>
<td>5</td>
<td>17.066667 17.133333 16.8</td>
<td>8.5315104 6.8920882 0.0857143</td>
</tr>
<tr>
<td>Arson</td>
<td>10</td>
<td>17.066667 17.133333 16.8</td>
<td>2.9260417 5.6819715 0.4666667</td>
</tr>
<tr>
<td>Total</td>
<td>256</td>
<td>257 252 765</td>
<td>256 257 252</td>
</tr>
</tbody>
</table>

Chi-squared = 535.91, with 28 degrees of freedom.
Critical value at 0.005 level is 50.994.