USE OF THESES

This copy is supplied for purposes of private study and research only. Passages from the thesis may not be copied or closely paraphrased without the written consent of the author.
REGULATING CYBERSPACE: AN APPROACH TO STUDYING CRIMINAL BEHAVIOUR ON THE INTERNET

Sascha Walkley BA (Hons)

A thesis submitted for the degree of Doctor of Philosophy of The Australian National University

May, 2005
DECLARATION

I certify that this thesis does not incorporate without acknowledgement any material previously submitted for a degree or a diploma in any University and that to the best of my knowledge and belief it does not contain any material previously published or written by any other person except where due reference is made in the text.

Sascha Walkley
# Table of Contents

Declaration ii  
List of Tables vii  
List of Figures vii  
Acknowledgements viii  
Abstract x  

Chapter 1: Introduction 1  
1.1 The Internet Age 1  
1.2 The Discipline of Criminology 3  
1.3 Thesis Aims and Objectives 5  
1.4 Thesis Approach and Methodology 5  
1.5 Thesis Structure 9  

Chapter 2: The Concept and Study of White-Collar Crime – A Review of the Literature 13  
2.1 Introduction 13  
2.2 Early Influences on the Study of White-Collar Crime 14  
2.3 The Pre-Eminent Scholar of White-Collar Crime – Edwin Sutherland 15  
2.3.1 Sutherland’s Seminal Study of Corporations 17  
2.4 Defining ‘White-Collar Crime’ – Past and Present Contributions and Contestations 19  
2.4.1 Redefining the Concept of White-Collar Crime 21  
2.4.2 Offender and Offence-Based Definitions of White-Collar Crime 24  
2.4.3 Conceptual Challenges to the Study of White-Collar Crime 29  
2.5 The Study of White-Collar Crime – Periods of Change 31  
2.6 Studies in White-Collar Crime 33  
2.6.1 Corporate Crime 33  
2.6.2 Seminal Studies in Corporate Crime 34  
2.6.3 Occupational Crime 39  
2.7 Ways Forward – Refining the Typology of White-Collar Crime 42  
2.8 Summary 42
Chapter 3: Theories of Criminal Behaviour and Their Relationship to the Study of White-Collar Crime

3.1 Introduction

3.2 Traditional Paradigms of Criminology
   3.2.1 Classical School of Criminology.................................................. 44
   3.2.2 Positivist School of Criminology.................................................. 48
   3.2.3 The Chicago School........................................................................ 52

3.3 Towards a Paradigm for Understanding Crime and Criminal Behaviour
   3.3.1 Theories of Crime and Criminal Behaviour – A Contemporary Profile............................... 59

3.4 Constitutional Learning Theory

3.5 Differential Association Theory

3.6 Strain Theory

3.7 Techniques of Neutralisation

3.8 Routine Activity Theory

3.9 General Theory of Crime

3.10 Summary

Chapter 4: The Next Generation – Computer and Cyber crime

4.1 Introduction

4.2 Defining Computer Crime
   4.2.1 Defining Cyber Crime................................................................... 90

4.3 The Origin of the Internet

4.4 The Nature of Computer Crime – A Review of the Focal Periods
   4.4.1 Computer Crime – a Fifty Year Journey........................................ 95
   4.4.2 The Criminalisation of Computer Crime..................................... 101
   4.4.3 The Changing Perception of Hackers........................................... 104

4.5 The Emergence of Cyber Crime
   4.5.1 Criminogenic Attributes of the Internet....................................... 113

4.6 Diverse Forms of Cyber Crime – A Traditional and New Modus Operandi
   4.6.1 Cyber Stalking ............................................................................. 118
   4.6.2 Internet Sex Crimes against Children and Youth............................ 120
   4.6.3 Cyber Terrorism.......................................................................... 122
   4.6.4 Internet Fraud............................................................................... 123
   4.6.5 Unauthorised Access to Computer Programs and Files.................. 127
   4.6.6 Computer Viruses....................................................................... 127
   4.6.7 Computer Worms....................................................................... 129

4.7 Summary

Chapter 5: Theories of Crime and Criminality and their Relationship to the Internet

5.1 Introduction
5.2 A Cyber Perspective of Criminal Behaviour .................................................. 132
5.3 Differential Association Theory ................................................................. 132
  5.3.1 Hacking .................................................................................................. 133
  5.3.2 Internet Piracy ....................................................................................... 140
  5.3.3 Internet Sex Crimes against Children and Youth .............................. 145
  5.3.4 Internet Fraud ..................................................................................... 150
5.4 Strain Theory ............................................................................................... 157
  5.4.1 Innovation ............................................................................................ 158
  5.4.2 Rebellion .............................................................................................. 167
5.5 Techniques of Neutralisation ....................................................................... 169
  5.5.1 Denial of Responsibility ..................................................................... 170
  5.5.2 Denial of Injury ................................................................................... 173
  5.5.3 Denial of the Victim ........................................................................... 178
  5.5.4 Condemnation of the Condemners ..................................................... 180
  5.5.5 Appeal to Higher Loyalties .................................................................. 183
5.6 General Theory of Crime ........................................................................... 185
  5.6.1 Low Self-Control ............................................................................... 186
  5.6.2 The Correlation of Crime and Age ..................................................... 188
5.7 Routine Activity Theory ............................................................................ 191
  5.7.1 A Supply of Motivated Offenders ....................................................... 192
  5.7.2 The Availability of Suitable Targets .................................................. 193
  5.7.3 The Absence of Capable Guardianship ............................................. 195
  5.7.4 Testing Routine Activity Theory ......................................................... 197
5.8 Summary ...................................................................................................... 211

Chapter 6: Criminal Behaviour on the Internet – the Use of Trust ................. 213
6.1 Introduction .................................................................................................. 213
6.2 Trust Violation Theory ................................................................................ 213
6.3 Lying ............................................................................................................ 214
  6.3.1 Phishing ................................................................................................ 215
  6.3.2 Auction Fraud ..................................................................................... 220
  6.3.3 Internet Sex Crimes against Children and Youth .......................... 223
  6.3.4 Misuse of Personal information ......................................................... 224
  6.3.5 Cyber Harassment and Stalking .......................................................... 226
6.4 Self-Dealing ................................................................................................ 227
  6.4.1 Misuse of Personal Information .......................................................... 228
  6.4.2 Identity Theft ....................................................................................... 229
  6.4.3 Insider Trading .................................................................................... 230
6.5 Corruption ................................................................................................... 231
  6.5.1 Espionage ............................................................................................. 231
6.6 Role Conflict ................................................................................................ 232
  6.6.1 Internet Piracy ..................................................................................... 233
  6.6.2 Espionage ............................................................................................. 233
6.7 Summary ...................................................................................................... 236
Chapter 7: A Synthesis of Cyberspace – Networks of Trust on the Internet

7.1 Introduction 237
7.2 The Concept of Trust 237
  7.2.1 What is Trust? 238
  7.2.2 Trust - A Terrestrial and Virtual Perspective 241
7.3 Trust and the Internet – An Empirical Perspective 244
7.4 Regulating the Internet 248
  7.4.1 Self-Regulation 251
  7.4.2 Market Approaches 258
  7.4.3 State-Based Regulation – Law Enforcement 261
  7.4.4 Global Cooperation 264
7.5 Examples of Regulatory Approaches to Controlling Behaviour on the Internet 266
  7.5.1 Auction Fraud 266
  7.5.2 Internet Securities Fraud 269
7.6 Summary 272

Chapter 8: Discussion and Conclusion 273

8.1 Criminal Behaviour on the Internet – Summary of Findings and Implications of Research 273
8.2 Issues and Future Challenges in Regulating Cyberspace 278

Bibliography 282
LIST OF TABLES

Table 3.1  Merton’s Typology of Modes of Individual Adaptation .................................. 70
Table 4.1  Reported Incidents of Computer Crime ......................................................... 98
Table 4.2  Computer Related Crimes Reported in Hong Kong 1995-2003 ................. 100
Table 4.3  Traditional Crimes – Traditional and New Methods .................................. 117
Table 4.4  Usage of Internet payment Systems in Four Countries - July 2000 .......... 126
Table 5.1  Analysing the Applicability of Techniques of Neutralisation Against Cyber Crime .................................................................................... 185
Table 5.2  Phishing Attacks by Targeted Company: December 2003 – May 2004 210
Table 7.1  Concerns Covered in Different National Codes of Conduct in the European Union (EU) ................................................................. 255

LIST OF FIGURES

Figure 4.1  Virus Prevalence Survey 2002 .................................................................. 128
Figure 5.1  DrinkOrDie's Organisational Structure ...................................................... 143
Figure 5.2  World Wide Internet Population ................................................................. 193
Figure 5.3  Types of Attack or Misuse ............................................................................. 194
Figure 5.4  Security Technologies Used ....................................................................... 200
Figure 6.1  Hijacked Brands by Month .................................................................... 217
ACKNOWLEDGEMENTS

No doctoral student walks alone through the forest of scholarship. The path on which they tread is illuminated by scholars who light the way with a sure and steady hand. My path has been no different and much is owed to their wisdom, which is so freely given. For this, I am indebted to Professor Kerry Carrington, my mentor and friend, who opened my eyes to the fascinating world of criminology, and who first led me onto the path which I now tread with such fascination.

Peter Grabosky has led me through the thickets and into the arcane world of cyber crime with the profound knowledge and learning of the truly expert. Peter's dedication to the pursuit of excellence in his academic life has inspired me in my own research. He has kept me utterly focused on completing this thesis. I am most grateful for his guidance.

With equal significance, Professor John Braithwaite has given his time freely throughout my period of research. John has the rare human gift of knowing what to say and when to say it in the difficult moments of a student's life. John has been the steadying hand of the wise guide.

These three important guides have been instrumental in leading me through the paths unknown and extended my horizons. No student could be more grateful.

I have also been fortunate enough to have the support and wisdom of Dr. Marian May. Marian has been a wonderful mentor and friend, and she has refined my skills with the true judgement of experience. Marian's knowledge has also me afforded me a great research experience at ANU for which I am truly grateful.

Thank you to Dr. Gregor Urbas who provided valuable commentary and suggestions on my draft. I must also thank Dr. Valerie Braithwaite for giving her time freely to listen and provide feedback on my research.

No student's life is complete without important friendships being formed. Many wonderful friends, colleagues, and mentors have enriched my experiences and over the past years have provided encouragement and support. I must particularly thank Tali Gal, Jenny Job, and Susan Cochrane who have also shared the highs and lows of every student.
Tali has opened her family and wonderful home to me. Whilst away from my family, she has been a pillar of strength, particularly when life’s challenges can be confusing. Tali often reminded me of the many other joys in life, providing delicious home cooked meals, and much-needed support.

Jenny has also welcomed me into her home and been a shining light for my thesis. The many exchanges of ideas, advice in moments of confused thought, and continued encouragement of my research have been most valuable.

Susan Cochrane has selflessly provided commentary on draft chapters, support and many enjoyable lunches whilst completing her own PhD.

Undertaking a thesis inevitably affects those close to you. I am incredibly fortunate to have such a wonderful, supportive, and loving family - my parents, Ross and Elly, sister Elissa, grandparents, Jean and Pora, and my deceased grandfather, Leslie Walkley. My family has always supported me and given selflessly, of which not enough can be said and written. I thank my parents and sister for also providing invaluable commentary and feedback on drafts of my thesis.
ABSTRACT

The Internet has opened up a Pandora’s Box of crime: the proliferation of traditional as well as the emergence of new forms of crime; the extension of opportunities and methods to carry out crime; new offender profiles; and the ease of recruiting willing participants in global organised networks. Central themes that explain criminal behaviour on the Internet are motivated offenders, availability of suitable targets, absence of capable guardianship, and strategies of trust violation.

This thesis provides an exploratory analysis of criminal behaviour by examining five promising criminological theories against a diverse range of cyber crimes. Much of the scholarship of computer and cyber crime initially focused on defining new types of crime and analysing the behaviour of particular offender groups, such as hackers, pirates, and paedophiles. Despite the significance of research in these areas, few studies have sought to examine criminal behaviour through the lenses of existing theories, and identify whether there are criminological attributes specific to the Internet that explain the rise and proliferation of cyber crime.

The study of white-collar crime is traced and the various contributions that have shaped its definition and development over the past seven decades are outlined. The thesis questions whether traditional categories of white-collar crime and criminals can adequately embrace new forms of crime such as cyber crime. It argues that the study of criminal behaviour should not be confined to pre-existing criminological categories of conventional crime on the one hand and white-collar crime on the other.

The growth and proliferation of computer and cyber crime is analysed. A broad range of theories of criminal behaviour are assessed in terms of whether they can explain cyber crime. This analysis concludes that Cohen and Felson’s (1979) routine activity theory and Shapiro’s (1990) theory of trust violation are most fertile for explaining different forms of cyber crime. This is because three criminogenic attributes of the Internet are found to assist in the facilitation and growth of cyber crime: anonymity, multiplicity, and target exploration. Moreover, it is found that violation of trust is a significant element that assists in the commission of cyber crime. Trust violations on the Internet are patterned. The following types of trust violation recurrently appear in the literature: lying, self-dealing, corruption, and role conflict.
As the study of crime and criminal behaviour on the Internet gathers momentum, the thesis raises a number of new questions about its effective methods of control, and the future role of regulatory networks on the Internet. Given the Internet's global nature and lack of harmonised laws, an approach that emphasises credible self-regulation, well attuned market strategies, law enforcement, and mutual global cooperation will be necessary to control the phenomenon of cyber crime. In doing so, this thesis opens up alternative paths to understanding trust and guardianship in the Internet age.
CHAPTER 1:  INTRODUCTION

1.1  THE INTERNET AGE

The post-1980s was defined in one sense by the advent of the Internet. Since its commercial inception in the early 1990s, the Internet has attracted a worldwide clientele and its predominant use is for commerce, communication, and entertainment. To date, the Internet continues to reach record levels of use.\(^1\) According to Nua, the Internet’s estimated world online population in January 1996 was 30 million users (0.73 per cent of the world’s total population), 102 million in January 1998 (2.49 per cent), 254.29 million in January 2000 (4.19 per cent) and this figure more than doubled in January 2002 to 562.47 million (9.26 per cent) (Nua Surveys 2002:1). In 2004 the estimated online population was 812 million with close to 200 countries connected to the network worldwide (Westby 2003).\(^2\) These figures reveal growth of more than 900 per cent over an eight-year period.

The Internet comprises an amalgam of networks connected through the use of portable and open protocols in a place known as cyberspace. William Gibson (1985:67) first imagined the concept of cyberspace, describing it in the classic science-fiction novel, *Neuromancer*, as:

> A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts ... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding ... \(^3\)

\(^1\) Whilst Internet take-up on a global scale has increased, the rate of use varies across countries According to Schleifer (2004) Internet take-up in the Middle East, for instance, 'is not a level thing. It varies from country to country to the degree you have countries which are fairly relaxed where there is a degree of liberalisation – whether it’s economic liberalisation or political liberalisation, you are getting increasing usage of the Internet ... strong market penetration ... countries like the Gulf and Dubai which is an absolutely booming free market society ... On the other hand; you go to a place like Syria, which still is pretty much of a police state ... and their Internet use ... penetration is restricted ...'.

\(^2\) Variations that report the estimated online population are evident and therefore these figures are simply used to illustrate the growth of this technology (see also Nielsen/NetRatings (2003); Internet World Stats (2004); International Telecommunications Union (2004)).
CHAPTER 1: INTRODUCTION

This description was written prior to the existence of cyberspace and prior to Internet technology being part of popular culture and everyday knowledge. In an interview almost a decade later, Gibson reflected on his account of the concept 'cyberspace':

Cyberspace has a nice buzz to it, it's something that an advertising man might of thought up, and when I got it I knew that it was slick and essentially hollow and that I'd have to fill it up with meaning ... a consensual hallucination ... the point at which media [flow] together and around us. It's the ultimate extension of the exclusion of daily life. With cyberspace as I describe it you can literally wrap yourself in media and not have to see what's really going on around you (cited in Woolley 1992:122).

The terms 'network' and 'cyberspace' have since become ubiquitous in the offline and online environment to an extent that Gibson may not have foreshadowed.4

The origins of the Internet date back to the mid-twentieth century. During the early 1990s, the Advanced Research Projects Agency (ARPA) (a division of the United States Department of Defence) transferred responsibility for the backbone of the Internet to the National Science Foundation (NSFNET), the research network of the Internet. Initially, the NSFNET operated within and between United States academic and research-based institutions, but communication soon spread to Canada and other parts of Europe to form global networks (Frazer 1998:1). The open means of protocols meant that there were no secrets about the operation of software; however, a greater level of trust was required by users of the network due to the computer-mediated nature of communication.

The increase in interest and uptake by academics and researchers led to pressures by the broader corporate community to expand the Internet for commercial use. In 1995, the NSFNET opened up the network to commercial entities where it continued to operate as an unregulated network.5 The Internet appears to have been founded on the principle of

---

3 There has been a rapid growth in the number of networks made available – both for private and commercial applications, such as Local Area Networks (LANs), Wide Area Networks (WANs), Intranet, and Virtual Private Networks (VPNs). These networks are forms of information systems, which also connect to the Internet.

4 See also Castell (1996), The Rise of the Network Society.

5 Frazer (1998:3) notes: 'On April 30, 1995, the NSFNET was officially dissolved, although, returning to its roots, the NSF retained a core research network for research only use called the Very High Speed Backbone Network Service (vBNS), which went on to form the basis for the Internet2 project'.
freedom of information without control, and a degree of trust between users and providers of information was necessary.\textsuperscript{6} If this had not been the case, communication within research networks may not have succeeded during the mid to late-twentieth century.

The aggressive growth of the Internet into a commercial enterprise has changed the way information is collected, distributed, and stored from that of previous networks. Moreover, it has significantly reduced the costs of these services, thereby enabling greater global access (see O’Brien 2000). Opportunities created by greater global access as well as the varied functions performed by the Internet present both advantages and disadvantages to individuals, communities, organisations, businesses, and agencies of government.

The advantages of the Internet include unprecedented access to information, entertainment, and a range of goods and services, a direct means of communication, and an ability to reach the four corners of the globe almost instantaneously (through modes such as e-mail, bulletin boards, FTP servers, peer-to-peer or file sharing applications, and chat rooms). In addition, the Internet provides the means to promote social and economic development, and the potential to enrich individual and community life.

Unlike previous technologies, the Internet is far more direct, more difficult to view, and the elements of space and time are not as apparent. In some cases, it can be used anonymously. The reliance on computing technologies and willingness of users to participate in computer-mediated-communication (CMC) such as the Internet have also provided the means to develop and expand methods of criminal activity in cyberspace. It is the criminal use of the Internet and criminal behaviour of Internet users that is examined in this thesis.

\textbf{1.2 THE DISCIPLINE OF CRIMINOLOGY}

The discipline of criminology has broadly constructed the study of crime into two distinct categories – conventional or ‘street’ crime and white-collar crime. Traditionally,

\begin{footnotesize}\textsuperscript{6} Accordingly, the hacker’s ethic posits that information should be free (see Levy 1984).\end{footnotesize}
street crime has been the central focus (see Bequai 1978; Clinard and Yeager 1980; Sutherland 1983; Braithwaite 1985; Coleman 1985; Schlegel and Weisburd 1992; Fattah 1997; Weisburd et al. 2001; Lynch et al. 2004). Studies have largely concentrated on those crimes considered serious in nature with a perceived physical community impact and public profile. This approach has focused on the criminal behaviour of the poor, relatively powerless section of the community, and individuals, largely juvenile delinquents (see Vold 1979; Sutherland 1983; Braithwaite 1979, 1991; Fattah 1997; Young 1998; White and Haines 2000; Weisburd et al. 2001).

The study of white-collar crime emerged in the late 1930s through the work of Edwin Sutherland. Sutherland's study of 70 United States corporations significantly challenged earlier criminological studies by drawing attention to crimes committed by elites, those of the upper classes, and corporations. Theoretical contributions post-Sutherland have seen the concept of white-collar crime broaden to include crimes committed by organisations, governments, and those in the course of their occupation (see Geis 1967, 1984; Clinard and Yeager 1980; Braithwaite 1984; Grabosky and Sutton 1989; Simon and Eitzen 1993; Punch 1996; Smith 2002a). Prior to these studies, white-collar crime was a neglected area within criminology.

The early studies of white-collar crime play a major role in shaping our understanding of the nature and implications of new forms of crime, namely computer and cyber crime. Not all white-collar crimes are carried out by the wealthy and powerful, as theorised by Sutherland (1983), but also from the middle (see Weisburd et al. 1991) and even the lower classes. The emergence of computer and cyber crime is an important area to study given that both forms of crime – conventional and white-collar – can be carried out on one platform. This research may therefore uncover possible challenges for the future study of crime and criminal behaviour through the two pre-existing categories of crime – conventional and white-collar crime.

\[7\] File Transfer Protocol (FTP) is a protocol that allows files to be exchanged over the Internet.
1.3 THESIS AIMS AND OBJECTIVES

This thesis aims to contribute to criminology by examining criminal behaviour on the Internet. The rapid development of computer crime and most recently the rise and proliferation of cyber crime has led to various studies over the past decade (see for example, Grabosky and Smith 1998; Denning and Baugh 1999; Broadhurst 2001; Grabosky et al. 2001; Smith et al. 2004). Given the magnitude of cyber crime, however, little research has been carried out that applies criminological theories to criminal behaviour on the Internet.

The central objective is to explore whether existing theories of crime and criminal behaviour can be used to explain different forms of cyber crime and, if so, to what extent. In doing so, the thesis identifies indicators that may assist theoretical understandings of different forms of cyber crime and ways of controlling it. In the light of this, a second broad objective is to develop the issue of trust as a significant concept to understand criminal behaviour on the Internet, as few theories have concentrated on this issue. A third broad objective is to explore approaches to networks of trust as a core regulatory dimension to control criminal behaviour on the Internet. The umbrella hypothesis is that existing theories of criminal behaviour do explain criminal behaviour committed on the Internet.

1.4 THESIS APPROACH AND METHODOLOGY

The approach entails an overview of mainstream criminological theories and a test of their applicability to crime involving cyberspace and the Internet. The purpose of theoretical exegesis is to assess whether theories developed in the pre-Internet age have any application to the post 1980s phenomenon of crime on the Internet. A critical approach is applied to existing criminological theory through analyses of data and case studies to interpret their validity and applicability.

---

8 This thesis applies Crow’s (2000:117) concept of theory, which he describes as ‘... an attempt to make sense of interconnected relationships so that the empirical world can be understood in a systematic manner, and hypotheses are specific working statements about particular relationships contained within such theories.’
CHAPTER 1:  

INTRODUCTION

Six contrasting theories are examined: differential association (Sutherland 1939), anomie (Merton 1938), neutralisation (Sykes and Matza 1957), social control (Gottfredson and Hirschi 1990), routine activity (Cohen and Felson 1979), and trust violation (Shapiro 1990). The mainstream criminological theories chosen are those that appear to have some application to white-collar crime. The next step is to evaluate how each of these theories can explain a number of case studies of cybercrime. If they do, they might be regarded as robust or at least fertile. Indeed, the thesis comes to a view as to which of the mainstream theories can be seen to have the best fit to cyber crime. The theories that pass the test of survival and critical analysis are Cohen and Felson’s (1979) routine activity theory and Shapiro’s (1990) theory of trust violation.

The thesis examines a diverse range of offences from hacking, to piracy, Internet sex crimes against children and youth, child pornography, fraud (auction fraud, online securities fraud, phishing, identity theft, insider trading), stalking, espionage, Denial of Service (DDoS) attacks, and misuse of personal information. Chapters Five, Six, and Seven examine a total of 41 cases of cyber crime with some claims to typicality. Specific cases are chosen that were the subject of law reports and/or learned commentary.

The challenge for the thesis then becomes one of critically assessing whether there is a way of synthesising theories. Arrigo (2001:84) suggests that ‘synthesising criminological theory is a useful, practical endeavour. Ultimately … it allows for greater explanatory and predictive power when addressing such matters as the cause, nature, and response to crime’ (see also Pearson and Weiner 1985; Thornberry 1989). Conversely, Hirschi (1979, 1989) argues that theoretical integration is a bad thing and advocates competing theories and a ‘fact-based approach’ (Liska et al. 1989:21).

In Hirschi’s (1989:44) view, ‘... we should take individual theories as far as we can before we abandon them or try to save what is left of them by adding them to some integrated stew’. Despite these observations, Hirschi along with Gottfredson (1990) developed a general theory of crime, which combined elements of classical theory with

---

9 Thornberry (1989:52) defined theoretical integration as ‘... the act of combining two or more sets of logically interrelated propositions into one larger set of interrelated propositions, in order to provide a more comprehensive explanation of a particular phenomenon’. 

Page 6
the concept of self-control. For a new problem like cyber crime that may combine different elements of older crimes, the case for integration may be stronger than Hirschi allows. The test of whether the integration path was a good choice is ultimately how fertile, revealing and useful in a policy analytic sense the choice turns out to be.

The Internet was used as the primary source to research cases of white-collar, computer, and cyber crime. The process of research involved scanning Internet databases such as online law links and scholarly journals, which contained information relevant to legal cases on cyber crime. Australian and overseas law enforcement and government websites also provided relevant information and commentary on specific legal cases on cyber crime. The cases used predominantly emanate from the United States. This is due to the greater availability of information and statistical data on cyber crime. Only recently has there been evidence of a number of other government websites detailing official statistical information and cases of cyber crime from Australia, the United Kingdom, Hong Kong, and Japan, and these are illustrated in this thesis. Additional sources of information relating to cyber crime cases were found in books and published research papers, and through the print media.

The predominant method of inquiry involved secondary analysis. According to Jupp et al. (2000:57-8), ‘secondary analysis is a form of investigation which is based upon existing sources of data … which has been collected by someone other than the researcher …’. The Internet was also used as the primary source of gathering existing statistical information and sources of data on white-collar, computer, and cyber crime. This information was largely found through government and corporation websites that publish statistical data specific to white-collar, computer, and cyber crime. According to Jupp et al. (2000:58), ‘… the forms of data that have a major impact on criminological research are official statistics on crime’.\(^\text{10}\) The reports cited in this research were also collected by agencies within both public and private sectors from Australia and overseas.

\(^{10}\) There are obvious limitations of official statistics (Jupp et al. 2000:64). In the case of cyber crime, few governments around the globe collect and record data on cyber crime. One of the difficulties with this is that some countries do not recognise particular forms of cyber crime that other countries criminalise.
Traditionally, official statistics on crime have focused on conventional forms of crime—robbery, homicide, assault, and theft of property. As Jupp et al. (2000:58) argue, 'the police rely heavily on victims and on the general public to notify 'crime-like' acts to them. If they do not it is unlikely that the police will know about these acts let alone record them in official statistics'. This presents obvious challenges in analysing statistics of crime on the Internet. As this thesis shows, many forms of cyber crime are carried out unbeknownst to the victim, for example, fraud, hacking, and piracy. Furthermore, it shows that a reluctance to report cyber crime for fear of adverse publicity contributes to the difficulties in collecting and recording cyber crime through victim surveys and official statistics (Richardson 2003).

This thesis did not set out predominantly to find new statistical data. Rather, what the thesis examines is whether theories fit such qualitative case data as exist, and seeks to assess whether they throw up any challenges. Punch (1998:190) asserts that:

Documents, both historical and contemporary, are a rich source of data for social research. A distinguishing feature of our society may well be the vast array of "documentary evidence" which is routinely compiled and retained, yet much of this is neglected by researchers, perhaps because the collection of other sorts of social data has become more fashionable.

A core section of this thesis (Chapters Three, Five and Six) analyses existing theories of crime and criminal behaviour. At the time of the research, few studies of cyber crime had been carried out in Australia, with the exception of work by Grabosky and Smith (1998), Grabosky et al. (2001), and Smith et al. (2004). These works have concentrated on emerging forms of crime and examined the enforcement, legal, and regulatory challenges that arose from the commission of these crimes in the digital age.

The transnational nature and borderless geographical boundaries of the Internet have made it difficult to conduct empirical research on a global scale. For example, surveys and interviews that would be methodologically sound and represent a broad section of the Internet population are beyond the scope of this research. Moreover, given the thesis' focus on crime, the challenges posed in exploring crime and criminal behaviour on the Internet through these approaches raises ethical dilemmas, and anonymity on the Internet may also challenge the legitimacy and validity of responses.
1.5 THESIS STRUCTURE

This thesis is divided into four primary sections: the history and nature of white-collar crime; the emergence and development of computer and cyber crime; theories of criminal behaviour; and the role of trust and regulation. Chapter Two confronts the study of white-collar crime. First, it provides a historical overview of the concept 'white-collar crime'. Second, it questions the way the study of white-collar crime has proceeded – from its initial focus on the type of offender to a shift to the type of offence. Third, it examines significant empirical studies that have shaped the development of white-collar crime over the past six decades, namely corporate crime and occupational crime. Lastly, this chapter explores the challenges associated with broadly constructing the boundaries of the study of crime into two distinct categories.

Chapter Three examines seven theories of criminal behaviour and their applicability to different forms of white-collar crime. The chapter introduces the traditional contributions to the study of crime and criminal behaviour through the classical and positivist schools, to a more recent contribution – the Chicago school, and then focuses on a range of contemporary theories. The six theories chosen represent a broad selection of dominant criminological theories. They are categorised into learning (Sykes and Matza 1957; Sutherland 1983; Wilson and Herrnstein 1985), opportunity (Cohen and Felson 1979; Gottfredson and Hirschi 1990), and strain (Merton 1938). Each theory is examined individually and the most critical contemporary empirical studies that have been applied to assess its applicability are introduced.

Chapter Four explores computer and cyber crime. Part One of this chapter defines computer and cyber crime and then provides a critical examination of the historical and scholarly analyses of its development. It achieves this by examining four focal periods: the emergence of computer crime; the criminalisation of computer crime; the changing perception of hackers; and the emergence of cyber crime. The next section explores the criminalisation of computer crime through four waves: the development of computer crime from its early detection in the 1970s; the emergence of scholarly contributions to

---

11 The term 'period' refers to set periods of time in which the study of computer and cyber crime has been explored.
CHAPTER 1:

INTRODUCTION

computer crime in the 1980s; the rise of cyber crime in the early 1990s; and the enactment of various computer laws.

Part Two of Chapter Four explores the development of new forms of cyber crime. It also examines whether criminogenic attributes, such as anonymity, multiplicity, and target exploration are more common to the Internet in understanding the proliferation of cyber crime. The analysis strongly suggests that anonymity, multiplicity, and target exploration are important contributors to the proliferation of cyber crime, and in particular have shown relevance to trust violation.

Chapter Five questions whether the theories presented and examined in Chapter Three are adequate to explain crimes committed on the Internet (cyber crime). This chapter continues the examination process by applying five theories to a broad range of cyber crimes. The crimes examined in this chapter are categorised into three groups and represent a broad cross-section of crimes carried out on the Internet: first, those crimes to which a dollar value is attached, including fraud, software piracy, sale of child pornography, and espionage; second, crimes which impact directly on a personal level against an individual and groups of individuals, such as Internet sex crimes against children, and cyber stalking; and third, crimes in which the predominant targets are businesses and companies such as hacking, and Denial of Service (DoS) attacks.

Chapter Six elaborates on Shapiro’s theory by examining the relationship between violation of trust and criminal behaviour on the Internet through lying, self-dealing, corruption, and role conflict. This theory of trust violation is particularly important to understanding criminal behaviour on the Internet because of the lack of focus on exploring these elements from a cyber perspective.

Chapter Seven integrates the work of the previous five chapters by evaluating criminal behaviour and trust on the Internet. It also explores what regulatory approaches can be applied to control crime on the Internet. First, this chapter explores the concept of trust and analyses whether differences in the way trust is viewed in the terrestrial and virtual world impact upon violation of trust on the Internet. Second, this chapter analyses whether empirical research on trust and the Internet informs our understanding of the
link between trust and criminal behaviour. Third, it briefly outlines the various discourses surrounding regulation on the Internet: self-regulation, law enforcement, and global co-operation. Lastly, this chapter applies two examples of cyber crime, auction fraud and Internet securities fraud, to identify which regulatory response might effectively control it.

The final chapter outlines the critical issues central to regulating cyberspace. First, it discusses whether theories of criminal behaviour can explain different forms of crime committed on the Internet, and, if so, to what extent, and examines the implications for future research. Second, it discusses the critical issues and future challenges for regulating cyberspace.

As shown in this thesis, the Internet's commercial emergence in the late twentieth century has opened up opportunities for different forms of crime to be carried out on a single global platform. The fact that old forms of crime can be committed on a new medium raises the question of whether distinctions between street crime and white-collar crime are today as clear as they once were, particularly given the birth and proliferation of cyber crime. Consequently, the question remains: what are the implications for the discipline of criminology?

Advantages in technology coupled with the capabilities of computer-mediated communication and the increase in Internet take-up appear to account for the considerable growth and subsequent proliferation of cyber crime (see Adamski 1998). Traditional offences that were once confined to the terrestrial world have emigrated to the Internet, and criminals have developed new methods as well as new crimes due to the technological application and sophistication of the Internet. Given the record levels of online use, it is clear that the Internet and its misuse are a phenomenon worthy of further criminological attention. Testing existing theories of criminal behaviour in the domain of cyberspace is a useful agenda. Now that the Internet has been in commercial use for over a decade, the study of crime and criminal behaviour is timely and important.

12 This is with the exception of Wilson and Herrnstein's (1985) constitutional learning theory.
in understanding future challenges and regulatory responses that new technologies bring.
CHAPTER 2: THE CONCEPT AND STUDY OF WHITE-COLLAR CRIME – A REVIEW OF THE LITERATURE

2.1 INTRODUCTION

The study of white-collar crime emerged in the early part of the twentieth century yet attracted considerable criminological and legal attention only in the latter half of the twentieth century (Bloch and Geis 1962; Erman and Lundman 1982; Braithwaite 1985; Coleman 1987; Schlegel & Weisburd 1992; Weisburd et al. 2001). Edwin H. Sutherland introduced the concept of white-collar crime and opened up the field of study within criminology in the late 1930s. His study of the violations and criminal behaviour of 70 United States corporations paved the way for significant research into a broad range of white-collar crimes that have developed over the past seven decades (Clinard 1946; Lane 1953; Geis 1967; Clinard & Yeager 1980; Braithwaite 1984; Shapiro 1984; Grabosky and Sutton 1989; Rosoff et al. 1998). The concept and study of white-collar crime has been marked by a number of distinct changes that separate more recent work from early scholarship (Geis 1984, 1992; Coleman 1992).

This chapter reviews historical and contemporary literature that has shaped the study of the development of white-collar crime. The objective of this chapter is to demonstrate the different ways in which the study of white-collar crime has been approached and applied over the past six decades and develop a broader insight into the changing dynamics of this growing body of criminological scholarship. Section 2.2 explores the early influences on the study of white-collar crime in the early twentieth century. Section 2.3 focuses on the pre-eminent scholar of white-collar crime, Edwin Sutherland, and his seminal study of corporations and public companies in the United States of America. Sections 2.4 to 2.5 examine the concept and definition of white-collar crime drawing on a broad range of contributions which illuminate the contributions and debates that have shaped the study of white-collar crime. Lastly, section 2.6 outlines empirical studies of new forms of white-collar crime.
2.2 EARLY INFLUENCES ON THE STUDY OF WHITE-COLLAR CRIME

The existence of crimes committed by those considered respectable people and people in positions of power was acknowledged in the early part of the twentieth century (Ross 1907; Morris 1935). E.A Ross, a prominent sociologist of the time used the term ‘criminaloid’ in his book, *Sin and Society* (Ross 1907), to refer to businessmen who committed acts to maximise profit and gain while appearing respectable behind the public image of decency. Ross (1907:44-45) made the point:

> The immunity enjoyed by the perpetrator of new sins has brought into being a class for which we may coin the term “criminaloid”. By this we designate those who prosper by flagitious practices which have not yet come under the effective ban of public opinion ... The criminaloid prefers to prey on the anonymous public (in Geis and Meier 1977:30-31).\(^{13}\)

Examples of the ‘criminaloid’ referred to by Ross were corporate executives, corrupt judges, and politicians. For these individuals, it was the lack of moral sensibility that Ross argued was the key to becoming a ‘criminaloid’. Similarly, during the mid 1930s, criminologist Albert Morris recognised ‘criminals of the upper world’. Morris (1935:153) observed that such criminals were those ‘... whose social position, intelligence and criminal technique permit them to move among their fellow citizens virtually immune to recognition and prosecution as criminals’— a view later shared by Sutherland (1939, 1947) (cited in Sutherland 1983:xxxi).

Early twentieth century writers, such as Steffens and Tarbell (1903) also revealed examples of political and corporate misconduct and labour racketeering (Weisburd et al. 2001). Commonly acknowledged as the ‘muckrakers’ (Braithwaite 1985; Friedrichs 1996), Steffens and Tarbell (1903) were writers who exposed illegal activities as part of a journalistic endeavour. Friedrichs (1996:26) notes that ‘journalists historically have been a thorn in the side of the establishment because of their periodic exposures of wrongdoing by the powerful and privileged’. A broad range of illegal and unethical practices incorporating breaches of occupational and corporate crime and misconduct

\(^{13}\) This was the language of positivism, i.e. the idea of a ‘type’ of person or class – ‘criminaloid’ and indeed Lombroso used just such a term in his work (see Lombroso 1872).
and political deviance was exposed during this time, particularly during the 1930s (Friedrichs 1996).

The Dutch criminologist, Willem A. Bonger, concentrated his research on the inequality and distribution of crime among the different classes in society. As Braithwaite (1985:2) remarks, Bonger was the first to develop a theory of crime in *Criminality and Economic Conditions* ([1916] 1967), which incorporated both ‘crime in streets’ and ‘crime in the suites’. Bonger acknowledged that crimes occurred in the upper classes, although crimes of the poor and disadvantaged were more likely to be punished and the perpetrators prosecuted – a view later shared by some criminologists. According to Bonger ([1916] 1967), it is not poverty alone that causes crime because that does not account for crimes committed by those in ‘the suites’. The research by Bonger moved beyond positivism in its present sense.\(^{14}\) Furthermore, his focus on ‘class’ as a contributor to criminal behaviour continued later through the work of Edwin Sutherland.

In the mid-twentieth century, Henry and Short (1954) and Durkheim ([1893] 1964) explored the correlation between economic conditions of society and rates of crime. Cohen and Felson (1979) later challenged the link between economic conditions and crime rates. The poor were seen as committing crimes not only because of their lack of wealth, but also because of the lack of opportunities afforded them by capitalism. Crimes committed by people in ‘the suites’ appeared to be motivated by greed and made possible by opportunities inherent in the capitalist structure.

### 2.3 THE PRE-EMINENT SCHOLAR OF WHITE-COLLAR CRIME – EDWIN SUTHERLAND

Edwin H. Sutherland (1883-1950) coined the term ‘white-collar crime’ during his Presidential address to the American Sociological Society Meeting in 1939. Sutherland proposed a number of definitions of white-collar crime during the course of his work. His most cited definition affirmed that white-collar crime ‘... may be defined approximately as a crime committed by a person of respectability and high social status

\(^{14}\) Bonger was also recognised for his publications, *An Introduction to Criminology* (1936) and *Race and Crime* (1943).
in the course of his occupation ...’ (1983:7).  

Sutherland’s definition of white-collar crime identified two central characteristics:

- the individual’s social status (respectability, perceived decency).
- the conduct of the individual (who, even when acting within a corporate setting, is nevertheless a distinctly identifiable moral agent):
  - exploiting that social status;
  - in the course of occupational activities.

It was the wilful act of taking advantage and abusing a position of trust and power (including financial power) that Sutherland believed characterised white-collar crimes. Despite undertaking research primarily on corporations, Sutherland continued to believe that it was the individuals working within the corporation that carried out these violations (Meier 2001).

Historically, much criminological research and theory concentrated on conventional crimes, crimes committed by the powerless, and crimes carried out by individuals (usually male juvenile delinquents), largely drawn from the lower classes (Taylor et al. 1973; Fattah 1997). To Sutherland, the seriousness of white-collar crimes committed by the wealthy, powerful, and those in a position of trust were equivalent to conventional or street-style crimes committed by those in the lower classes and were in violation of the law.

During the 1930s and 1940s, Sutherland published numerous research papers on crimes committed by those in the upper class, those (considered) respectable in the business sector, and corporations. Sutherland’s call to pay attention to corporate executives committing ‘white-collar crime’ attracted criticism from the broader business community during the mid-twentieth century. Until that time, little had been published

---

15 It is interesting to note that in quoting Sutherland’s definition of white-collar crime, a number of scholarly contributions exclude the use of the word ‘approximately’ (Shapiro 1990; Fattah 1997; Johnson and Yeo 1999; Johnstone 1999; Simpson 2002). This exclusion may encourage the reader to interpret that Sutherland was confident in narrowing a definition of white-collar crime.
identifying white-collar crimes and white-collar criminals. As Coleman (1985:3) notes, ‘the idea that the fabled ‘captains of industry’ could even be considered criminals had a very un-American sound to it ...’. Sutherland’s research and theory of white-collar crime represented a fundamental break in criminological theory, challenging pre-existing studies by demonstrating that crimes are also committed by the wealthy (often seen as taking advantage of their position), the powerful and by corporations.

2.3.1 Sutherland's Seminal Study of Corporations

To validate his theory of white-collar crime, Sutherland set about examining and documenting the extensive range of illegal corporate activity and criminal behaviour that occurred within 70 of the largest American corporations and public companies – manufacturing, mining, and mercantile (Sutherland 1983:13). These corporations were responsible for a wide range of offences he labelled ‘white-collar’. The most frequent forms of white-collar criminality included restraint of trade, misrepresentation in advertising, unfair labour practices, financial manipulations, tax fraud, embezzlement, misrepresentation in corporations’ financial statements, violations of regulations and bribery.

Sutherland appeared not to consider those who committed more offences worse offenders because he was more concerned about the principle of law violation. He argued that:

... the criminality of the corporations, like that of professional thieves, is persistent: a large proportion of the offenders are recidivists. Among the 70 largest industrial and commercial corporations in the United States, 97.1 percent were found to be recidivists in the sense of having two or more adverse decisions (Sutherland 1983:227).

Based on this seminal study, Sutherland considered white-collar crime also a form of organised crime because the preponderance of illegal behaviour involved informal and formal practices of organisation (see Hobbs 2000). Sutherland (1983:129-30) noted that ‘the informal organisation for crimes by corporations consists in consensus among

16 The Chicago School of Sociology is one example of a centre of scholarly research focusing on crime and juvenile delinquency.
17 Part of the material required for this analysis was available through public resources, including court documents.
businessmen’. Furthermore, Sutherland (1983:229-230) maintained that corporations also used formal organisational structures and systems of crime for the purpose of controlling legislation, for ‘... selection of administrators, and restriction of appropriations for the enforcement of laws ...’.

In a number of cases that Sutherland identified as white-collar crime, the offences were committed to benefit the corporation directly. The organised nature of some forms of crime committed within corporations may be most aptly described as corporate crime (an issue discussed in sub-section 2.6.1).\textsuperscript{18} Sutherland’s study revealed examples of corporate and occupational crime; however, he failed to distinguish adequately these concepts from each other in his definition of white-collar crime.

At the time of publication of Sutherland’s research, his study held little influence in the corporate sector. Rawlinson (2002:294) argues that ‘this is hardly surprising given its unrestrained criticism of the bedrock upon which economic development has occurred in western capitalist states’. Towards the end of the twentieth century, corporate collapses such as Enron and WorldCom in the United States of America, and HIH Insurance in Australia\textsuperscript{19} have attracted further studies and research similar to that of Sutherland some seven decades ago (see for example Rosoff et al. 1998, 2003; Westfield 2003; Bakan 2004; Clarke et al. 2003).

Sutherland’s studies led to the centre-piece of his analysis in the publication of his book, \textit{White-Collar Crime} ([1949]1983), which was the major contribution on the topic before his death in 1950. It was not until after his death that an unabridged version of Sutherland’s book was published, as the original edition was altered to protect the corporations named in his study for fear of legal action.

\textsuperscript{18} It is interesting to note that Coleman’s (1985) typology of white-collar crime also applies to this analysis of organised crime.

\textsuperscript{19} The HIH Royal Commission was born out of the collapse of the insurance company HIH. One purpose of the HIH Royal Commission was among others to identify the reasons and circumstances that brought about the collapse (see Owen 2001).
2.4 DEFINING ‘WHITE-COLLAR CRIME’—PAST AND PRESENT CONTRIBUTIONS AND CONTESTATIONS

This concept [of white-collar crime] is not intended to be definitive, but merely to call attention to crimes which are not ordinarily included within the scope of criminology (Sutherland 1983:7).

Sutherland’s definition of white-collar crime is one of the most recognised and cited in criminological, sociological, and legal literature, although it has endured frequent challenges as it covers a diverse range of criminal behaviours (Tappan 1960; Edelhertz 1970; Clinard and Yeager 1980; Shapiro 1980; Braithwaite 1985; Vaughan 1990; Croall 1992; Geis 1992; Schlegel and Weisburd 1992; Friedrichs 1996; Nelken 1997; Slapper and Tombs 1999; Weisburd et al. 2001; Griffin 2002). Consequently, a large number of divergent interpretations of the definition of white-collar crime exist.

Sutherland’s contribution to the study of white-collar crime is well documented (Mannheim 1965; Geis 1984; Braithwaite 1985). It was first and foremost Gilbert Geis who believed that the central principle worthy of support was Sutherland’s acknowledgement and study of the abuse of power perpetrated by individuals in high places, notably in otherwise legitimate business environments. Geis (1992:35) made the point:

... what stands out is a sense that Sutherland was most concerned with the illegal abuse of power by upper-echelon businessmen in the service of their corporations, by high-ranking politicians against their codes of conduct and their constituents, and by professional persons against the government and against their clients and patients.

Geis also noted that some of these individuals were aware of the violations and illegal activity but chose to proceed nonetheless.

Mannheim (1965:470) also acknowledged the merit of Sutherland’s research and contributions to criminology by asserting: ‘there is no Nobel Prize as yet for criminologists, and probably there never will be one, but if it had been available, Sutherland would have been one of the most deserving candidates for his work on WCC’. Mannheim believed that white-collar crime was a significant field of study within criminology that needed to continue. However, Mannheim also noted the limitations posed by Sutherland’s definition and the lack of progress of the study of white-collar crime as illustrated within the discipline of criminology.
Sutherland’s definition of white-collar crime has drawn support from Braithwaite (1985:117), who argues that we should continue to employ the overarching definition proposed by Sutherland. In relation to Sutherland’s focus on the characteristics of the individual i.e. of ‘high social status’ and power, Braithwaite (1979:187) points out that the illegitimate opportunities afforded by being in a position of power open up possibilities that may be unavailable to lower classes, an element fundamental to understanding the nature of white-collar crime. Braithwaite (1979:187) draws on examples such as ‘... the power to embezzle, to defraud, to misappropriate, to abuse safety laws, to engage in price-fixing ...’ to validate his point. Commission of such offences requires decision-making by individuals at least at management level. Traditionally, lower level employees may not have had access or opportunity to embezzle funds or make decisions on occupational health and safety issues (Braithwaite 1979).

Sutherland’s reluctance to define white-collar crime is evident in his early publications, which cited a number of broad definitions. Meier (2001:1) argued that ‘Sutherland’s lack of a definitive explanation, with the use of the term ‘approximately’, meant that if there was a structural definition, the field of criminology may be in disarray’. Furthermore, Sutherland showed that he was unsure of the validity of his most commonly identified definition by placing it in a footnote rather than as part of the main body of his research. In Meier’s (2001:10) view:

... Sutherland’s path-breaking work was possible in part because of his not narrowing his inquiry to fit some particular definition of white-collar crime. Had Sutherland addressed the definitional issue in 1949 and as some scholars have today, the field might look even more parochial and confusing than it presently does (in Pontell and Shichor 2001:10).

As well as using a number of definitions during the course of his career, Sutherland demonstrated his ambiguity by adding the word ‘approximately’ to his final definition. However, in Nelken’s (1997:895) view, ‘... ambiguity about the nature of white-collar crime and the best way of responding to it, forms an essential key to the topic and can be used to provide insights into this type of crime as well as the ‘ordinary’ crime with which it is contrasted’. Ambiguity about Sutherland’s definition of white-collar crime spawned reactions from the broader criminological and legal community.
Challenges to the concept over the past six decades have strengthened the study of white-collar crime as a significant field within the discipline of criminology. The following section draws upon a number of these contributions that highlight the debate surrounding Sutherland’s definition.

2.4.1 Redefining the Concept of White-Collar Crime

Sutherland’s definition of white-collar crime has drawn criticism from a number of different areas within criminology, sociology, and from legal professionals. The definition of white-collar crime proposed by Sutherland may be challenged in three distinct ways:

- *Crimes occurred in the course of one’s occupation* – the offender had to commit the offence within the (physical) working environment. This does not take into account some forms of fraud and forgery, which can be committed outside this area.

- *The labelling of the offender as ‘high social status’* – this usually implies the offender occupied a management or executive position, excluding other individuals from also committing forms of white-collar crime (such as those from the lower and middle class levels).

- *Not adequately distinguishing between crimes committed on an individual level and those crimes/violations committed by corporations* – individual crimes include embezzlement whilst crimes committed by corporations can include price fixing.

Tappan (1947) made an early challenge to Sutherland’s definition of white-collar crime, by proposing a more legally oriented definition. Tappan (1947:101), a lawyer-sociologist, argued that ‘... the ‘white-collar criminal’, the violator of conduct norms, and the antisocial personality are not criminal in any sense meaningful to the social scientist unless he has violated a criminal statute’. Sutherland believed that administrative as well as criminal violations should be included under the umbrella of white-collar crime. According to Tappan, for a crime to be considered white-collar, criminal law had to be breached. If this was not the case, an individual should not be labelled a ‘white-collar offender’.
Mannheim (1965:472) also noted that, despite the problems associated with his definition (the main challenge was that his concept extended the boundaries beyond crimes punishable by criminal law), Sutherland’s objective, to call attention to crimes that had previously been neglected within criminology, was achieved. Mannheim (1965:471-2) maintained ‘... that some of his many pronouncements on the subject seem to justify such charges; basically ... he tried to keep WCC strictly within the scope of criminal law’. Further to this debate, Tappan (1960:10) argued:

Our definitions of crime cannot be rooted in epithets, in minority value judgments or prejudice, or in loose abstractions. Within a system of justice under law, crime must be defined quite precisely and in accordance with the explicit formulations of the legislature. Such crime will not include all behaviour that is anti-social ... nor even all conduct that should be made criminal.

Conversely, Sutherland (1983) asserted that many white-collar crimes go undetected by enforcement agencies and, if detected, individuals committing white-collar crimes may not be charged. Sutherland’s position also reflected the nature of the current system, where many of those in positions of power or wealth were more likely to escape punishment, further reinforcing his opposition to Tappan’s definition of white-collar crime. In other words, Tappan argued that you need precision to ground criminalisation of conduct. Sutherland’s view is that socio-political conditions mitigate against criminalisation, however precisely prohibitions may be formulated. The distinction between Sutherland’s definition and Tappan’s can be traced to two central issues: first, to be a crime it is defined through statute as opposed to civil penalties; and second, to be a crime there has to be a conviction.

In response to Tappan’s position, Goldsmith et al. (2003:146) argued that ‘... people such as British publishing mogul Robert Maxwell, who misappropriated large amounts of employee superannuation funds to prop up his failing companies, cannot be described as a ‘white-collar criminal’ because Maxwell’s behaviour only became public after he fell, jumped, or was pushed to his death off his luxury yacht’ (cited in Bower 1996:146). The example of the Australian entrepreneur, Christopher Skase, who fled Australia to Majorca after the collapse of his multibillion-dollar company, Qintex Group, may also apply here. The Director of Public Prosecutions and the Australian
Securities and Investment Commission (ASIC)\textsuperscript{20} recommended charges, however, there were no prosecutions due to Skase’s ill health and subsequent death in 2002 (see Clarke et al. 2003).

Rising to challenge Sutherland’s definition from a law enforcement position was Herbert Edelhertz. Edelhertz (1970:3) defined white-collar crime as ‘... an illegal act or series of illegal acts committed by non physical means and by concealment or guile, to obtain money or property, to avoid the payment or loss of money or property, or to obtain business or personal advantage’. The definition provided by Edelhertz was more concerned with the act itself and the way in which it was carried out rather than the ‘social-status’ of the offender (cited in Weisburd et al. 2001:8). Furthermore, the definition omitted the role occupation plays in the commission of white-collar crimes.

To incorporate the broad nature of white-collar crime, Edelhertz (1970:19-20) devised additional subcategories within his definition. These include:

1) Crimes by persons operating on an individual, \textit{ad hoc} basis, for personal gain in a non business context (e.g. credit card fraud, Medicare fraud);

2) Crimes in the course of their occupations by those operating inside businesses, government, or other establishments, or in a professional capacity, in violation of their duty of loyalty and fidelity to employers or clients (e.g. computer crime, share-market manipulation);

3) Crimes incidental to and in furtherance of business operations, but not the central purpose of such business operations (e.g. misrepresentation);

4) White-collar crime as a business or as the central activity of the business (e.g. fraud, pyramid schemes).

Edelhertz’s position on defining white-collar crime was somewhat influenced by his role as chief of the fraud section in the Criminal Division of the United States Federal Department of Justice (Geis 1992). In this sense, his definition is suitable for the environment in which he worked, although it is not a definition suitable for all forms of white-collar crime. For example, it does not include crimes that create or result in

\textsuperscript{20} The Australian Securities and Investment Commission (ASIC) was formerly called the Australian Securities Commission.
physical harm or violence (see Braithwaite 1985; Coleman 1985). Furthermore, not all white-collar crime is motivated by financial reward (Duffield & Grabosky 2001; Krambia-Kapardis 2001). Fraud is one example where additional motivating factors, such as ego and power may contribute to the crime. According to Duffield and Grabosky (2001:2):

This can relate to power over people as well as power over situations. In terms of the former, the sensation of power over another individual or individuals seems to be a strong motivating force for some fraud offenders to the point that it becomes an end in itself.

Since Sutherland coined the term ‘white-collar crime’ in the late 1930s, it has been reshaped and redefined due to the wider focus needed to embrace its changing categories and nature. In attempting to address contemporary developments of the concept of white-collar crime, two alternatives to the definition are proposed: first, the adoption of Sutherland’s overarching definition proposed by Braithwaite (1985), or second, the creation of a wider definition to embrace more diverse forms of white-collar crime (Coleman 1985). The next section continues this review and explores how white-collar crime is conceptualised through offence or offender-based definitions.

2.4.2 Offender and Offence-Based Definitions of White-Collar Crime

The parameters of defining categories of crime have often been guided by the focus on offence (Shapiro 1990) or offender-based (Sutherland 1983) definitions of crime (see Griffin 2002). A number of past and contemporary examples of attempts to redefine white-collar crime through these common classifications of crime are evident. It was, first and foremost, Edwin Sutherland who defined ‘white-collar crime’ through the status of the offender, which continued the doctrine of criminological positivism. Sutherland’s focus on ‘class’, namely those in a position of wealth and status, was a direct break with established and contemporary criminological theory, which linked crime and poverty. At the time of Sutherland’s research, the collection of crime data in the United States in the early twentieth century focused almost exclusively on conventional crime thus eliminating white-collar offences and the types of individuals who commit white-collar crimes. This posed challenges in identifying criminal characteristics of a white-collar offender.
Sutherland's profile of a white-collar offender was essentially an individual in a position of power or with a high level of social status. This implied that white-collar offenders were drawn from the upper classes of society. Despite the opportunities and access that may have been afforded to individuals in a position of status, Braithwaite (1985) makes the point that 'the requirement that a crime cannot be a white-collar crime unless perpetrated by a person of 'high social status' is an unfortunate mixing of definition and explanation, especially when Sutherland used the widespread nature of white-collar crime to refute class-based theories of criminality'. One of the objectives of Sutherland was to refute the view that poverty was the established causal factor in crimes essentially committed by people who were in a position of wealth and status.

Weisburd et al. (2001) acknowledged that white-collar offenders today are also drawn from the middle classes rather than specifically the upper classes as claimed by Sutherland (see Croall 1992; Shapiro 1984). Weisburd et al. (2001:9) argue that 'most of those who are prosecuted for crimes like bribery, tax fraud, or bank fraud are rather average in their social backgrounds and positions'. Weisburd et al. (2001:9) illustrate this point with the example of '... the “fraudsters” who manipulate stocks [who] are very far from elite status'. The point to be drawn from this analysis is as Weisburd et al. (2001:10) pose, '... whether it is useful to begin with an understanding of white-collar crime that allows us to speak not only of the rich and powerful white-collar criminals, but also of those offenders much closer to the middle of our society ...', thus representing a shift in the traditionally accepted characteristics of a white-collar offender.

Some critics argue that Sutherland's preoccupation with the status and occupation of the offender has narrowed the nature of his definition. According to Ellis and Walsh (2000:517), Sutherland's definition was wrong in three important ways: first, most white-collar criminals are not of 'high social status'; second, many are not otherwise respectable people, and third, it fails to distinguish between crimes committed by individuals acting for personal gain, and crimes committed on behalf of the employer with the employer's blessing and support. While Sutherland's description of the white-collar criminal may have been valid during the 1930s, Ellis and Walsh's (2000) argument is valid because white-collar criminals can no longer be distinguished by status.
Sutherland’s focus on the status of the offender may fit the paradigm of criminality within the business sector that was evident in the early to mid-twentieth century. Weisburd et al. (2001:11) argued that, 'it was natural for Sutherland to focus on businessmen in lofty positions when examining the problem of white-collar crime because relatively few Americans beyond these elite men had any opportunity for committing such illegalities'. However, this promotes the concept that those who commit white-collar offences do so merely because the opportunity for concealment exists over and above other factors such as greed.

Despite the focus of Sutherland’s research on corporations rather than individual offenders, Vold et al. (2002:161) noted that ‘... Sutherland argued that the key factor determining whether people violate the law is the meaning they give to their social conditions they experience, rather than the social conditions themselves’. In other words, it is learned behaviour, not innate. This was therefore an offender-based definition of criminality, which could account for all forms of crime, typically committed during the course of one’s occupation. In more recent times, criminologists have challenged the validity of this argument, as contemporary debates are focused around whether the term should refer to an offence committed by those of high social status, whether it should distinguish between crimes committed by corporations or individuals, or whether it should refer to economic or financial crimes (see Friedrichs 1996).

In relation to crime in the professions, Hayne (2002:27) observes that this category of crime ‘... seeks to classify crimes by reference to the offender rather than the offence. In doing so, it directs attention to why the occupation of the offender should be regarded as a matter of significance’. As a sub-category of white-collar crime, the offender is not restricted in the forms of crime committed within their occupation. Taking this view into consideration, the offender may commit a range of offences that are considered a form of common crime, for example, robbery or theft or a white-collar crime such as forgery or fraud.

The focus on the offender within this broad paradigm can diminish the act or the significance of the act within the working professional environment. In addition, the very use of the term ‘professionals’ automatically separates the type of offence as it presumes that the individual is a professional or is considered to be educated and of at
least middle-class status. The emphasis on Hayne’s definition rests on the status of the offender. Its association with the concept ‘white-collar crime’ restricts the identity and labelling because of these historical connotations: the association with people committing crime in ‘the suites’, and second, the emphasis rests on the notion that some researchers distinctively examine crime through the nature of the offence. This further reinforces the two distinct schools of thought within the study of white-collar crime.

White-collar crime has traditionally been associated with crimes committed by those labelled as white-collar workers – thus it implicitly describes a class of criminals, not just a type of crime. This may further imply that those who hold traditional ‘blue-collar’ positions have fallen outside this category, according to Sutherland, even though they may commit crimes on the job too! Conversely, this may also mean that white-collar criminals are excluded from this category of offender entirely, even though they may commit street crimes (or hidden crimes of violence in the home, for example).

Although new categories of crime under the rubric of white-collar crime have emerged, there still appears to be an attempt to separate white-collar crime through offence or offender-based definitions (Bloch and Geis 1962; Clinard and Quinney 1967; Coleman 1985; Friedrichs 1996). Ellis and Walsh (2000:517) make the point that, ‘... contemporary researchers define white-collar crime by the nature of the offence rather than by the social status of the offender, so blue and pink collar workers, the unemployed and welfare recipients can commit ... white collar crimes ...’. Ellis and Walsh’s argument has merit and the concept that Sutherland saw as being specific to the middle and upper classes is somewhat dismantled.

While Coleman (1985) recognised the significance of the concept of white-collar crime, he offered a broader approach, which focuses on an offender-based classification (with the inclusion of offences such as tax evasion). Coleman (1985:5) defined white-collar crime as ‘... a violation of the law committed by a person or group of persons in the course of an otherwise respected and legitimate occupation or financial activity’. This definition is problematic in three significant ways. First, it assumes that an individual who commits a white-collar crime has to be in a respectable occupation. Second, the individual is in a position of power, thereby assuming that their illegitimate activity may be legitimised through their status as ‘respectable’ (a point Sutherland strongly argued 1983). Third, it attempts to address violent crimes by including the term ‘occupation’.
Coleman (1985) also attempts to broaden the concept and nature of white-collar crime by acknowledging the role of organisational and occupational crime within white-collar crime. For example, Coleman (1985:8) argues that as organisational crime:

> White-collar crimes [are] committed with the support and encouragement of a formal organisation and intended at least in part to advance the goals of that organisation. Occupational crime ... is white-collar crime committed by an individual or a group of individuals exclusively for personal gain ...

Despite a shift in understanding and recognising the changes of white-collar crime, the definition proposed by Coleman does not adequately distinguish offenders as it involves crimes within an occupational setting, regardless of who gains from the transactions. Therefore, it appears that either definition occurs in an occupational setting.

This section has shown that in more recent times, greater attention has been directed to the offence than to the offender (Calavita and Pontell 1993; Hayne 2002). According to Nelken (1997:899), ‘of greater value are the more ambitious efforts aimed at finding a key theoretical variable which could produce a coherent focus for further research’. A recent example that Nelken (1997) identified includes the work of Shapiro (1984) on trust violation (this will be explored in sub-section 2.6.2).

Braithwaite (1985:3) acknowledges the debates associated with the concept of white-collar crime and notes:

> Most researchers have dealt with the problem of definition by simply studying violations of particular laws (tax, environmental, antitrust, consumer protection, fraud). Patterns and processes of violations of such laws are all phenomena worthy of study in their own right, yet it is a pity that the phenomena do not comfortably sit as building blocks for theorising around a more all-encompassing concept.

In summary, contemporary research on white-collar crime focuses more attention on offences rather than offenders, albeit with many exceptions such as the scholars Shapiro and Braithwaite. Furthermore, this analysis has identified that the growing trend of research examines particular forms of offences rather than all offences under the rubric of white-collar crime.
2.4.3 Conceptual Challenges to the Study of White-Collar Crime

One of the challenges identified in criminological literature is the way in which various sub-categories of white-collar crime are identified and conceptualised. Friedrichs (1996:5) highlights this challenge by making the point that:

In some cases different terms refer to the same activity; in other cases the terms refer to very different types of activity. Obviously the invocation of so many different terms, interrelated in such a bewildering variety of ways, contributes to the general confusion about white-collar crime.


Wellford and Ingraham (1994) conducted a study in 50 states in the United States of America targeting Attorneys-General to determine current understandings of the nature and extent of white-collar crime. Wellford and Ingraham’s (1994:81) study found that a definition of white-collar crime is absent among most of the respondents (cited in Roberts 1994). The respondents also revealed that the term ‘white-collar crime’ means many different things to many different people. Their study showed that a list of representative crimes most commonly resembled a definition of white-collar crime. The fact that white-collar crime is viewed in terms of the offence rather than the offender in this particular study differs from the traditional conception of the offender as an individual in a position of wealth and status.

In challenging criminology’s boundaries of categorising crime, Vande Walle (2002:289) offers an alternative view and argues that:

White-collar crime is an emotionally loaded term, a “political barricade term”, rather than a scientific one. It refers to economic discrimination and the political protection of economic power from prosecution. A more neutral alternative could be “organised economic crime”, which describes the dynamics of crime in general.
Whilst the alternative term ‘organised economic crime’ proposed by Vande Walle attempts to broaden the concept of white-collar crime, a number of problematic issues arise. Firstly, not all forms of white-collar crime are ‘organised’ whether it is within an informal or formal structure. Secondly, new sub-categories of white-collar crime are viewed as economic crime yet the motivation to commit crime varies. This is in contrast to Schlegel and Weisburd (1992) who propose a common ground by arguing that white-collar crime should be viewed from a series of reference points that interact with each other rather than one (rigid) perspective such as the offence or offender paradigm.

To broaden the definitional debate, it is important to note that in its current context, contemporary debates about whether white-collar crime should be defined through the offence or offender (Edelhertz 1970; Coleman 1989; Shapiro 1990; Benson and Moore 1992) or a mixture of the two (see Schlegel and Weisburd 1992) constitute part of the broader response by scholars to the concern about a conceptual consensus on white-collar crime. The emergence of new forms of crime such as cyber crime may underscore a new direction in the study of white-collar crime.

In summary, Sutherland’s research was groundbreaking in that he was the first scholar to open up the area of white-collar crime. His contributions marked a distinct period over the past seven decades in the study of white-collar crime and his research has been instrumental to those who have followed in the area. As the world increasingly develops into a more complex place and new forms of crime emerge, this chapter proposes that if Sutherland’s definition is retained as a foundation for research (i.e. its focus on the status of the offender), it may exclude understanding new forms of crime (see Grabosky et al. 2001) and emerging technologies such as the Internet, which is accessible to a range of people regardless of their social status. In this sense, it is important to consider the point made by Weisburd et al. (2001:10): ‘... were we to narrow the scope of white-collar crime research to the most elite white-collar criminals, we would exclude the bulk of those people who are convicted for so-called white-collar crimes’. Therefore, a broader perspective of scholarly research into white-collar crime opens up the diversity of classes committing such crimes.
2.5 THE STUDY OF WHITE-COLLAR CRIME - PERIODS OF CHANGE

The legacy of Sutherland’s research of white-collar crime has proliferated over the past seven decades (Bloch and Geis 1962; Braithwaite 1985; Coleman 1987; Geis 1992; Schlegel & Weisburd 1992; Geis et al.1995; Weisburd et al. 2001). Contributions that immediately followed were largely the work of Sutherland’s students and colleagues who held a desire to expand the research and concept set out by Sutherland. The focus on white-collar crime after the 1950s also marked the beginning of a new direction of future contributions largely reflected in the work of Clinard (1946), Geis (1967), and Clinard and Yeager (1980).

The development of white-collar crime research over the past seven decades can be categorised into three distinct periods (see Geis 1992). The first period is characterised by the emergence of white-collar crime as a field of study in the late 1930s led by Edwin Sutherland and continued until the early 1960s. The second period encompasses the decline in interest and contributions to white-collar crime research from the mid 1960s to the mid 1970s. The final period is characterised by the renewed interest and large volume of research that emerged towards the end of the 1970s, and which has continued to flourish today.

After its meteoric rise with the work of Edwin Sutherland, the lack of attention to white-collar crime from the mid 1960s to the mid 1970s has been well noted in criminological literature (Katz 1980; Braithwaite 1985; Geis 1992; Punch 1996). Geis (1992:38) acknowledges that ‘after the first burst of creative research on white-collar crime, the subject was virtually abandoned by scholars in the United States during the 1960s’ (cited in Schlegel and Weisburd 1992:38). This is with the exception of Geis’ (1967) study of the heavy electrical industry in the early 1960s, which was the most notable contribution during this period.

During the early part of the 1970s, a social movement against white-collar crime identified by Jack Katz (1980) was well documented (see also Friedrichs 1996; Simpson 2002). Despite the lack of continued developments, the social movement against white-collar crime was largely directed at corporate executives, politicians and governments. The corporate community appeared to ignore or not accept the literature produced by Sutherland and his successors. Geis et al. (1995:5) also observed that during this period,
‘economic conditions were both good and poor ... [whilst] the cold war standoff between the United States and the Soviet Union also produced a patriotic acceptance at home of the status quo’. Notwithstanding the economic climate during this time, white-collar crime was a growing concern among researchers and policy makers.

Despite the limited number of scholarly investigations of white-collar crime from the mid 1960s to the mid 1970s, Katz (1980) notes that the American administration attempted to reduce white-collar crime in different ways. For example, ‘President Johnson initiated ‘Operation Snowball’ in 1964, a nationally coordinated campaign to prosecute the use of corporations for illegal campaign contributions’ (Katz 1980:162). In the early 1970s, individuals were charged with political corruption offences. Katz (1980:162) points out that ‘The United States Attorney in Chicago indicted 256 individuals in 118 political corruption cases ...’ between 1971 and 1976. While practical methods were employed during this period it remains one marked by a significant lack of scholarly research.

It was not long before interest in crimes of the wealthy and powerful rose to even greater prominence with scandals such as the Watergate affair in the United States. Between 1972 and 1974, some three decades after the concept was first articulated, the Watergate scandal became the symbol of public notoriety throughout the US (Simpson 2002). During the 1980s, a resurgence of scholarly research and writing marked the return of the prominence of white-collar crime in the English vocabulary (Braithwaite 1985; Nelken 1997; Rosoff et al. 1998).

In a similar vein, the local and global business sectors have been characterised by a growing number of corporate collapses (for example, Enron, WorldCom, and Arthur Anderson in the United States and HIH Insurance and Harris Scarfe, in Australia) and consequent judicial action against corporations and individuals over the last decade of the twentieth century and in the early twenty-first century. This resurgence of corporate misconduct has re-ignited contemporary debate on what constitutes white-collar and corporate crime (Tomasic 2002; Clarke et al. 2003; Rosoff et al. 2003; Westfield 2003; Pontell forthcoming).
CHAPTER 2: THE CONCEPT AND STUDY OF WHITE-COLLAR CRIME – A REVIEW OF THE LITERATURE

2.6 STUDIES IN WHITE-COLLAR CRIME

The influential work of Clinard and Quinney (1967) and Clinard and Yeager (1980) marked a significant change in the study of white-collar crime by introducing broader orientations such as ‘occupational crime’ and ‘corporate crime’ into the criminological vocabulary. Studies under the rubric of white-collar crime include Sutherland’s (1949) study of 70 United States corporations; Hartung’s (1950) study of the Detroit wholesale meat industry; Clinard’s (1946, 1952) study of black market violations during World War II; Cressey’s (1953) study of embezzlers; Lane’s (1953) study of violations of labour relations and fair-trade laws in the shoe industry; Quinney’s (1963) study of the prescription violations by retail pharmacists; Geis’s (1967) study of the heavy electrical equipment antitrust cases; Clinard and Yeager’s (1980) study of legal violations of the largest United States industrial corporations; Braithwaite’s (1984) study of the pharmaceutical industry; and Shapiro’s (1984) study of securities violations. These studies provided strong direction for understanding the changing nature and extent of white-collar criminality.

2.6.1 Corporate Crime

Corporate crime is one of the most publicly recognised forms of white-collar crime (Smith 2002a) and has attracted considerable legal and criminological attention over the past five decades within and beyond Australia (Clinard & Yeager 1980; Sutherland 1983; Braithwaite 1984; Grabosky 1984; Jamieson 1994; Simpson 2002). According to Clinard and Yeager (1980:13), ‘the increased recognition ... has been a quite natural response to identifiable social forces, perhaps particularly the dramatic increase in the impact of the major corporations on American society’.

Clinard and Yeager (1980:16) defined corporate crime as ‘... any act committed by corporations that is punished by the state, regardless of whether it is punished under administrative, civil, or criminal law’. The definition proposed by Clinard and Yeager marked a distinct separation by acknowledging that corporate crime is a particular type of white-collar crime with different objectives. According to Clinard and Yeager (1980:17):

Corporate crime actually is organisational crime occurring in the context of complex relationships and expectations among boards of
directors, executives, and managers, on the one hand, and among parent corporations, corporate divisions, and subsidiaries, on the other.

This definition needs to take into account whether the acts committed by corporations are to benefit the corporation or act as a mask to benefit individuals or groups of individuals within a corporation. A definition that appears to address this gap and one that has received considerable scholarly attention is offered by Braithwaite. Braithwaite (1984:6) defines corporate crime ‘... as conduct of a corporation, or of employees acting on behalf of a corporation, which is proscribed and punishable by law’. This definition underlines one of the main points distinguishing corporate crime from other forms of white-collar crime: the offences carried out are on behalf of a corporation (in order to benefit the corporation in some way) rather than an individual.

Grabosky (1984) drew attention more broadly to corporate illegality in Australia and provided a paradigm for its analysis (see also Grabosky and Sutton 1989). Grabosky (1984:95) defined corporate crime as an ‘... act, defined as criminal, committed under the auspices of an organisation ...’. Grabosky (1984) identified a range of corporate crimes which include: ‘companies and securities law, taxation, occupational safety and health, environmental protection, consumer protection, restrictive trade practices, discriminatory practices, financial crimes against other businesses, bribery and corrupt practices, economic offences against employees and illegal trading’. Grabosky and Sutton (1989) undertook a comprehensive study of fourteen cases of corporate crime in Australia. The study analysed various forms of corporate criminality such as fraud and included cases which involved the subsequent loss of life through negligence and other means.

2.6.2 Seminal Studies in Corporate Crime

(a) The Heavy Electrical Equipment Industry

Geis (1967) conducted a seminal study of the heavy electrical equipment industry. The heavy electrical equipment industry antitrust violation cases were the subject of intense scrutiny during the early 1960s. Geis (1967) provided a

---

21 The concept of corporate crime also faces conceptual challenges due to the numerous ways in which it has been defined and the forms of crimes that fall under its ambit.
damning account of the various violations perpetrated by executives in the electrical industry. It was noted that 'the most notable characteristic of the 1961 antitrust conspiracy was its wilful and blatant nature. These were not complex acts only doubtful in violation of a highly complicated stature. They were flagrant, criminal offences ...' (Geis et al. 1995:152). These developments were viewed as significant and important steps towards exposing white-collar criminals at a time when corporate offending was relatively hidden.

A number of employees within the heavy electrical equipment industry who committed violations were imprisoned for short periods of time. Although some of the sentences appeared relatively short, it is important to note that these were one of the first recognised cases of imprisonment for white-collar offenders. The offenders ranged in status from sales managers to division managers and vice presidents. Furthermore, corporations such as General Electric were financially penalised for their role in violations of anti-trust, which mainly emanated from settlements to claimants against General Electric. Geis et al. (1995:154) maintain that the settlements amounted to between US$45 and US$50 million by 1962. Fines imposed on General Electric by the courts were minimal (half a million dollars) compared to the earnings by executives, senior management, and against their yearly profit. Empirical research by Geis during this time has since provided criminology with a clearer understanding of white-collar crime (see Meier 2001). Geis’s approach has also broadened the scope of white-collar crime, departing from a focus on specific forms of offenders to the nature of the offence.

**(b) Fortune 500 Companies**

Clinard and Yeager (1980) carried out a study on the violations of regulations enforced by the Office of Price Administration within Fortune 500 companies in the United States of America. The study uncovered legal violations by 477 of the largest industry corporations between 1975 and 1976. The main forms of violations included:

1) *Administrative violations* involve non compliance with the requirements of an agency or court ...
2) *Environmental violations* include incidents of air and water pollution, including oil and chemical spills ...

3) *Financial violations* include illegal payments or failure to disclose such violations

4) *Labour violations* [include] ... discrimination in employment, occupational safety and health hazards, unfair labour practices, and wage and hour violations”

5) *Manufacturing violations* [include] electric shock hazards, chemical and environmental hazards, and fire and thermal burn hazards”

6) *Unfair trade practices* involve various abuses of competition, vertical combinations and horizontal combinations (Clinard and Yeager 1980:113-115).

A number of federal agencies were at some point involved in the process of legal actions brought against the Fortune 500 corporations. During the period 1975-1976, Clinard and Yeager’s (1980:113) study revealed that approximately 60 per cent of the corporations had at least one action initiated against them, and even more notable, 42 per cent of the corporations had multiple cases charged against them. Their study also found that corporate offending was more likely to have been committed by larger corporations than by the smaller or medium sized ones within the Fortune 500 list. Clinard and Yeager (1980:44-9) articulated a number of factors that may explain corporate crime, such as organisational expansion and delegation of responsibility, a desire to strive for and maintain profits over business ethics, to increase market share and corporate growth, and political influence.

The study undertaken by Clinard and Yeager was one of the largest since the pioneering study by Sutherland in the 1940s. In addition to the study of Fortune 500 corporations, Clinard and Yeager (1980:110) undertook a study of 105 wholesale, retail, and service corporations. Although this study was smaller in scope they uncovered a broad range of corporate criminality. Their study identified certain industries in which violations of law were more common, which included oil, pharmaceutical, and motor vehicle industries. Clinard and Yeager’s (1980:32) study also revealed that those corporations violating the law were large, less financially successful, and experienced relatively poor growth rates. The studies undertaken by Sutherland (1983) and later Clinard
and Yeager (1980) both illustrate the extent of corporate criminality amongst some of the largest corporations in the United States. Furthermore, the findings reveal that corporate criminality is not limited to particular forms of companies, industries, or individuals.

(c) The Pharmaceutical Industry

In the late 1970s and early 1980s, Braithwaite (1984) conducted an extensive study of the global pharmaceutical industry. It was also the first major study of corporate crime in Australia. Rather than relying on official documents or media reports, Braithwaite heard first-hand accounts about corporate criminality through interviewing a number of company executives within the industry. Braithwaite (1984:1) observed that not all executives resort to illegal methods; some do attempt to prohibit certain forms of activity such as the exportation of dangerous products to third world countries. There are, however, particular individuals who, in order to increase company profits, participate in illegal activity. For example, one respondent asserted that, ‘... in business you can come up against a dirty stinking bunch of crooks. Then you have to behave like a crook yourself, otherwise you get done like a dinner’ (cited in Braithwaite 1984:2).

Braithwaite (1984:51) noted that a number of pharmaceutical companies whose products do not meet testing standards at home distribute their products to countries where stringent standards are not enforced. Furthermore, Braithwaite identified the falsification of drug testing in order for products to reach the marketplace. Other offences included bribery, which Braithwaite noted was of greater significance than in other industries. There are many forms of bribery, however, as Braithwaite (1984:11) argues, it ‘... has a less acceptable gloss if its purpose is to persuade a health official to allow a dangerous drug on to the market; or, failing that, to entice a customs officer to allow the banned product into the country’. Braithwaite’s study identified a number of these offences as real life examples, which were viewed as common practice in some countries. This study was instrumental in further identifying the extensive range of corporate illegality that occurred within one industry sector. Moreover, it
highlighted the flagrant attitudes taken by various executives to increase company profits at the expense of causing public harm or even death.

(d) **Securities Violations**

Shapiro’s research focused on violation of trust as the central characteristic of criminal behaviour, rather than on the characteristic of the criminal. According to Shapiro (1984:8):

> White-collar criminals cultivate trust. They disarm the protections that have been erected around property and economic transactions and steal freely. Trust allows property thieves to steal without direct contact with victims or physical proximity to the property appropriated, hence protecting them from the risk of discovery and apprehension.

Shapiro’s research underscored the increasing need to trust agents, and the consequent exposure to various forms of abuse of such trust in which agents subordinate the interests of their principals to their own gain (Shapiro 1984).

Shapiro (1984) analysed data based on a study of securities violations from the late 1940s to the early 1970s. The study of offences investigated and prosecuted by the Securities and Exchange Commission (SEC) documented hundreds of cases where ‘wayward capitalists’ were in a position of trust and manipulated individuals in misrepresenting the true nature of their criminal activity. Shapiro’s research identified nine categories of offences – misrepresentation, stock manipulation, misappropriation, self-dealing, investment schemes, registration and technical violations, improper sales techniques and violations of previous restriction.

The most common violations identified were registration violations, misrepresentation, misappropriation and stock manipulation. Shapiro also analysed data on the victims and perpetrators of these offences and illustrated patterns of victimisation. Shapiro’s detailed analysis provided a significant

---

22 Recent corporate collapses have highlighted the strategies used to exploit trust in furtherance of financial gain. In Australia, the collapse of HIH Insurance illustrated strategies of self-dealing and misrepresentation by some of the directors of the company (see Owen 2001). ASIC’s investigation into
CHAPTER 2: THE CONCEPT AND STUDY OF WHITE-COLLAR CRIME – A REVIEW OF THE LITERATURE

contribution to the field of white-collar crime and moved the study of white-collar crime beyond traditional conceptualisations of the white-collar criminal.

2.6.3 Occupational Crime

Occupational crime is defined as a ‘... violation of the legal codes in the course of activity in a legitimate occupation (Clinard and Quinney 1967:131). The concept of occupational crime emanated from the work of Clinard and Quinney (1967) who initially proposed that the terms ‘white-collar crime’ and ‘occupational crime’ should be viewed as interchangeable. Although as Clinard and Quinney (1967:131) point out, ‘... the behaviour to be included in the concept [occupational crime] must be directly related to occupations that are regarded as legitimate in the society’. The problem that this interchangeability poses is that particular crimes such as forgery may not be considered occupational crime because they may not occur within the occupational environment.

This ideation proposed by Clinard and Quinney (1967) arose out of research which examined crimes committed by individuals in their occupations, such as businessmen, politicians, government employees, labor union officials, doctors, and lawyers. Clinard and Quinney point out the various offences that individuals in government may engage in although they accord relatively little attention to the lower or middle management employees who may also commit occupational crimes.

Sutherland’s (1983) concept of white-collar crime referred to an individual ‘... during the course of his occupation’ implying that to commit white-collar crime, it must be undertaken within the business or occupational environment. However, Sutherland never separated occupational crime from other forms of crime in legitimate business occupations. Clinard and Quinney (1967) developed the concept of occupational crime further by arguing that occupational crime usually involves a certain degree of organisation. The validity of this is questionable because not all crimes are committed with other individuals or are organised. This may therefore imply that other participants involved are willing and that organisational factors contribute to the crime. A lawyer,
for example, who fraudulently embezzles funds from his client’s trust account, would be considered to have committed a form of occupational crime (as it was committed during the course of his occupation) despite the fact that it was carried out alone (see Cressey 1953).

Crime in the professions, a sub-category of white-collar crime, has also attracted attention in more recent years (Smith 2002a). Yet concerns about the adequacy of conceptualising it in a framework relevant to the future direction have led Hayne (2002:27) to ask the question:

What is meant by “crime in the professions”? Does it refer to any crime committed by any person who pursues a profession? Is it a more restricted field of enquiry? Is “crime in the professions” all “white-collar crime”? Are the two fields of crime in the professions and white-collar crime coincident or is one a subset of the other?

Hayne (2002:27) asks, ‘are the problems presented by crime in the professions so different that they call for special consideration?’ If this is the case, are the boundaries traditionally and broadly construed by criminology outdated? Although ‘crime in the professions’ is largely committed in the suites rather than in the streets does this mean we abandon the concept because street-style crimes such as murder are occurring in different settings? Hayne (2002:28) argues:

These definitional issues may not seem all that important but there are two elements ... which are important in understanding what is meant by crime in the professions and why it may be thought appropriate to study it separately. Those elements are the relationship of trust or dependence and the abuse of that relationship for personal gain.

According to this school of thought, the element of existence and abuse of trust would be categorised within the ambit of white-collar crime (see Shapiro 1990).

In addition, Hayne (2002) points out that professionals are considered to have obtained a high level of education and are of high social status, a view expressed by Sutherland 1983). Similarly, adopting Sutherland’s definition of a person of respectability and high status in the course of their occupation would again qualify crime in the professions as a sub-category of white-collar crime. Beyond these definitional elements, the views expressed by Hayne (2002) point out that although there are intrinsic differences between the study of crime in the professions and that of white-collar crime, one can identify different elements and argue whether white-collar crime should be viewed as a
separate category. Furthermore, if crime in the professions is viewed primarily through the offender criterion, it may not warrant a separate category from that of white-collar crime.

Although it may appear a significant and transparent development or evolution, the introduction of new categories of crime such as those examined above has also increased the volume of criminological debate about the forms of crime that constitute these sub-categories. For example, Johnstone (1999:117) argues that:

The inclusion of serious frauds by business employees into the category white collar crime should not, however, be seen as an exclusive term. There is a danger in compartmentalising offences. Patterns of criminality develop over time and from a wide range of origins, to dissect white collar crime as separate and different from corporate crime or organised and economic crime may be dysfunctional and hamper meaningful debate.

A crime against capital is another relatively recent offence categorised under the ambit of occupational crime (see Hollinger and Clark 1983; Snider 2001). Snider (2001:109) asserts that ‘...offences committed by outsiders and insiders, customers and employees, who victimise the employer’ are considered a crime against capital. Snider applies examples of fraud, computer crime, shoplifting, and expense account theft to demonstrate her point. Snider (2001:105) examines theft of time as the most recent example despite its historical roots embedded in the nineteenth century. Theft of time refers to ‘...the misuse of the employer’s time and property by an employee ...’. The point to be made here is the extent to which sub-categories of crime under the ambit of white-collar crime are further deconstructed in order to determine elements that define it as crime.

In summary, the inclusion of corporate and occupational crime under the ambit of white-collar crime has enabled greater clarification of scholarly contributions. Of greater significance is the narrowing down of specificity of corporate and occupational crimes to establish new forms of crime as well as enabling a deductive approach by focusing on particular aspects of organisational offending (Erman and Lundman 1982).
2.7 WAYS FORWARD – REFINING THE TYPOLOGY OF WHITE-COLLAR CRIME

Should we talk of white-collar crime or organisational crime or corporate crime? Or, instead of crime, should we talk of law breaking, or deviance, or violation of trust, or misconduct, or transgression? (Braithwaite 2001:17)

As Sutherland’s legacy continues within the field of criminology, distinct shifts in research have clearly emerged. These conceptual shifts developed due to attempts to redefine the parameters of white-collar crime, which were viewed as inadequate in their current form. As the previous sections illustrated, most notable have been the introduction of sub-categories of white-collar crime, such as occupational crime (Clinard & Quinney 1967), organised crime (Cressey 1969), corporate crime (Clinard & Yeager 1980), elite and political deviance (Erman and Lundman 1982; Simon & Eitzen 1993), and crime in the professions (see Smith 2002a). These sub-categories appear to further separate forms of common or conventional crime from white-collar crime at a definitional level.

2.8 SUMMARY

Traditional and contemporary research presents a multifaceted view of the concept of white-collar crime. Attempts to redefine the parameters of white-collar crime have meant that new concepts such as those aforementioned have emerged over the past six decades and continue to do so. The types of people committing crime cannot be identified solely by reference to class or status as theorised earlier by Sutherland, which suggests the limited applicability of defining white-collar crime through offender-based classifications. The consequential questions become whether white-collar crime and criminals can be incorporated productively within the explanatory scope of traditional criminological theory. To these questions we turn in the next chapter.
CHAPTER 3: THEORIES OF CRIMINAL BEHAVIOUR AND THEIR RELATIONSHIP TO THE STUDY OF WHITE-COLLAR CRIME

3.1 INTRODUCTION

As illustrated in Chapter Two, the concept of white-collar crime, developed in the 1930s by Edwin Sutherland, has undergone a number of distinct changes to incorporate new and emerging categories of crime. One of the more important observations made in the previous chapter was the way in which scholars have both built upon and contested the original concept of white-collar crime over its 70-year history. Scholars have also developed white-collar crime as a significant field of study through the application of empirical research to a wide range of industries.

The parameters of white-collar crime have broadened significantly due to the growing development of new forms of criminality and the changes in technology and accessibility. The concept has developed through a number of different axes – theoretical, ideological, empirical, legal, and philosophical. Subsequently, a range of approaches has tried to explain white-collar crime and criminal behaviour. Given that theoretical explanations of crime and criminal behaviour date back to the eighteenth century, contemporary criminology has been challenged to explain criminal behaviour beyond the framework of conventional or street crime.

The objective of this chapter is twofold. First, it traces the historical development and early principles of criminology. Second, it explores six theories of criminal behaviour and demonstrates the scholarly contributions made to the study of white-collar crime. Section 3.2 outlines three traditional schools of thought – the classical school, the positivist school, and the Chicago school to develop a broader insight into contemporary perspectives of this growing body of criminological literature. Sections 3.4 to 3.9 analyse a diverse range of sociological and criminological theories beginning with Wilson and Herrnstein’s (1985) constitutional learning theory, followed by Sutherland’s theory of differential association (1939), Merton’s strain theory (1938), Sykes and Matza’s (1957) techniques of neutralisation, Cohen and Felson’s (1979) routine activity theory, and Gottfredson and Hirschi’s (1990) general theory of crime.
3.2 TRADITIONAL PARADIGMS OF CRIMINOLOGY

In most criminological histories, the true beginnings of modern criminological thought are seen in writings of the eighteenth and early nineteenth centuries (Garland 1997:23).

Following on from Garland’s observations, this chapter begins with the traditional criminological schools of thought to develop an understanding of their relevance to contemporary theories. Early scholarly influences on the discipline of criminology are distinguished through the classical school and the positivist school. Given the focus of this thesis, it is also important to discuss contemporary criminological schools of thought. The Chicago school for example, developed much later and represented a marked divergence from the positivist school’s explanations of criminal behaviour.

In the nineteenth century, the classical school and the positivist school exerted considerable influence over the development of criminology. In the twentieth century, the Chicago school exerted equally strong influences over the development of less positivist strands of criminological thought. The following sub-sections will focus on a number of these influences and contributions, which have received considerable criminological and sociological attention over the past two centuries (see Sykes and Matza 1957; Matza 1964; Taylor et al. 1973, Garland 1997; Gartrell and Gartrell 2002).

3.2.1 Classical School of Criminology

Tracing the development of criminology is more than a matter of historical interest. Some ideas from the past continue to provide the framework for current thinking in the field. Some ideas, long since rejected by criminologists, still influence popular thought. Bits and pieces of older theories continue to float to the surface, like debris from a sunken ship; and some formulations, now abandoned, warrant re-examination (Sykes and Merton 1978:7).

The classical school of the eighteenth century emanated from the Age of Enlightenment (Taylor et al. 1973). The classical school reacted against the contemporary system of law and justice by challenging the structure of sentencing and barbaric punishments, which dominated legal systems in eighteenth century Europe (Taylor et al. 1973). The philosophy of the classical school was based on the doctrine of free will, and behaviour
was guided by rationality and hedonism (see Fattah 1997; Liska & Messner 1999). The approach by the classical school, that people were guided by free will, was a shift from emphasis on individualism and criminal characteristics (during the age of enlightenment). As Taylor et al. (1973:1) point out ‘the central tenet of classicism was that the rights of man had to be protected against the corruption and excesses of existing institutions ...’. The classical school adopted a legalistic approach to criminal behaviour.

Classical criminology’s focus was directed towards defining the offence rather than the offender because criminality was predominantly seen as a matter of making the wrong choice (White and Haines 2000). Punishment was therefore determined by the offence committed and viewed in terms of the severity of the crime, not the behaviour of the offender.

Critical criminologists such as Taylor et al. (1973:2-3) made the following observations about classical theory and noted that:

... Classical theory is above all a theory of social control: it delimits first, the manner in which the state should react to the criminal, second, those deviations which permit individuals to be labelled as criminals, and third, the social basis of criminal law.

Two prominent scholars in the eighteenth century who were closely identified with the work of classical criminology were Cesare Bonesana, Marchese de Beccaria (1738-1794) and Jeremy Bentham (1748-1832). Beccaria, an Italian philosopher and Enlightenment thinker, has been recognised in contemporary literature as one of the leading philosophers and penal reformers during the Age of Enlightenment (see Vold 1958, 1979; Fattah 1997; Vold et al. 2002). Beccaria’s work reflected the criticisms levelled at government policies and the management of public affairs through an empiricist approach (see Vold 1979).

Beccaria’s ideologies followed in the path of Hobbes (1588-1679) and advocated a theory of social contract. Social contract refers to an understanding that is implicit between individuals and the society in which they live, whereby individuals give up certain rights to the state in exchange for protection of their rights and security of their

---

23 Hedonism was based on a pleasure/pain principle which meant that individuals may see that the pain of the sentence received for crimes committed would outweigh the pleasures received from committing the
property from other individuals (White and Haines 2000). This understanding between the individual and society was seen as implicit to retaining stability while advocating freedom to individuals. If an individual violates another’s freedom, Beccaria ([1764] 1963) believed he or she violated the social contract by which they all lived.

One element Beccaria advocated strongly was equality in the eyes of the law. This was because Beccaria felt the system at the time was ineffective and brutal and therefore advocated a restricted capacity of criminal law (Sykes and Merton 1978). Beccaria ([1764] 1963:13-14) maintained that:

... only the laws can decree punishments for crimes; authority for this can reside only with the legislator who represents the entire society united by social contract. No magistrate can, with justice, inflict punishments upon another member of the same society.

Individuals during this period were deemed to be responsible for their own actions and their behaviour was viewed as a result of individual choice. Vold (1979:25) points out that for Beccaria, ‘... prevention of crime is more important than punishment for crime committed; that punishment is desirable only as it helps prevent crime ...’. This meant that punishment would play a fundamental role as a deterrent to crimes that detract from the welfare of other individuals and the state (Taylor et al. 1973). Beccaria argued strongly that punishments should not be modified for each individual, regardless of the crime (Fattah 1997), therefore promoting standardised penalties.

Beccaria proposed a number of doctrines to further enable the criminal justice system to operate at a greater level of competence and value to the public. Despite being recognised as one of the leading reformers of his time, it is important to note that penal reforms were largely developed with a focus on the poor and disadvantaged rather than the privileged and elite who appeared to be relatively immune from criminal punishment (Newman and Marongiu 1990). This was despite the idea of the classical school that an individual’s choice to commit crime could be made by anyone, regardless of social status.

At the time, Beccaria’s theories were viewed as radical, deviating from traditional, spiritual and religious explanations of criminal behaviour (Vold et al. 2002:15).
Chapter 3: Theories of Criminal Behaviour and Their Relationship to the Study of White-Collar Crime

Beccaria's work, while not considered within the framework of criminology, rose to prominence in criminological literature. However, there is contestation of his contributions (see Newman and Marongiu 1990; Fattah 1997). For example, Newman and Marongiu (1990) maintain that Beccaria's contribution to reform was not as profound as other social contract thinkers of that period. They cite the work of Voltaire (1694-1778) and Bentham as having more significance during this period. Despite the various challenges posed by social contract thinkers, the work of Beccaria influenced the work of others who followed him, such as Jeremy Bentham, and greatly influenced criminological theory.

Jeremy Bentham (1748-1832) has been recognised as one of the influential thinkers and contributing scholars of the classical school (Newman and Marongiu 1990). Bentham, a prominent legal reformer, demonstrated an approach to the role of law and legislation which enabled him to contribute significantly to classical criminology. For example, Bentham advocated that all individuals should be aware of the law and that they be treated with due process. Bentham's profound knowledge of the law and legal system (having studied and practised as a lawyer) laid the foundation for his role as an advocate, through which he developed ideas for social and political reform. As Sykes and Merton (1978:10) observe, Bentham '... played a major part in developing these ideas and forcing them upon the attention of the English legal system ...'. Beccaria viewed law as a negative element for individuals, however, he also understood that laws benefited the social order and government (Merton 1978).

Bentham ([1798] 1907) was greatly influenced by the work of David Hume (1711-1776) (see Atkinson 1969). During his time, Bentham had written and published numerous books and papers, for example, A Fragment on Government (1776) and Principles of International Law (1798). It was A Fragment on Government, which Atkinson (1969:35) notes were Bentham's '... first work of any importance ... and took the form of destructive, if somewhat cautious, criticism applied to certain doctrines of constitutional law ...'. Despite the influence of Bentham's work and that of others such as Voltaire, a new direction within criminology subsequently challenged the doctrines of classical criminology, especially its notion of free will and rationality. This new direction came from the emergence of criminological positivism.
3.2.2 Positivist School of Criminology

The positivist school of criminology developed in the nineteenth century through the work of the pioneering criminologist, Cesare Lombroso (1835-1909) and was later carried on through Enrico Ferri (1856-1929) and Raffaele Garofalo (1851-1934).\textsuperscript{24} Criminological positivism applied a scientific method to the study of crime, a technical means of finding the origins of criminal behaviour by using empirical methods of science. Furthermore, criminological positivism sought foolproof foundations of knowledge. This was a direct move to reduce the central ideology of classical criminology: the doctrine of free will.

Criminological positivism constructed the idea of a criminal class. Lombroso and his associates believed they could discover the hereditary causes of criminal behaviour, in other words, a determined category of conduct – biological and psychological factors that determined criminal behaviour. Lombroso-Ferrero and Savitz (1972:x) comment that Lombroso and his associates

... believed they had created a "new science": criminal anthropology. The basic methodology of this science comprised anthropometric measurements of the cranium and the description of anomalies of the face and of peculiarities of the bodily structure.

This was a significant departure from the classical school's focus on the criminal justice system and legal reform. This ensured that the focus of the positivist school's doctrines lay with the criminal actor, rather than the criminal law as proposed by the classical school (see Matza 1964; Fattah 1997).

The philosophy of the positivist school meant that there was less emphasis on punishment and greater emphasis on rehabilitation (Krambia-Kapardis 2001). According to Young (1998:15), 'the positivist school claimed to have discovered evidence of the existence of 'criminal forms' whose behaviour was determined rather than chosen and for whom treatment rather than punishment was appropriate'. The emergence of prisons provided a laboratory for the study of criminal behaviour in which

\textsuperscript{24} It is important to note that the Belgian astronomer and social statistician, Quetelet (1796-1874) and Guerry, were equally strong influences to positivism. Quetelet's research explored the social mechanics of crime with an emphasis placed on mathematics, biology, and meteorology to determine the causes of
observations and measurements allowed criminologists to classify criminals (Young 1998). In the case of criminological positivism, an individual’s background was recognised as the causal factor of crime, and therefore committing a crime could no longer be considered an act of choice.

Lombroso, regarded as the founding father of the positivist school (Taylor et al. 1973), initially studied delinquent soldiers and was the first philosopher to use the term ‘criminaloid’ to describe thieves.25 Lombroso developed a theory based on a number of primary elements, such as the belief that some individuals possessed physical traits that demonstrated he or she was a born criminal (atavistic) (for example, cranial and bodily measurements) and therefore distinct from non-criminals (Lombroso-Ferrero and Savitz 1972); that some criminals were insane, shared atavistic characteristics and were influenced by environmental factors, and that criminals committed crimes out of passion.

Lombroso and his associates undertook a major research project on inmates to measure proportions of physical features of criminals (see Lombroso 1872). For example, Lombroso measured the size of an individual’s skull to determine criminality. The empirical study examined the classification of populations and developed a psychological system to allow for the individualisation of crime, a shift from the classical school’s focus on the offence. Inherent in Lombroso’s initial theory was the belief that a criminal did not become so due to social conditions but predominantly through biological determinism, however, he later revised his theory to include environmental (climate, marriage, structure of government) and social explanations.

Although the central focus of criminological positivism remained on biological factors, emphasis on the aetiology of criminal behaviour shifted during the positivist period. Inherent in the development of other contributing variables to crime causation was Ferri’s interest in social, economic, and political correlations and Garofalo’s concern with psychological explanations of criminal behaviour (Hazelhurst 1996). In an examination of positivist criminology, Matza (1964) incorporates sociological factors

---

25 Lombroso was a serving medical officer in the army.
into the debate. Matza (1964:15) argues that, ‘with the advent of environmental primacy, positive criminology has taken two major forms – one stressing intimate factors, the other, broader and wide events’. Matza termed these ‘personality theory’ and ‘sociological theory’. These two additional elements incorporate multiple factors such as the social and cultural environment to ‘modify’ the notion of positivism.

Many critiques were offered to counter Lombroso’s focus on biological and psychological variables as the predominant explanations for criminal behaviour. According to Matza (1964:4):

Positive criminology has come very close to ignoring the defining character of delinquents – the fact that they commit infractions – in its various explanations of delinquency. Consequently, it has failed to scrutinise the nature of legal prohibitions and the emergence of delinquency customs which parallel and distort legal views.

Matza’s examination of juvenile delinquency illustrates one of the underlying criticisms of the positivist school. The view put forward by Matza is consistent with Broadhurst (2002:38), who argues that:

- Positivism ignores choice and creativity and denies individual activity as meaningful.
- Positivist limit the scope of agency in crime causation.
- Crime is abnormal not a protest or arising from different value systems.
- [Positivism] tends to ignore the fact that normal socialisation may lead to crime and relies too much on the success of meritocracy in determining one’s status by ignoring the many barriers to individuals fulfilling their potential.

While Lombroso and his associates postulated many theories that linked criminal characteristics with physical features of individuals, the methodology with which the observations were carried out calls into question the validity and nature of the data published during this time (see Fattah 1997). Lombroso’s study initially lacked a comparative analysis with non-criminals to give strength and validity to his theory that criminals were of a distinct physical type (see Goring 1913). Charles Goring, for example, carried out a study comparing a large number of English non-criminals to 3000 English convicts.
In general, Goring’s study found no significant physical anomalies that distinguished non-criminals from criminals, which Lombroso’s theory claimed. Vold (1979:59) notes, ‘there were no more protrusions or other peculiarities of the head among the prisoners than among the Royal Engineers’. Furthermore, other characteristics such as colour of hair and eyes were examined by Goring with only minor differences found (Vold 1979). In 1939, Hootan, a Harvard anthropologist, challenged Goring’s methodologies and conclusions after a re-examination of Goring’s study (Vold 1979:61). Hootan’s study, which examined more than 17,000 people, including prisoners and non-criminals, confirmed that there were significant physical differences between criminals and non-criminals, however, the study was met with controversy (see Vold 1979).

Positivism has continued its influence in parts of contemporary sociological thinking in a number of important ways. A content analysis of American and English sociological journal articles from 1966 to the late 1980s found that within the US, ‘... positivism has become increasingly encapsulated ...’, a contrast to that in the UK, where it has become disavowed, ‘... particularly in its ‘instrumental’ form’ (Gartrell and Gartrell 2002:653).

Lombroso’s emphasis on examining multiple factors explaining criminal behaviour has also been an influence upon contemporary theories of criminal behaviour. Furthermore, Lombroso and his associates shifted attention from the legal and juristic explanations of criminal behaviour to that of seeking explanations of the individual (White and Haines 2000).

Despite the various evaluations of Lombroso’s contribution to criminology, Radzinowicz (1961:3) makes the observation that:

Virtually every element of value in contemporary criminological knowledge owes its formulation to that very remarkable school of Italian criminologists who took pride in describing themselves as the “positivists” and who, in contradistinction to the “classicists” led by Francesco Carrara, regarded criminal law as a changing social institution and crime as a product of individual disposition and environmental forces.

---

26 Broadhurst (2002:32) notes that Goring’s (1913) criticisms of Lombroso’s research were largely methodological.
Radzinowicz (1961) notes that Lombroso’s theory should be viewed in relation to its time and the significant developments that have contributed to its position within criminology. However, White and Haines (2000) make the point that criminological positivism focused on conventional forms of crime and juvenile delinquents, neglecting white-collar crime and adult offenders. This appears to be a central theme in traditional criminological literature and an important issue to consider.

In summary, the two schools of thought (classical and positivist criminology) illustrate different ideological paradigms, which have laid the foundations for the explanation of crime, criminal behaviour, and penal reform through these broad-based offender or offence classifications. These approaches should not be viewed as paradigms that have been widely accepted in their applicability to crime causation (see Gorecki 1974). However, they do provide a historical focus for considering contemporary theoretical departures and developments from criminological positivism. With the emergence of new theories of crime and criminal behaviour, the emphasis on the social and ecological environment played a significant role towards the early part of the twentieth century.

3.2.3 The Chicago School

The early twentieth century spawned a number of sociological theories that focused on the influence of social and ecological variables to explain patterns of criminal behaviour. Sampson (2002:214) notes that ‘the very discipline of sociology was founded on late nineteenth-early twentieth century upheavals widely thought to have frayed the social fabric of American communities ...’. In this case, the community life in Chicago was marked by crimes committed mainly in slum areas. Crime was therefore viewed as a function of the social change taking place in Chicago. At the forefront of research during this period was the Chicago school of sociology.

During the 1920s and 1930s, the Chicago school was the leading edge in sociological research on juveniles. The Chicago school’s ecological and social-disorganisation approach to crime centred on the lives of ordinary people (largely male juvenile delinquents), and the social and cultural conditions that contributed to their particular environment. This was a departure from traditional research in those days, which focused almost exclusively on individual characteristics or the act itself.
Robert Park and Ernest Burgess, two of the leading scholars of the Chicago school, concentrated on the developmental structure and changing dynamics of community life in Chicago as part of their research. Drawing on the influential work of Park and Burgess, Clifford Shaw and Henry McKay (1931) made substantial contributions to the study of crime, social change, and ordinary people with their seminal research on juvenile delinquency in the Chicago area (see Bulmer 1984). Shaw and McKay’s research concentrated on the social disorganisation approach of crime rates for delinquents and proposed that delinquency rates in Chicago were higher in areas of social disorganisation. Their study concentrated on areas of public interaction such as work and place of residence (Taylor et al. 1973:110). Delinquency was most commonly found in areas that were in a process of deterioration. These areas were located near the central business and industrial districts in Chicago (see Byrne and Sampson 1986).

The seminal ecological studies of Shaw and McKay (1931) were distinguished by their method of research, which enabled them to study delinquents in their natural environment. Shaw and McKay undertook their research by living in ghettos and with families in their own community and continued their research by studying the neighbourhood. Over a three-year period researching different areas of the city, Shaw and McKay acquired significant statistical data on delinquency in these communities (see Vold 1979). Their empirical study was supported by applying their findings to areas outside Chicago, such as Denver and Philadelphia (Taylor et al. 1973). As Shaw and McKay (1931:18) observed, ‘... delinquency has become a more or less permanent aspect of the social activity of the boys living in this neighbourhood. It is, apparently, a part of the culture and tradition which is transmitted through the medium of social contact’. Shaw and McKay viewed the social and cultural condition in which the delinquency lived as accounting for criminal behaviour. This first-hand research represents a significant departure from the methodological approach of criminological positivism.

Shaw and McKay’s concept of delinquency was analysed in relation to the mental and physical condition of the offender, incorporating the total sequence of events in an individual’s life. Shaw and McKay viewed delinquency as a product of the social conditions and the environment in which they lived. Furthermore, they found that the deterioration of urban areas provided a platform for various social norms and
behavioural patterns to create social disorganisation. This disorganisation was largely attributed to juveniles living in densely populated areas, low socio-economic conditions, and also to the influx of migrants. Shaw and McKay (1942) observed that crime levels decreased away from the city centre.

Researchers of the Chicago school may have perceived that the origins of the problems in which they were studying lay in the larger social organisational network. This is because they sought not to place blame on the family, but to place responsibility squarely upon the community in which the delinquents were living. According to Park et al. (1925:106):

It is in the community, rather than in the family or the neighbourhood, that formal organisations like the church, the school, and the courts come into existence and get their separate functions defined ... However, neither the orphan asylum nor any other agency has thus far succeeded in providing a wholly satisfactory substitute for the home. The evidence of this is that they have no alumni association ... It is in this community with its various organisations and its rational, rather than traditional, schemes of control, and not elsewhere, that we have delinquency. Delinquency is, in fact, in some sense the measure of the failure of our community organisations to function.

Through their extensive research on the city’s social and human dynamics, Shaw and McKay’s study of delinquency resulted in the development of a social ecological approach to crime including a theory of delinquency areas in Chicago. The connection between social disorganisation and poverty was one of the primary variables that explained rates of criminal behaviour. Up until that time, the majority of research viewed delinquency only in relation to the context and life history of the individual.

Shaw and McKay’s (1931) research found that poverty was concentrated in urban areas with high levels of social disorganisation and racial and ethnic diversity. In addition, their research showed that the absence of social control predominantly contributed to high crime rates (see also Bursik and Grasmick 1993). It is important to note that studies have shown that crime rates may reduce where neighbourhoods are more resilient (see Markowitz et al. 2001).

In the early twenty-first century, the Chicago school’s research may be regarded as less scientific than that of the positivist school, although their methodologies were novel in their time. The distinction that gives the Chicago school its valued place in sociological
research is the emphasis on explaining rates of crime and delinquency through an understanding of the need to place these phenomena in a related social context. Their methodologies also allowed sociology and criminology to develop new insights into criminal behaviour.

The Chicago school’s enduring contribution was the emphasis on the social and ecological link instead of the previous biological or psychological explanations of crime and deviance. However, Taylor et al. (1973:111) argue that ‘... the ecological tradition is the tradition most responsible for the continuing hold of positivist assumptions in American sociology’. This approach has received considerable scholarly attention within criminological literature over at least the past five decades. In essence, the hallmark of the Chicago school was its broad, intellectual endeavour with the aim of social improvement of life in Chicago (Bulmer 1984). In addition, the Chicago school distinctly broke from its contemporaries by initiating what may be regarded as a series of quite different and creative approaches to these problems in attempting to analyse crime and deviance amongst juveniles.

Despite the considerable attention received by the Chicago school, there were limitations in Shaw and McKay’s research. The primary limitation was the inherent connection between poverty and crime, an established view that has continued to prevail within modern criminological thought. According to Sykes and Merton (1978:96-7) their research:

... strongly reinforced the idea that crime and poverty-stricken portions of the community went hand in hand; and if such “ecological” correlations needed to be interpreted with some caution ... the close association between crime and economic want seemed well established.

Furthermore, Shaw and McKay’s theory does not appear to apply to middle and upper class individuals, including white-collar offenders (see Makkai and Braithwaite 1994) and female offenders. It is important to note that research exploring whether social disorganisation contributes to white-collar offending is limited.

The Chicago school of criminology, a body of scholars who profoundly influenced Sutherland and were largely his contemporaries, never turned its attention to the problem of white-collar crime. Despite this, the Chicago scholars foresaw the importance of integrating theory and research. Moreover, it was the city of Chicago,
with its stark contrast and blend of ordinary people and architecture, which challenged epistemological positivism and therefore represented a dynamic shift from the historic preoccupation with criminological positivism.

Recent studies have empirically tested and built upon the social and ecological disorganisation theory of crime set out by Shaw and McKay (1942) in a number of divergent contexts (see Bursik and Webb 1982; Sampson and Groves 1989; Bursik and Grasmick 1993; Osgood and Chambers 2000; Smith et al. 2000;27 Markowitz et al. 2001; Kane 2002; Lane and Meeker 2004).

Osgood and Chambers (2000:81) expanded upon the social disorganisation approach of Shaw and McKay by analysing arrest rates for juvenile violence in 264 non-metropolitan counties of four states of the United States of America. This was a departure from traditional studies, which focused on urbanised areas. In general, the study by Osgood and Chambers (2000:81) supports social disorganisation theory, in particular where residential instability, family disruption, and ethnic heterogeneity were variables associated with juvenile violence. However, their study found that juvenile violence was not a product of poverty, a claim made by Shaw and McKay. The broader argument by Shaw and McKay demonstrated that social disorganisation creates delinquency, with poverty as the primary factor.

Kane (2002) applied the social ecological approach to misconduct cases within the police precincts and divisions in New York City. Kane's (2002) study analysed data for the period 1975-1996 to determine whether patterns of police misconduct were a result of the variations in social ecological conditions. Kane (2002:887) observed that:

... structural disadvantage, population mobility, and increases in Latino population predicted increases in police misconduct, and further, that most of the variation at both the precinct and division levels occurred primarily within territorial areas rather than between them.

Kane's study concluded that within a professional network, social disorganisation and a change of a community's conditions can impact upon the level of criminal offending.

27 Smith et al.'s (2000) study seeks to integrate social disorganisation theory and routine activity theory through an analysis of street robbery.
Lane and Meeker’s (2004) study applied social disorganisation and fear of gang crime among various groups – Caucasians, Latinos, and Vietnamese. The study found that ethnicity and race impact upon perceptions of fear and victimisation particularly among minority groups. According to Lane and Meeker (2004:57), ‘... both Latinos and Vietnamese were more likely than Whites to live in areas with more social disorganisation, so their stronger concern about community problems made sense’. Concerns about gang crime elevated the fears particularly among the Vietnamese followed by Latinos, rather than feelings of risk. Lane and Meeker’s (2004:58) study therefore found that fear and risk are not inherently connected

As prior studies indicated, community diversity and disorder problems might prompt a general unease in people about their future safety from crime and gangs, even if they did not believe that they were in immediate danger of being victimised.

In summary, this section has shown that the three schools – classical, positivist, and the Chicago school – sought to explain the nature and aetiology of crime and criminal behaviour through different theoretical approaches. The classical school believed that behaviour was guided by the pleasure/pain principle, criminality was viewed as a matter of making the wrong decisions, and crime was defined as a violation of law. A distinct shift emerged in criminological positivism towards a focus on the individual (offender) and individual characteristics such as mind and body (Garland 1997). At their simplest, those conceptualisations that focus on the offence borrow heavily from various classical positions, and those which focus on the offender borrow from positivist positions. During the mid-twentieth century, sociological theories of criminal behaviour such as the Chicago school dominated research, with less emphasis on the offender and greater emphasis on social and ecological factors.

3.3 TOWARDS A PARADIGM FOR UNDERSTANDING CRIME AND CRIMINAL BEHAVIOUR

... If we look beyond the immediate data of crime and punishment to the processes that underpin them – to routines of social life and social control, the circulation of goods and persons, the organisation of families and households, the spatial ecology of cities, the character of work and labour markets, the power of state and authorities – it becomes apparent that criminology’s subject matter is centrally implicated in the major transformation of our time (Garland and Sparks 2000:1).
The study of crime and criminal behaviour can be categorised in two distinct categories, conventional or ‘street crime’ and white-collar crime. Traditionally, conventional crime has been the central focus of criminological research, in other words, crimes of a personal nature, such as theft, robbery, and murder (see Clinard and Quinney 1967; Bequai 1978; Sutherland 1983; Braithwaite 1985; Coleman 1985; Schlegel and Weisburd 1992; Fattah 1997; Weisburd et al. 2001; Simpson 2003; Lynch et al. 2004). This focus is consistent with empirical studies, which have largely concentrated on those crimes considered serious in nature with a perceived physical ‘community’ impact and ‘public profile’ (see Wilson 1975). Furthermore, criminological theories have focused on the behaviour of the poor and relatively powerless and also upon juvenile offenders (see Taylor et al. 1973; Sykes and Merton 1978; Braithwaite 1979; Vold 1979; Sutherland 1983; Fattah 1997; Young 1998; Krambia-Kapardis 2001; Weisburd et al. 2001).

A range of studies continue to underscore criminology’s focus on conventional crime with examinations of white-collar and corporate crime’s significance appearing in criminological journals, textbooks, criminal justice education, and PhD programs (Wright and Friedrichs 1991; Cullen and Benson 1993; Lynch et al. 2004). Lynch et al. (2004) conducted a study that analysed criminological literature to find whether previously long-held assumptions of criminology’s focus on street crime are still valid. Their study showed that:

... across both journals and textbooks, traditional research focusing on various forms of ordinary street crime far outweighed research on corporate and white-collar crime. The ratio of articles and pages published on ordinary crime relative to corporate/white-collar crime coverage was fairly consistent across journals and textbooks: 10:1 (Lynch et al. 2004:395-6)

Despite significant research into corporate and white-collar crime over the past seven decades, Lynch et al’s study confirms that white-collar crime is still underrepresented in criminological literature. Corporate crime scholar, Simpson (2003:1) pointedly remarks:

... it is striking how little my generalist colleagues know about this area of specialisation ... a quick perusal of most criminology textbooks reveals what passes for “common” knowledge in this area ... In fact, these summaries have changed little over the years ...
The fundamental challenge to criminology has been whether theories of criminal behaviour that have focused on the poor and powerless can be generalised to those of the middle and upper classes and to corporations. Despite the early research, which neglected crimes of the upper class world, various contemporary theories of criminal behaviour have sought broader explanations of the nature and aetiology of crime, including white-collar crime. As such, criminology has seen attempts by theorists to devise one theory to explicate all forms of crime and criminal behaviour (see Sutherland 1939; Gottfredson & Hirschi 1990). The following section will explore six contemporary theories of criminal behaviour and assess what contributions have been made to explain white-collar offending through existing theories of criminal behaviour.

3.3.1 Theories of Crime and Criminal Behaviour – A Contemporary Profile

Theories are conceptual means of interpreting and explicating information. They come into competition only when they offer alternative and incompatible explanations for the same data. Since one theory effectively supersedes another only when it explains the same range of data and problems more plausibly ... (Garland 1990:13).

Garland’s point effectively captures the diverse nature and contribution theories can offer in order to develop broader frameworks for understanding crime and criminal behaviour. Theories of crime and criminal behaviour have fascinated philosophers, criminologists, sociologists, and psychologists for at least three centuries. Early theoretical approaches to crime causation have been predominantly grouped into three categories – biological and physiological, psychological, and sociological. Sykes and Merton (1978) observe that this categorisation occurred during the 1920s and 1930s.

Psychological explanations arose from the focus on the psyche of an individual, while the work of sociologists attempts to explain crime causation through the social and ecological environment (see Shaw and McKay 1942; Sykes and Merton 1978). Psychological theories initially arose from the work of Sigmund Freud (1856-1939) with psychoanalytic theory. Freud’s doctrines have played a major role in the explanation of human behaviour through shaping contemporary theories in modern society (Williams 1997). Other theoretical contributions include cognitive development theory (see Kohlberg 1976), learning theory (Eysenck 1964, 1977), and constitutional learning theory (Wilson & Herrnstein 1985).
There are a number of theoretical strands within the discipline of psychology that have played a significant role in explanations of criminal behaviour.  Williams (1997:197) explains that ‘psychology is often separated into two groups of theories or schools of thought: cognitive and behavioural’. Explanations of criminal behaviour have also been offered through positivism, in which emphasis was placed on biological and neurological factors (Krambia-Kapardis 2001). In more recent times, attention has also been directed towards connecting environmental and social variables to determine the cause of criminal behaviour (see Williams 1997).

Sociological theories of crime and criminal behaviour have three broad areas of focus. These areas will be discussed in the following sections and incorporate: the disintegration of societal values and cultural beliefs under the constraints of a social disorganisation approach (see Shaw and McKay 1931; Sutherland 1939); the focus of strains and norms that are inherent in the functioning of society which, under certain conditions, produce a state of anomie (see Merton 1938); and the existence of subcultures and their role in fostering attitudes and behaviour where crime is accepted (Sykes and Merton 1978:247). These areas of focus are not exhaustive and illustrate a number of variations depending on the influencing factors (see Wilson and Herrnstein 1985). However, these approaches underlie the paradigm shift towards disparate explanations of criminal behaviour.

The challenges posed for criminology in more recent times have been the overwhelming number of theories and explanations which continue to focus on conventional crimes and juveniles. However, while this may be so, not all theories have adequately presented a strong argument and many have lacked empirical support (see Gorecki 1974). Over the second half of the twentieth century, theories of crime and criminal behaviour have become increasingly important for understanding the changing nature of crime. Accordingly, a number of contemporary theories have expanded on earlier models, while new theories have been put forward in the hope of providing a stronger paradigm of explaining criminal behaviour.

28 It is important to note that psychological theories of crime can be drawn to the earlier work of the positivist school in the late nineteenth century (Krambia-Kapardis 2001).
3.4 CONSTITUTIONAL LEARNING THEORY

Wilson and Herrnstein's (1985) constitutional learning theory developed towards the end of the twentieth century and extended beyond the traditional boundaries of criminological theorising. This was achieved via its application to include different forms of white-collar crime such as fraud and embezzlement in their study of criminal behaviour. Wilson and Herrnstein identify a number of different factors to explain the aetiology of criminal behaviour. For instance, their theory incorporates psychological arousal and intelligence in an effort to understand individual differences in behaviour. Integrated in their theory are biological influences, social learning patterns, and environmental factors that Wilson and Herrnstein view as developing over the course of an individual's life, which becomes intrinsic to further understanding individual behaviour.

The premise of Wilson and Herrnstein's theory takes into account the determining factors that lead an individual to commit crime, and the consequences of such actions. For example, if the gain of committing a criminal act (rewards) exceeds the loss (punishment) for such an action, then an individual may be more inclined to commit the crime (Wilson and Herrnstein 1985). Wilson and Herrnstein (1985:44) argue that 'the larger the ratio of the net rewards of crime to the net rewards of noncrime, the greater tendency to commit the crime'.

Using biological and psychological explanations, Wilson and Herrnstein (1985) identify and outline a number of variables that play a significant role in criminality. Two of these variables include time discounting and equity. Wilson and Herrnstein note that behaviour is controlled by a number of factors, for example, that poorly socialised children and those individuals with low-level intelligence are more likely to become criminals. They make a distinction between crimes carried out by individuals with low level intelligence, such as property crimes and sexual crimes, as opposed to individuals with a higher level of intelligence who commit crimes which require greater organisation, planning, preparation and at times negotiation (Wilson and Herrnstein 1985). This assumes that individuals with low-level intelligence are less likely to carry out white-collar crimes. Although few studies have correlated level of intelligence to different forms of crime, it assumes that most white-collar crime involves a higher degree of planning.
Some individuals consider that they are less likely to be caught than conventional offenders and consequently there is a ‘dark figure’ of white-collar crime. Traditionally, punishment of white-collar offenders appeared to be less likely than street or conventional offenders (see Sutherland 1983). Sutherland demonstrated this through the use of statistical data about white-collar offenders and the lack of evidence in a number of cases, which resulted in lower conviction levels than conventional crime. According to Wilson and Herrnstein (1985:50):

The increase in criminality resulting from the decreased probability of punishment occurs as a result of two processes – one involving instrumental conditioning, and the other, classical conditioning. If the threat of being punished oneself is reduced, the rewards for noncrime (i.e. the punishment that is not received) are weakened making non crime seem less profitable ...

Williams (1994:407) points out that Wilson and Herrnstein’s search for causes of criminality ignores ‘... all social economic, structural and materialistic ideas and concentrates solely on the individual and the behavioural conditioning which is most strongly connected with the family’. Wilson and Herrnstein’s theory is limited in its application to white-collar crime and white-collar offenders.

Psychological approaches to crime are distinguished from sociological theories in a number of ways. Psychological theories have developed quite distinct approaches to explain why particular individuals may be more predisposed to commit crimes (see Wilson and Herrnstein 1985). According to Krambia-Kapardis (2001:29), ‘... psychologists are interested in explaining individual differences. In this way, they supplement the sociologists’ focus on social and cultural factors as determinants of criminal behaviour’. Sociological theories encompass a diverse range of explanations for criminal behaviour and in general can be distinguished through strain, social control, routine activity theory, and opportunity. The next section outlines a number of these theories in contrast to Wilson and Herrnstein’s constitutional learning theory.

3.5 DIFFERENTIAL ASSOCIATION THEORY

Historically, theories that concentrated on the lower classes primarily committing conventional crimes were unable to explain crimes committed by the upper classes and those with a relatively high level of power and status. Furthermore, traditional theories
almost exclusively focused on male juveniles rather than adult offenders. This focus within criminology led Edwin H. Sutherland to pursue an alternative understanding of criminal behaviour to account for crimes committed by those in the upper classes and adult offenders. Sutherland developed a theory he termed ‘differential association’.

In developing his theory of differential association, Sutherland dismissed psychological and biological explanations of crime, the traditional criminological paradigm of criminal behaviour. In Sutherland’s (1983:258) view:

The current tendency is to advocate emotional instability as the psychological characteristic which explains ordinary criminal behaviour, and this explanation has been presented particularly by psychiatrists and psychoanalysts. Even these advocates, however, would suggest only in a jocular sense that the crimes of the Ford Motor Company are due to the Oedipus complex, or those of the Aluminium Company of America to an inferiority complex, or those of U.S. Steel to frustration and aggression, or Du Ponts to traumatic experience, or those of Montgomery Ward to regression to infancy.

In the early criminological milieu, criminals of relatively high social status and power were not a significant concern, as studies focused on conventional crime (Weisburd et al. 2001). Research emphasised poverty and social and personal pathologies attributed to poverty as the basic cause of crime and criminal behaviour (Shaw and McKay 1931; Sutherland 1983). It would appear that such criminals as the wealthy or powerful fell outside this paradigm. This position may have further developed Sutherland’s long-standing notion that white-collar crimes are not linked to poverty or the social and cultural variables that connect to poverty, as many offenders did not fit the ‘poor and powerless’ paradigm (Sutherland 1949). Similarly, corporate executives and politicians did not appear to be associated with committing conventional crime (see Weisburd et al. 2001).

In part, Sutherland’s theory was influenced by the ecological and social disorganisation approach of the Chicago school (Taylor et al. 1973) as he drew upon the social disorganisation of society to explain differing rates of crime in sub-groups (Pfohl 1985). In addition, Sutherland drew upon the concept of culture conflict (see Vold 1958) and
symbolic interactionism in order to explain criminal behaviour.\(^\text{29}\) By adopting these broad approaches, Sutherland's goal was to develop a theory of criminal behaviour that could account for all forms of conventional and white-collar crime through individual and group offending.

*Principles of Criminology* in its various editions (Sutherland 1939, 1947, 1974) provided a foundation for Sutherland to publish his theory of criminal behaviour. Differential association theory was devised as a set of nine principles to further explicate criminal behaviour through a process of learning:

1) Criminal behaviour is learned.

2) Criminal behaviour is learned in interaction with other persons in a process of communication.

3) The principal part of the learning of criminal behaviour occurs within intimate personal groups.

4) When criminal behaviour is learned, the learning includes (a) techniques of committing the crime, which are sometimes very complicated, sometimes very simple; (b) the specific direction of motives, drives, rationalisations, and attitudes.

5) The specific direction of motives and drives is learned from definitions of the legal codes as favourable or unfavourable.

6) A person becomes delinquent because of an excess of definitions favourable to violation of law over definitions unfavourable to violation of law.

7) Differential association may vary in frequency, duration, priority, and intensity.

8) The process of learning criminal behaviour by association with criminal and anti-criminal patterns involves all of the mechanisms that are involved in any other learning.

9) While criminal behaviour is an expression of general needs and values, it is not explained by those general needs and values, since noncriminal behaviour is an expression of the same needs and values (Sutherland and Cressey 1974:75-6).

\(^{29}\) The method of culture conflict may be '... explained through varying crime rates while the process by which individuals became criminal was expressed by the symbolic interactionism approach' (Atthi 1999:1).
Differential association theory focuses on how individuals perpetrate crime through a process of learning (in most cases through peer group learning). Learning in association with others is not isolated to the corporate milieu, but rather exists in any environment where an individual whose friend or associate has criminogenic attitudes may therefore be more predisposed to criminal deviance. It is important to note that mere association with individuals who display favourable attitudes to crime may not necessarily lead an individual to commit deviant acts.

If an individual is exposed to criminal behaviour more frequently, however, Sutherland believed there is a greater chance of adopting attitudes favourable to violation of the law (Sutherland and Cressey 1974). Similarly, if an individual sees the benefit of committing crime, it may be easier to carry out the crime.\(^3\) Sutherland points out that the desire for achieving goals may not necessarily be different for non-offenders although the means to attain them is (Williams 1991, 1997). The strength of Sutherland’s theory lies in its applicability to offending by both juveniles and adults.

The inherent connection between definitions favourable to crime and differential group association, proposed by Sutherland, has been an enduring issue and is well supported (see Cressey 1953; Matsueda 1982; Tittle et al. 1986; Waring 1993; Alarid et al. 2000). A number of scholarly contributions have since empirically tested Sutherland’s theory to different forms of criminality. For example, Tittle et al. (1986) carried out a study and tested Sutherland’s theory against six offences: tax cheating, illegal gambling, assault, $5 and $50 theft, and marijuana smoking. Their study showed that association is an influence on crime mainly through its effect on criminal motivation. It is important to note that despite general acceptance for Sutherland’s theory, Tittle et al. demonstrated that differential association is limited in its explanation of all six offences of the aforementioned and is therefore limited as a general theory of criminal behaviour.

Krambia-Kapardis (2001) applied differential association to different examples of fraud management and found it applied to the professional career conman where the intent to target a company is evident. In relation to the professional career conman, the study showed that:
CHAPTER 3: THEORIES OF CRIMINAL BEHAVIOUR AND THEIR RELATIONSHIP TO THE STUDY OF WHITE-COLLAR CRIME

Such an offender would often get him/herself into a position of trust within the company (sometimes by forging qualifications and work references or would set up a company to prey on other company by exploiting the trust he/she manages to establish) or vis-a-vis the company. In their association with other criminals, such offenders can acquire skills and techniques useful in committing fraud, such as how to produce forgeries of various documents and how to otherwise deceive financial institutions (Krambia-Kapardis 2001:37).

Krambia-Kapardis (2001:37) argued that associations formed between offenders influence the attainment of skills and techniques used to carry out some forms of white-collar crime. Krambia-Kapardis also found that differential association is applicable when concentrating on the significance of the corporate culture.

Hochstetler et al. (2002) examined the validity of Sutherland's theory by applying it to group and solo offending in the United States. Their study involved analysing data from the National Youth Survey based on the participation of 1492 youths and explored the influence of delinquent friends' behaviours and attitudes in general, and offending for crimes such as vandalism, theft, and assault. Hochstetler et al.'s (2002:561) study categorised three variables: respondent attitude towards deviance, perception of friends' attitudes towards deviance, and perception of friends' offending behaviours. In general, their study provided support for differential association theory; however, they concluded that the study eliminated the influence of group association as an element of differential association. This is in contrast to Sutherland's theory, where learned behaviour within a group environment plays a primary role in influencing criminal behaviour among individuals.

While it has been pointed out that differential association can apply to different forms of crime, Sutherland's theory has been refuted in a number of ways. From a critical perspective, the following points broadly identify the problems his theory encounters:

- Differential association does not take into account crimes that can be committed by a single individual (such as a forgery or embezzlement) not directly linked with criminogenic associations (see Cressy 1953; Friedrichs 2001).

---

30 This supports the positivist notion of hedonism where individuals may feel that the pleasure gained from committing the crime outweighs the pain of the punishment.
CHAPTER 3: THEORIES OF CRIMINAL BEHAVIOUR AND THEIR RELATIONSHIP TO THE STUDY OF WHITE-COLLAR CRIME

- It is difficult to observe whether the individual became involved in criminal offending as a result of learned behaviour in association with others or previously held favourable criminal values without group influence.

- It does not account for some individuals who hold attitudes that are favourable to law (see Friedrichs 2001). It cannot account for how the individual became involved in criminal offending other than through the interaction of a group dynamic.

- Sutherland’s ability to explain the inception of criminality is challenged because the criminal offending of individuals may have begun prior to involvement within a group environment (see Williams 1991).

- Sykes and Merton (1978:270-271) argue that significant issues such as ‘... why cultural definitions favourable to the violation of law exist in the first place ... [and] why some persons are more exposed than others to patterns of criminal behaviour’ are absent in differential association theory.

- It does not explain criminal behaviour that occurs as a result of individual motivation, such as an employee seeking revenge after his or her sacking or crime committed through opportunity, as outlined in the Ponzi scheme.31

- It is difficult to assess or measure the validity of the proposition that all forms of crime and criminal behaviour can vary in intensity, priority, and duration.

The criticisms levelled at Sutherland’s work point to the difficulty of trying to develop a singular universal theory to account for all forms of crime and criminal behaviour (Gorecki 1974; Coleman 1985; Williams 1991, 1997; Krambia-Kapardis 2001; Vande Walle 2002). According to Williams (1997:289), Sutherland’s theory can be contested because:

31 The Ponzi scheme is defined by the United States Securities and Exchange Commission (SEC) ‘... as a type of illegal pyramid scheme named for Charles Ponzi, who duped thousands of New England residents into investing in a postage stamp speculation scheme back in the 1920s. Ponzi thought he could take advantage of differences between United States and foreign currencies used to buy and sell international mail coupons ... Decades later, the Ponzi scheme continues to work on the ‘rob-Peter-to-pay-Paul’ principle, as money from new investors is used to pay off earlier investors until the whole scheme collapses’ (SEC 2001:1).
... It does not explain the criminality of those who have never been subjected to criminals or to people who would hold criminal ideas. Such people could not have learnt criminality by inter-personal contact: if it was learnt at all, it would probably have been from the media, which Sutherland relegates to a relatively unimportant position in the learning process [and];

It ... cannot explain irrational, impulsive, opportunist or passionate criminals, who would then be acting due to one of those factors rather than as a result of anything they have learnt.

Cressey’s (1953) study showed some support for the applicability of differential association among embezzlers. According to Cressey (1978:96):

The idea that criminality is a consequence of an excess of intimate associations with criminal behaviour patterns is valuable because, for example, it negates assertions that deviation from norms is simply a product of being emotionally insecure or living in a broken home, and then indicates in a general way why only some emotionally insecure persons and only some persons from broken homes commit crimes (cited in Sutherland and Cressey 1978:96).

This is a valid point. However, it dismisses the notion that criminal behaviour can occur or be influenced without an excess of intimate associations. Gorecki (1974) makes the point that Cressey (1978) omits certain elements when testing the applicability of Sutherland’s theory. Therefore, in Gorecki’s view, it is difficult to support in its entirety. Gorecki (1974:464) notes that ‘the hypothesis is, however, not precise enough to be tested: there is no way of measuring whether anybody’s contacts with criminal patterns are ‘sufficiently’ greater than his contacts with anti-criminal patterns’.

Sutherland spent a great deal of the latter part of his career formulating, revising, and defending his theory. The assessment of Sutherland’s theory has demonstrated that it is by no means universally applicable to all forms of crime and criminal behaviour despite proposing it to be so. It does, however, attempt to explain organisational deviance and certain forms of criminal behaviour identified with particular white-collar crimes, regardless of age and social status.

The strengths and weaknesses of Sutherland’s theory have been widely debated; however, broader theoretical perspectives have also emerged to explain criminal behaviour among white-collar offenders. The following section draws upon psychological and sociological explanations of criminal behaviour which have evolved
over the past century from the traditional contributions of classical and positivist criminology.

3.6 STRAIN THEORY

The American sociologist, Robert K. Merton, developed strain theory in the late 1930s. Merton, one of the influential theorists of the twentieth century, was influenced by the work of French sociologist and philosopher, Emile Durkheim ([1863] 1964), who viewed crime as having a functional role. Durkheim introduced the concept of anomie in his book, *The Division of Labour in Society*, in 1893. Anomie theory attracted a great deal of criminological attention and debate during the 1950s and 1960s and has continued to attract contemporary scholarly interest through a number of varieties of strain theory (Merton 1938; Cloward & Ohlin 1960; Agnew 1992).

Merton expanded on the tradition of social structure and anomie scholarship set out earlier by Durkheim in the late nineteenth century. In 1938, Merton published his theory of anomie, entitled *Social Structure and Anomie*. According to Merton (1968:186), his objective was to determine ‘... how social structures exert a definite pressure upon certain persons in the society to engage in non-conforming rather than conforming conduct’. Merton’s primary focus in devising his theory was not on crime or the behaviour of individuals but the rate of occurrence of individual deviant behaviour, that is, its structural features in contemporary society.

Merton (1938:672) was particularly interested in the role that social and cultural structures play in the aetiology of crime. Merton identified the first structure as culturally assigned goals and aspirations, which includes interests such as material possessions and the measure of success and monetary wealth. According to Merton (1938), cultural goals are legitimate and for all members of society; however, different values are placed on them within the social structure. The second part of the cultural structure in the words of Merton (1968:187) ‘... defines, regulates and controls the acceptable modes of reaching out for these goals’.

Merton’s typology is based on five modes of adaptation: conformity, ritualism, innovation, retreatism, and rebellion. Vold (1979:216) notes that these modes ‘... describe an individual’s choice of behaviours in response to the strain of anomie’.
Briefly, these variables set out by Merton either accept or reject cultural goals and institutionalised means as shown in Table 3.1.

<table>
<thead>
<tr>
<th>Modes of Adaptation</th>
<th>Cultural Goals</th>
<th>Institutionalised Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Conformity</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>II. Innovation</td>
<td>+</td>
<td>–</td>
</tr>
<tr>
<td>III. Ritualism</td>
<td>–</td>
<td>+</td>
</tr>
<tr>
<td>IV. Retreatism</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>V. Rebellion</td>
<td>±</td>
<td>±</td>
</tr>
</tbody>
</table>

+ Signifies acceptance
– Signifies ‘rejection’
± Signifies rejection of the prevailing values and substitute for alternative values.


Merton observed that adaptation to strain exists when individuals conform, provided the structure of society is stable. Out of the five adaptations, conformity accepts both forms of cultural goals and institutionalised means and is considered to be the most dominant of all forms. Merton (1968) applied his theory of deviant behaviour to individual and group offending.

In particular, Merton’s interest lay with the process that occurs when an individual’s behaviour is strained and norms conflict with the reality of social processes. According to Mannheim (1965:502):

Like Durkheim, Merton bases his analysis on the dangers inherent in any sort of discrepancy between human needs and the means available to satisfy them, but while Durkheim’s discussion remains somewhat abstract, almost independent of time and place and remote from the realities of life, Merton uses a wealth of observations drawn from the contemporary American scene to demonstrate in a far more concrete way the consequences of a conflict between “cultural goals and institutional norms” and to work out a typology of different responses to this conflict.
CHAPTER 3: THEORIES OF CRIMINAL BEHAVIOUR AND THEIR RELATIONSHIP TO THE STUDY OF WHITE-COLLAR CRIME

The central proposition of strain theory is that crime and deviance is a product of the pressures that individuals face in order to fulfil the ‘American dream’. A ‘strain’ emerges between the goals set by society and the means to achieve them. Merton foresaw that crime was largely concentrated in the lower classes due to the restriction of access to fulfil their dreams and desires and the pressures individuals face in society if they use legitimate means to achieve this. According to Merton (1957), individuals commit crime in order to conform to the rest of society’s dreams of wealth, however, as he further points out, not every individual will conform to this pressure through illegitimate means.

Significant to Merton’s theory was the individual aspiration to achieve power, prestige, and wealth. To secure these goals, illegitimate means are sometimes used by those denied access to such means. Merton (1957:260) points out that ‘central to this process of disciplining people to maintain their unfulfilled aspirations are the cultural prototypes of success, the living documents testifying that the American dream can be realised if one but has the requisite abilities’. Merton viewed delinquency as a product of an individual’s inability to achieve goals through legitimate means. Merton (1957) maintained that the continued need of individuals to build wealth and status produces crime because of the lack of social structures to support it. However, in this sense, little regard in Merton’s theory is paid to whether pressures, other than materialistic or societal expectations, motivate the individual to commit crime.

In the 1950s, Albert Cohen applied Merton’s theory to delinquency of subcultures. Cohen (1955) recognised that much delinquency occurred through subcultures rather than as individual offenders. To Cohen, subcultures within society have a different set of values, and belief systems from the predominant culture in society. In addition, subcultures have a different language and way of thinking. Cohen was interested as to why subcultures exist and how they influenced the behaviour of juveniles. Cohen found that most deviant behaviour occurred because of the empowering position within the group and the status of members. Although Cohen acknowledged that most delinquents

---

32 Albert Cohen (1955:13) argues that subcultures ‘... are the boys’ gangs that flourish most conspicuously in the “delinquency neighbourhoods” of our larger American cities. The members of these gangs grow up, some to become law-abiding citizens and others to graduate to more professional and adult forms of criminality, but the delinquent tradition is kept alive by the age-groups that succeed them.'
were from the lower classes, this was not the central concern for Cohen. Cohen (1955:26) argued that ‘... a humane and compassionate regard for their economic disabilities should not blind us to the fact that stealing is not merely an alternative means to the acquisition of objects otherwise difficult of attainment’. Cohen (1955) noted that there were many goods that delinquents stole for the sake of it, rather than for their purpose or economic value.

Hagan and McCarthy (1992) conducted a study of street life and delinquency in the late 1980s. Their sample was selected from school youth (563 students aged 13-19 years) and street youth (386 youths aged 13-19 years) from Toronto, Canada. Their study correlated a number of variables, such as gender, age, class conditions (parental employment), family structure, parental control and conflict, school involvement, life on the street and involvement in criminal activity such as serious theft to explain delinquency. Hagan and McCarthy’s (1992) study estimated the probabilities of delinquency through three frequency levels – low, medium, and high risk within the street and school samples.

Although each study was conducted separately and in different periods, at each level, the street youth were at a greater risk of delinquency. For example, the study showed ‘... the probability of low risk youth being involved in 20 or more serious thefts is .204 on the street and .005 in school; at medium levels of risk the comparison is .283 and 0.10 ...’ (Hagan and McCarthy 1992:553). The results did illustrate that the probability of being involved in 10 or more serious thefts for low risk youth was 0.363 for the street sample and 0.156 for school students.

Hagan and McCarthy’s (1992:555) findings showed that:

... youth from surplus population families are in part more likely to be on the street because of difficulties and disruptions in parenting. Youth from intact families are much less likely to take to the street and the effect of family disruption is transmitted through reduced levels of control and increased levels of coercion.

Hagan and McCarthy’s study revealed that strain plays an important role in delinquency. Their study did not examine whether opportunity also plays a role and the significance of other motivations for serious theft such as survival or entertainment as opposed to lack of family structure and conflict with teachers. If, as Merton (1957)
argues, crime is concentrated in the lower classes, his theory assumes that middle and upper class individuals fall outside this framework.

Shover et al. (2004) conducted research based on interviews with 47 fraudulent telemarketers who predominantly derive from middle class backgrounds. Their study confirms that the participants interviewed aspired to and considered themselves to be living the ‘American dream’, as one participant explained:

You’re always pursuing more money, most of us are. We’re raised that way, we are in this country. And that’s the way I was raised. But I also wanted to do my own thing. I wanted to be in business for myself, I wanted the freedom that came with that (cited in Shover et al. 2004:65).

Despite many of the participants’ middle class backgrounds, many of the individuals interviewed were irritated with their legitimate ambitions. According to Shover et al. (2004:66), ‘they were mindful of the possibility of growing economic marginality if they did not find and settle upon a satisfactory means of livelihood’. Shover et al. found that these individuals used justifications to account for their criminal behaviour and that their behaviour was stimulated by the opportunities available to them.

Despite the opportunities and access that these individuals had, Shover et al.’s study found that ‘... their perceptions of viable alternatives were limited by their desire to avoid the disadvantages, effort, and encumbrances of legitimate occupational pursuits’. The study also revealed that the participants nevertheless engaged in illegal conduct in furtherance of financial gain to pursue and maintain the ‘American dream’. According to Braithwaite (1991:42), ‘white-collar crime highlights the fact that legitimate opportunities are grasped not only to satisfy need but also to gratify greed’. Shover et al.’s study provides support that crime is not only concentrated in the lower classes buy applying it to a group of fraudulent telemarketers.

Although it may be argued that the material needs of the upper classes are relatively satisfied, it does not mean that they will not carry out white-collar crimes. In Braithwaite’s (1991:44) view:

---

33 Shover et al. (2004:65) study notes that some family members of the perpetrators held managerial positions and were business owners.

34 At least one quarter of the telemarketers that Shover et al. (2004) interviewed had previous convictions.
... just as the poverty of the poor in unequal societies contributes to crime, so does the wealth of the wealthy. We have established that the latter cannot be true because of a purely Mertonian analysis of legitimate opportunities to satisfy needs because the rich have more of their needs satisfied by ready access to legitimate means of need satisfaction.

This is supported by Duffield and Grabosky (2001:2) who argue that, ‘even those of above-average affluence may feel economically deprived in comparison to what they perceive to be their relevant standard. At times, ‘keeping up with Jones’s” may require other than lawful conduct’.

One of the most recent and largest cases of insider trading in Australia involved a former bank executive director, an individual whose wage would be considered above that of most average wage earning Australians. Hannes, a former Macquarie Bank executive director, constructed an alias, ‘Mark Booth’, to purchase shares of which he had insider knowledge involving a corporate takeover. After the takeover was announced, shares in the corporation increased so that Hannes’ investment profited by $2 million. According to David Knott, former chairman of ASIC, ‘... it was important that Mr Hannes stand convicted of these offences. He was a person in a position of trust who cynically embarked on a calculated plan to profit from insider trading’ (ASIC 2002:1). After investigations, Simon Hannes was convicted of insider trading and sentenced to two and a half years jail (ASIC 2002:1).

Sydney stockbroker, Rene Rivkin, was found guilty of one count of insider trading through his purchase of 50,000 Qantas shares. According to the ASIC, ‘the charge followed an investigation by ASIC into the circumstances surrounding trading in Qantas shares shortly before Qantas announced that it would take over the operations of Impulse Airlines’ (ASIC 2003:1). Rivkin’s access to wealth and status was not absent prior to this transaction. Rivkin was often reported in the media and photographed on his yacht and at his mansion.35

Merton’s theory has a number of valid points. However, it can be argued that people from the middle and upper classes also aspire to greater levels of wealth in order to live or maintain the ‘American dream’ (see Messner and Rosenfeld 2000). Merton’s theory can apply to forms of street crime and white-collar crime as illustrated above, it should
not be restricted to crimes concentrated in the lower classes. Among the criticisms of strain theory, Shover et al. (2004:71) note that it ‘... has also been accused of being inadequate as an explanation of rule violations by affluent members of the society who enjoy positions of privilege and have ready access to legitimate means of goal achievement’. This is consistent with the examples of Hannes and Rivkin.

Merton’s is a class-based theory, which attempts to use different variables of adaptation for predominantly the lower classes in society. It provides little explanation for individuals in the middle to upper classes who commit crime (see Mannheim 1965).\(^{36}\) The lack of empirical evidence of strain theory’s applicability to different forms of white-collar crime makes it difficult to assess its strengths. In addition, strain theory does not explain the rate of criminal behaviour as most of the crimes carried out are negligible and at times considered impulsive. One alternative to strain theory is the theory of neutralisation, proposed by Sykes and Matza (1957) some two decades later.

3.7 TECHNIQUES OF NEUTRALISATION

In the late 1950s, Gresham Sykes and David Matza developed a theory of how social control produced deviance and the importance of social reaction in the process of becoming deviant. Their theory attempts to explain criminal behaviour through the concept of techniques of neutralisation. Sykes and Matza (1957) assert that delinquents use justifications to protect themselves from self-blame prior to committing crime and thereby insulate the individual from guilt after the crime is committed (Cromwell and Thurman 2003). As Sykes and Matza (1957:666-7) maintain:

Disapproval flowing from internalised norms and conforming others in the social environment is neutralised, turned back, or deflected in advance [and thereby] ... the individual is freed to engage in delinquency without serious damage to his self image.

Believing that these techniques are credible allows the delinquent to excuse their behaviour. Sykes and Matza’s (1957) perspective on social control explains why certain individuals drift into (conformity) and drift out (non-conformity) of delinquency.

\(^{35}\) Rene Rivkin was found dead at his Sydney home on May 1 2005 after a battle with depression.
Neutralisations are two mechanisms that pave the way for crime, as they enable individuals to protect themselves against the moral constraints of society.  

Sykes and Matza’s (1957:667-9) five techniques of neutralisation include:

- **The Denial of Responsibility** limits the ‘personal accountability’ by pursuing social forces as the primary cause, for example, a crime-ridden neighbourhood or neglectful parents. Williams (1997:364) applies this to white-collar offenders and argues that ‘such offenders frequently claim that they were forced to act by their superiors; or acted only out of a sense of responsibility to some larger entity; or that it was the fault of subordinates who had been negligent’.

- **The Denial of Injury** occurs when the individual feels that nobody has been hurt by the deviant act/s by neutralising or by ‘playing down’ their actions as harmless. This may include defrauding a wealthy individual and justifying the actions because they can afford it. Similarly, stealing from a corporation can also be justified because they are a large company and can afford it and also the argument that other individuals do it.

- **The Denial of the Victim** occurs when the individual acknowledges the actions and accepts responsibility, but justifies the response taken in view of the circumstances and actions taken in the first place. An example is an individual illegally entering a company’s computer system to illustrate the lax security system by exposing individuals’ credit card numbers.

- **The Condemnation of the Condemners** is used to justify the delinquent’s actions by shifting the focus to ‘... those who disapprove of his violations’ (Sykes and Matza 1957:668). An example is the police officer who the individual feels is corrupt, or the individual who feels parents are picking on him or her. In relation

---

36 Merton later acknowledged this, however, with the example of robber barons in the nineteenth century, where illegal practices were used to obtain economic goals (see Friedrichs 1996).

37 Sykes and Matza’s (1957) theoretical paradigm is based on the following observations:
1. Delinquents express guilt over their illegal acts.
2. Delinquents frequently respect and admire honest, law-abiding individuals.
3. A line is drawn between those whom they can victimise and those they cannot.
4. Delinquents are not immune to the demands of conformity.
to white-collar crime, the offender may claim that other individuals in the company have also defrauded the company and therefore he/she should not be condemned by his or her actions (Williams 1997).

- *The Appeal to Higher Loyalties* is used to provide the rationalisation for the deviant act. This can be carried out to assist friends or for political causes. In other words, the crime in question is necessary in order to prevent a necessary evil. For example, Williams (1997:364) argues that ‘the approval of the group or gang (or the corporation) may be said to be more important than those of the family or of society’.

The theory proposed by Sykes and Matza connects to Sutherland’s theory where techniques of neutralisation may be learned through association. Sykes and Matza’s techniques of neutralisation theory have been empirically evaluated with a substantial body of research focusing on juvenile delinquency and conventional crime (Hirschi 1969; Minor 1981; Box 1983; Thurman 1984; Mitchell et al. 1990; Costello 2000; Cromwell and Thurman 2003). Variations of Sykes and Matza’s techniques of neutralisation have also been used in quite disparate contexts (Hindelang 1970; Minor 1981; Agnew 1994; Pershing 2003).

Despite the overwhelming contributions (of Sykes and Matza’s theory) applied to juvenile delinquency and conventional crime, techniques of neutralisation have also been applied to white-collar crime and adult offenders (Cressey 1953; Rothman and Gandossy 1982; Benson 1985; Jesilow et al. 1992; Strutton et al. 1994; Pershing 2003; Shover et al. 2004). Cressey’s (1953) study examined criminal violations of embezzlement perpetrated by individuals in a position of trust. The study explored rationalisations used and circumstances in which rationalisations were applied to explaining different forms of white-collar criminality in his study of embezzlers.

In relation to individuals in trusted positions, Cressey’s (1953:94) research showed that in some cases the motivation to rationalise behaviour occurred prior to carrying out the criminal act rather than after the event. According to Cressey (1953:95), ‘the essential point is that the person must perceive his position of trust as offering an opportunity for such violation, and that such perception, which involves the use of rationalisation, is a part of a process ...’. These processes involve a myriad of circumstances and behaviours.
that encompass the sources of rationalisations, such as cultural ideologies, language, and experiences (Cressey 1953).

One example that demonstrates a denial of responsibility involved a convicted criminal in a position of trust. The convicted criminal claimed:

I don’t know if I can tell you anything about this charge that I’m in for this time, but I’ve been stealing all my life so maybe I can tell you something about that. I’m in here for breaking a trust or something. I don’t understand it to this day. I know all about stealing, but I don’t know anything about this because I was working for a good man that was known to everyone, and he did lots of things for me (cited in Cressey 1953:87).

In this example, Cressey (1953:87) notes that the criminal assumed that he was not entirely accountable because criminality (and knowledge of it) appeared to be ‘in’ him thus rationalising his behaviour. Cressey’s study of embezzlers provided valuable insights into the role trust violation plays and the circumstances in which rationalisations are used to explain criminal behaviour.

Strutton et al. (1994) conducted a study of unethical business actions in a retail environment and applied techniques of neutralisation to determine how offenders justify illegal behaviour. The study involved approximately 2500 people who responded to a mail survey. The study found that techniques of neutralisation play a primary role in unethical business practices and was used as an acceptable means to justify their unethical behaviour. According to Strutton et al. (1994:257), condemning-the-condemners, denial-of-victim, denial-of-injury, and denial-of-responsibility wielded the most influence on the differences between unethical situations.

In relation to condemning-the-condemners and denial-of-victim, Strutton et al. (1994:258) make the point that:

... the acceptance of either signifies that the consumer perceives the retailing “victim” has previously engaged in some form of misbehaviour that stimulates and excuses the misbehaviour. Those who accept the neutralisation techniques may believe that the retailer deserves the mistreatment. Consequently, they do not view the retailer as a “victim” of the shoplifting behaviour.

Duffield and Grabosky (2001:3) applied Sykes and Matza’s techniques to different forms of fraud and found that variations of techniques are used. For instance:
Frauds against large companies or government departments are often rationalised with the excuse "they can afford it". Other examples of neutralisation include viewing the victim as culpable in some respect or, alternatively, trivialising the offence so that it becomes a "victimless crime" or so that there is no significant harm done.

Shover et al.'s (2004) study of fraudulent telemarketers (as discussed in the section 3.6) also found support that individuals apply techniques of neutralisation to rationalise their behaviour and guard against self-blame for their illegal actions. Accordingly, they note:

Central to the "vocabulary of motive" (Mills 1940) fraudulent telemarketers used to legitimate their deviant occupational activities and defend their personal identities was the "justification" (Lyman and Scott 1970) that their customers deserved to be victimised (cited in Shover et al. 2004:70).

Denial of the victim was the most common justification used by the fraudulent telemarketers, as they believed that they were not exploiting innocent victims (Shover et al. 2004:79). This rationale is supported by a comment from one of the individuals interviewed:

If these people can’t read, so be it. Screw them, you know. It [doesn’t say] everybody’s gonna get the diamond and sapphire tennis bracelet. They’re dumb enough not to read, dumb enough to send me the money, I really don’t care, you know. I’m doing what I have to do to stay out of jail (Shover et al. 2004:70).

In general, the studies explored above lend support to Sykes and Matza’s theory that individuals employ techniques to rationalise their actions in relation to different forms of white-collar criminality.

3.8 ROUTINE ACTIVITY THEORY

In the late 1970s, Lawrence Cohen and Marcus Felson (1979) proposed a new approach known as Routine Activity theory. It is sociologically and ecologically based, as it concentrates on analysing how the environment or routines in the everyday life of an individual can explain trends in crime rates. Their theory essentially departs from focusing on the ‘offender’ to concentrate on the opportunities that exist to commit crime within various structures. Routine activity theory has also been linked with elements of rational choice theory with its focus on the characteristics of the act rather than the actor (see Clarke and Felson 1993) and situational crime prevention (Clarke 1997) with a focus on theoretical integration.
Cohen and Felson (1979:593) defined routine activities ‘... as any recurrent and prevalent activities which provide for basic population and individual needs, whatever their biological or cultural origins’. Routine activity eliminates examining the history of the offender in order to characterise criminal behaviour (see Osgood et al. 1996). Furthermore, routine activity theory shifts attention from biological and psychological explanations as well as from the social and ecological approach of the Chicago school to explain criminality.

Cohen and Felson’s theory incorporates three elements that act as influencing factors for a crime to be carried out. For the successful completion of a crime, Cohen and Felson (1979:590) assert that all three factors need to be present:

- A likely and motivated offender;
- A suitable target available;
- The absence of capable guardians to prevent the crime from occurring.

Cohen and Felson’s theory has been the focus of empirical analysis over the past decade with a range of studies applied predominantly in the area of criminal victimisation (Massey et al. 1989; Anderson and Bennett 1996; Osgood et al. 1996; Rountree and Land 1996; Forde and Kennedy 1997; Bernburg and Thorlindsson 2001; Tewksbury and Mustaine 2003). For example, empirical studies have applied routine activity theory to property crime victimisation (Massey et al. 1989), fear of crime (Rountree and Land 1996), and crime victimisation surveys (Kennedy and Baron 1993), while others have explored various elements within routine activity theory. For example, Bernburg and Thorlindsson’s (2001) research examined the role of opportunity in deviant behaviour and Tewksbury and Mustaine (2003) explored the concept of guardianship within college students’ lifestyles.

Osgood et al. (1996) expanded on Cohen and Felson’s theory by building on the concept of situational motivation. Osgood et al. (1996:651) argued ‘... that situations conducive to deviance are especially prevalent in unstructured socialising activities with peers that occur in the absence of authority figures’. Their emphasis is on offending by individuals, a departure from the traditional emphasis on victimisation data.
Osgood et al.'s study tests the applicability of their theory to routine activities and individual offending. In general, their study found that in keeping with one of the central elements of routine activity theory, routine activities of everyday life are dependent on structural variables (Osgood et al. 1996:650). In addition, Osgood et al. (1996:651) found ‘... consistent evidence that socialising with peers away from home and authority figures is closely related to deviant behaviour, but only in the absence of a structuring agenda such as going on a date or participating in sport’. Routine activity in an unstructured environment can therefore play a large role in the motivation for a crime. Empirical studies of routine activity have demonstrated its merit for analysing different forms of conventional and white-collar crime and criminal behaviour.

3.9 GENERAL THEORY OF CRIME

No theory has received more attention since its inception than the general theory of crime, developed by Gottfredson and Hirschi (1990) (see Akers 1991; Benson & Moore 1992; Grasmick et al. 1993; Reed and Yeager 1996; Pratt and Cullen 2000; Vazsonyi et al. 2001; Stylianou 2002; Turner & Piquero 2002; Romero et al. 2003; Spahr and Alison 2004; Smith 2004). Hirschi, a prominent control theorist in contemporary criminology, presented his first version of control theory in *Causes of Delinquency* in 1969.

Hirschi’s (1969) research focused on the role of social bonds rather than on the characteristics of an individual’s personality in understanding the cause of criminal behaviour. Hirschi (1969) proposed that an individual’s bond to society prevents the violation of social rules. However, if the bond weakens, an individual is more likely to commit crime. According to Lilly et al. (2002:93):

... social bond theory rejected the attempt to explain crime through internalised control. Instead, taking a distinctly sociological approach, Hirschi (1969) emphasised that control is sustained by individuals’ continuing relationship with the conventional order – by their bonds to family, work, school, everyday activities, and beliefs.

In a distinct shift from the earlier research by Hirschi (1969), Gottfredson and Hirschi viewed low self-control as the primary mechanism that appeared to be indicative of the illegal decisions an individual makes, rather than the societal control placed on an individual as the cause of criminality (Vold et al. 2002:189).
CHAPTER 3: THEORIES OF CRIMINAL BEHAVIOUR AND THEIR RELATIONSHIP TO THE STUDY OF WHITE-COLLAR CRIME

Gottfredson and Hirschi’s general theory has been empirically assessed over the past decade with a number of different variables showing both support and criticism (see Akers 1991; Barlow 1991). In particular, low self-control has been applied to studies involving white-collar offenders (Benson and Moore 1992), drink driving (Keane et al. 1993; Piquero and Tibbetts 1996), binge drinking (Piquero et al. 2002; Gibson et al. 2004), organisational offending (Reed and Yeager 1996, Simpson and Piquero 2002), and adult criminal behaviours (Arneklev et al. 1993; Grasmick et al. 1993; Burton et al. 1999; Longshore 1998; Wright et al. 1999). The connection between Sutherland’s differential association theory and Gottfredson and Hirschi’s theory lies in a contemporary phenomenon within criminology, to articulate one theory to explain a complete range of criminal behaviours.

If Gottfredson and Hirschi suggest that self-control derives from childhood, the case of individuals in powerful positions such as executives and highly educated individuals, who appear to display a relatively high level of self-control, challenges this assumption (see Spahr and Alison 2004). Furthermore, Gottfredson and Hirschi’s theory is at odds with theories of drift proposed by Matza (1964), and Sampson and Laub’s (1990) life-course theory, which argues that criminality is linked to cultural expectations.

Burton et al. (1999) assessed the validity of self-control in accounting for crime for three specific age groups: ranging from 18-30, 31-50 and 51 and above. Burton et al.’s study involved self-report surveys in which questionnaires were sent to randomly selected individuals. The study found support that individuals with a lower level of self-control were more likely to engage in criminal behaviour.

Gottfredson and Hirschi’s (1989:360) theory extends the doctrines of classical criminology as they define crime as ‘... acts of force or fraud undertaken in pursuit of immediate self-interest that they provide uncomplicated pleasure or relief from pain, and are undertaken without concern for their long-term often painful consequences’. Their theory proposes that an individual is likely to be motivated to continue to commit crime and deviance throughout life if the individual commits crime as an adolescent. This is questionable in relation to particular forms of white-collar crimes, where traditionally white-collar offenders (typified by high social status and power) have seldom committed prior offences. The example of Hannes and Rivkin may challenge this hypothesis in relation to different forms of white-collar crime. Conversely, Shover et
al.’s (2004) study of fraudulent telemarketers found that at least one quarter surveyed had prior convictions. The theory is also problematic in explaining delinquency, as most did not re-offend.

A study carried out by Spahr and Alison (2004:100) challenges assumptions of low self-control made by Gottfredson and Hirschi’s general theory of crime through an observation of the ‘... frequencies of fraud among Employees and Directors/Officers’. Using a data set by Pontell et al. (1994), Spahr and Alison’s examination of 481 offenders of fraud showed that fraud was greater among Directors/Officers than Employees. This finding contradicts Gottfredson and Hirschi’s proposition that low self-control is found in individuals who have poor social involvement and are unable to maintain a responsible level of employment (Spahr and Alison 2004). If this is the case, the findings may have indicated that fraud would be predominately found among employees.

Gottfredson and Hirschi’s theory also contends that an individual’s predisposition to offend is connected with offending outcomes. They argue that ‘a valid theory of crime must see it as is: largely petty, typically not completed and usually of little lasting or substantial benefit to the offender’ (Gottfredson and Hirschi 1990:21). Given this view, earnings for fraud would be relatively low. Despite broad distinctions between outcomes, Spahr and Alison’s (2004:100) study revealed substantial benefits from fraud. For example, the dataset showed that the minimum amount was [US]$7,160 and the maximum was [US]$ 2,500,000,000. The mean for the sample was [US]$ 48,000,000. In addition, Morselli and Tremblay’s (2004:773) study on criminal earnings of incarcerated offenders for predatory crimes revealed that the lower an individual’s level of self-control, the higher the criminal earnings. Although this result is not analogous to white-collar offences, it shows that low self-control may impact upon the effectiveness of networking and criminal earnings.

Gottfredson and Hirschi’s correlation between age and crime can also be contested in a number of ways. They observe, for example, that involvement in crime reduces with advancement in age. This does not explain white-collar offenders who have no prior criminal offence and commit crime during the latter stages of their professional career such as Hannes and Rivkin. In addition, Gottfredson and Hirschi maintain that the
relationship between crime and age is consistent across different societies and social classes regardless of the type of crime (Greenberg 1985).

This proposition by Gottfredson and Hirschi does not apply to all forms of crime and criminal offenders. For example, Spahr and Alison’s (2004) examination of fraud among Employees and Directors/Officers contradicts Gottfredson and Hirschi’s age variable by showing that most of the offenders were much older than their claim that offenders committing crime peak in their early twenties. Spahr and Alison cite the work of Steffensmeier and Allan (1995) to provide further support that contradicts Gottfredson and Hirschi’s proposition. Spahr and Alison (2004:102) observe that:

Steffensmeier and Allan (1995) discovered that lucrative crimes “highest percentage” offenders were in their 40s. They believe that this reflects a realistic trend, because the peak of such crimes often occurs during career peaks around the same age. This may reflect greater opportunities and relevant skill acquisition to facilitate fraud.

Although Gottfredson and Hirschi’s theory has most recently gained prominence, many studies point to the lack of strength in endeavouring to apply a general theory to account for all forms of crime (see Akers 1991; Benson and Moore 1992; Coleman 1992; Reed and Yeager 1996; Spahr and Alison 2004). Akers (1991:203), for example, asserts that Gottfredson and Hirschi ‘... offer no general or specific empirical test of the theory they offer’ in order to validate it. Similarly, Coleman (1992:60) argues that, ‘Hirschi and Gottfredson see the classical theory as a foundation for a general theory ... yet ironically, they fell into the same trap as Sutherland by claiming their theory as a universally valid explanation of all crime’.


... its rejection of motives as important causal forces is misguided. Because motives are generated by macro social and organisational processes, a fully developed theory of white-collar crime must take these processes into account.

Reed and Yeager (1996) argue that the lack of attention paid to the connection between normative culture and corporate offending demonstrates its limitations as a theory, which can apply to all forms of crime. More specifically, Reed and Yeager (1996) point out that corporate offending is far more diverse and widespread than their explanation
allows, where Gottfredson and Hirschi focus more specifically on conventional crime such as fraud or forgery. Fraud is the most common form of white-collar crime for which statistics are routinely collected and it is therefore more easily identifiable.

In general, Gottfredson and Hirschi’s theory fails to address specific explanations for white-collar crime, as Reed and Yeager (1996) most notably pointed out. Further refinements to Gottfredson and Hirschi’s theory may give it wider acceptance. However, to encapsulate all forms of crime, particularly white-collar crime, in a general theory is a seemingly impossible task, given the diverse array of contexts in which crimes are committed and that the focus on situational factors should be taken into account. One of the challenges identified is that existing studies fail to address whether patterns have changed over time. Similarly, these studies are based on historical patterns which have traditionally failed to recognise white-collar crime as part of criminal statistics.

3.10 SUMMARY

This chapter has demonstrated that a number of early criminological theories have contributed to the development of contemporary understandings of criminal behaviour although they are limited to some extent as they have attempted to construct criminal behaviour for only the working class and for conventional forms of crime.

In this analysis, theories of crime and criminal behaviour, such as differential association, strain, techniques of neutralisation, and routine activity have in general demonstrated their applicability to white-collar crime. However, Sutherland, and Gottfredson and Hirschi’s general learning theory lacks the ability to explain both street crime and white-collar crime through the same principles of behaviour. It is also important to recognise that many of the theories discussed above were initially developed to explain juvenile offending, not adult and white-collar offending. Moreover, despite recent attention paid to explaining white-collar criminality, this chapter underscores criminology’s continued pre-occupation with conventional crime and juvenile offending (see Lynch et al. 2004).

Chapter Five tests the assumption that existing theories of criminal behaviour as discussed above would apply and therefore be testable in the area of cyber crime.
Studies into crime and criminal behaviour relating to cyberspace have been few and far between. The challenge that emerges is whether these theories are applicable to cyber crime and if so, to what extent. Prior to undertaking this analysis, the following chapter introduces this new category of crime - computer and cyber crime.
CHAPTER 4: THE NEXT GENERATION – COMPUTER AND CYBER CRIME

The convergence of communications and computing has begun to transform the world. Although this transformation has mainly been located in Western industrial societies, its effects are beginning to be felt globally (Grabosky et al. 2001:1).

4.1 INTRODUCTION

Chapter Three demonstrated first that theories initially developed to explain juvenile offending and conventional crime have some applicability to adult offenders and white-collar crime. Second, general theories of crime do not adequately explain criminal behaviour for all forms of white-collar crime and criminality. Third, more narrowly focused theories do illustrate a number of consistencies that explain criminal behaviour for different forms of white-collar crime.

This chapter extends a body of criminological scholarship that combines conventional forms of crime and white-collar crime. It complements Chapter Two by introducing a more recent contribution to crime and criminology – computer and cyber crime.38 The aim of this chapter is to examine the nature of computer and cyber crime,39 and what is distinctive about it.

This chapter is structured into four main sections. First, section 4.2 defines the term ‘computer crime’ and explores its early origins, and defines the term ‘cyber crime’. Second, section 4.3 outlines the origin of the Internet, from the early stages of military installation to commercialisation and public accessibility in the early 1990s. Third, section 4.4 examines the nature of computer crime and analyses a number of theoretical focal periods – from its inception in the mid-1950s, the criminalisation of computer crime, and the changing perception of hackers.40 Fourth, section 4.5 examines the emergence of cyber crime and discusses three criminogenic attributes of the Internet.

38 The terms ‘computer crime’ and ‘cyber crime’ are often used interchangeably in scholarly research (see Katyal 2001).
39 The transnational nature of cyber crime refers to crimes committed across the globe through the use of a computer. It is important to note that these crimes do not have to be committed in one particular location, and crime can therefore be considered non-local.
40 The framework for this analysis is drawn from Crime, Deviance and the Computer (Hollinger 1997).
Lastly, section 4.6 explores different forms of cyber crime, from traditional forms perpetrated through sophisticated methods (for example, fraud, stalking, terrorism), as well as new forms of crime, which have emerged through technological advances of the computer (for example, hacking, viruses, Distributed Denial of Service (DDoS) attacks, worms, and Trojan horses).

4.2 DEFINING COMPUTER CRIME

The discovery of computer abuse in the 1950s laid the foundations for a new category of crime and deviance within the discipline of criminology. Although it has existed in different forms, computer crime has been around for as long as the development of computers, an example of which is noted by the United Nations (1999:6):

... A textile manufacturer in France [Joseph Jacquard], ... design[ed] the forerunner for the computer card. This device allowed the repetition of a series of steps in the weaving of special fabrics. So concerned were Jacquard’s employees with the threat to their traditional employment and livelihood that acts of sabotage were committed to discourage Mr. Jacquard from further use of the new technology. A computer crime had been committed.

A definition of computer crime was first evident around the mid to late-twentieth century. Parker (1976) initially termed computer crime as computer abuse, which referred to ‘... any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain’. Parker’s (1988) definition of computer crime encompassed different forms of crime, such as fraud, larceny, and sabotage.

Early forms of computer abuse had been identified (Howard 1997) although it was difficult to distinguish between forms of computer misuse through negligence or accidental means. Furthermore, criminal law had not recognised computer crime as a distinctive form of crime prior to the 1970s and therefore the term ‘computer abuse’ was widely acknowledged (see Parker 1976).

As different forms of computer crime broadened, the nature and meaning of it also changed. Parker’s (1976:17-21) definition can be used to illustrate four ways in which crime can be committed with computers:

1) … the computer can be the object of the attack. The computer can be easily damaged and valuable programs and data within the computer
system can be destroyed [e.g. vandalism, malicious mischief, or sabotage].

2) ... creating a unique environment in which unauthorised activities can occur, or where the computer creates unique forms of assets subject to abusive acts [e.g. creating viruses, fraud].

3) ... the computer as the instrument of the act [e.g. computer used to forge documents to plan a white-collar crime such as embezzlement].

4) The computer can be used symbolically to intimidate, deceive, or defraud victims [e.g. false advertising, online securities fraud, telemarketing fraud].

Ahead of its time, Parker’s (1976) definition provided a strong paradigm for understanding early forms of computer crime as well as contemporary forms of cyber crime. Further modifications to the definition provided by Parker also highlight significant areas where a computer plays a role in the commission of crime. For example, Bequai (1978:4) suggests that:

An adequate definition of computer crime should encompass the use of a computer to perpetrate acts of deceit, concealment, and guile that have as their objective the obtaining of property, money, services, and political and business advantages. Computer crime may also take the form of threats or force directed against the computer itself. These crimes are usually “sabotage” or “ransom” cases.

A number of definitions of computer crime currently exist. This has meant that there is no singular internationally accepted definition. This is consistent with a report by the United Nations (UN) (1999:6) which notes that ‘a global definition of computer crime has not been achieved; rather, functional definitions have been the norm’. The challenge that this poses is the lack of global uniformity and standardisation as to what constitutes computer crime. Parker (1976:3) explains that part of the reason for this is that ‘computer abuse is a multi-faceted problem [where] it looks quite different from different points of view’. The various laws that different countries have enacted for different computer crimes also mirror this view (an issue that will be discussed in subsection 4.4.2). Whilst computer crime was recognised around the mid-twentieth century,

---

41 Parker’s (1976) definitional framework has been applied as the basis for defining different forms of cyber crime. However, in order to provide a contemporary understanding of its applicability to cyber crime, two areas require further consideration: first, the inclusion of digital evidence (see also Grabosky and Smith 1998; Casey 2000); and second, the inclusion of crime committed across the globe through networks.
the development and convergence of computer networks such as the Internet appear to have compounded criminal opportunities and behaviour.

4.2.1 Defining Cyber Crime

There are a number of ways in which cyber crime can be defined and distinguished from computer crime. This is because the computer is used in a number of different ways to commit crime. Many forms of cyber crime are an extension of traditional forms of crime that can be committed in the physical\textsuperscript{42} and virtual world\textsuperscript{43}. These crimes include fraud, extortion, espionage, sabotage, piracy, stalking, hate crimes, child pornography, money laundering, misuse of personal information, and terrorism. New crimes have also developed out of the advancement of computing technologies and include unauthorised access to computer systems and networks, hacking, worms, viruses, denial of service (DoS) attacks, and the use of Trojan horses.

A definition encompassing the complexities of cyber crime is important to distinguish between earlier forms of computer crime and current forms of cyber crime. Thomas and Loader (2000:2) argue that the prefix cyber is problematic because ‘... after all, [there is] nothing very new in the adoption by criminals of new technologies’. They provide examples of technological instruments used for crime, such as the telephone and more recently the mobile phone, which have been used to intercept communications or invade transmission. Thomas and Loader’s point is an important one because this form of crime is not new, rather an extension of previous technologies committed in new and diverse ways. However, the increase in technological sophistication and rapid take-up of the Internet has meant that methods to facilitate crime have altered to adapt to the extension of global networks, as well as leading to the emergence of new crimes that are specific to computing technologies.

There are interchangeable terms used to refer to cyber crime. These often occur in empirical research and literature in the following ways – ‘Internet crime’, ‘e-crime’, ‘computer crime’, ‘computer abuse’, ‘electronic crime’, ‘high-tech crime’, ‘net crime’,

\textsuperscript{42} Collin (2000:1) describes the physical world as ‘... matter and energy – light, dark, hot and cold, all physical matter – that place in which we live and function’.

\textsuperscript{43} Collin (2000:1) describes the virtual world as ‘... symbolic – true, false, binary, metaphoric representations of information – that place in which computer programs function and data moves’.

Page 90
‘information technology crime’, and ‘digital crime’. The multi-dimensional way of conceptualising cyber crime has its roots embedded in the study of white-collar crime.

Drawing on the work of Grabosky (2000b:4-8), computer-related crime, which includes cyber crime, can be identified through the following nine categories:

1) *Theft of telecommunication services* historically includes phone phreakers and hackers.

2) *Communication in furtherance of criminal conspiracies* can include crimes such as organised drug trafficking, fraud, and espionage.

3) *Information piracy and forgery* includes copyright infringement, piracy, and the reproduction of documents such as a driver’s licence to commit crimes such as identity fraud.

4) *The dissemination of offensive material* includes child pornography, hate speech and information pertaining to illicit activities such as terrorist threats. Given the global nature of computer-related crime, it is important to point out that what is illegal in one country may be acceptable in another (Grabosky 2000a).

5) *Stalking* can be in the form of harassment, threatening communication through telephone, e-mail, and chat rooms. This type of crime can also evolve from the virtual world to the physical world and vice versa.

6) *Extortion* can be carried out in a diverse range of ways. Most commonly it is through hacking to launch Denial of Service (DoS) attacks and for financial gain.

7) *Electronic money laundering and tax evasion* can be facilitated through the transfer of funds electronically, most often through concealment. Sophistication of technology has allowed greater access and speed to process funds on a scale that was once limited.

8) *Electronic vandalism and terrorism* can range from releasing viruses and worms to disabling websites, computer networks, and technological infrastructures.

9) *Fraud* can include credit card fraud, auction fraud, identity fraud, online securities fraud, phishing, and healthcare fraud.

---

44 Meyer (1988) points out that ‘… “phreaking” … came into general practice after the adventures of John Draper, aka Capt Crunch, were publicised in a 1971 Esquire magazine article. Phreaking is a way to circumvent the billing mechanisms of the telephone company. It allows one to call anywhere in the world, quite literally without cost. In many cases it also prevents, or at least inhibits, the possibility of calls being traced to their source thereby helping the deviant to avoid being caught’.

45 See for example, IPSOS (2002).
Katyal (2001:12) refers to cyber crime as ‘... the use of a computer to facilitate or carry out a criminal offence’. Katyal (2001:12) outlines three ways in which this can occur: ‘First, a computer can be electronically attacked [which can be further divided into] 1) unauthorised access to computer files and programs [for example a break-in to Defence Department Computers], 2) unauthorised disruption of those files and programs [for example the ‘I Love You’ virus], and 3) theft of an electronic identity’ [these examples above are typical of a situation where] a computer is the subject of an attack’.

4.3 THE ORIGIN OF THE INTERNET

The history of computers is marked by a number of distinct periods. One of the most notable periods is the development of computer networks. The early 1960s marked the prototype of a computer network, which formed the basis for the creation of the Internet. The United States Department of Defence (DOD) opened up a department known as the Advanced Research Projects Agency (ARPA) to pursue a commitment to information technologies. ARPA commissioned a project for a packet-switched computer network (Kleinrock 1961) as a response to the Soviet Union’s launch of Sputnik 1 in 1957 (see Hardy 1996; Winston 1998; Jensen 2001).

According to Jensen (2001:38):

If the explosion of the Russian atom bomb in 1949 could be seen as the genesis of the “reds under the bed” panic of the McCarthy era, then the flight of Sputnik in October 1957 was one of the major factors underlying America’s decision to create a strategic defensive system.

---

46 ‘On October 24, 1995, the FNC [Federal Networking Council] unanimously passed a resolution defining the term Internet ... The Federal Networking Council (FNC) agrees that the following language reflects our definition of the term “Internet”, “Internet” refers to the global information system that – (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.’ (Leiner et al. 2000)


48 Leonard Kleinrock published the first paper on packet-switching theory. This theory developed the creation of the Internet.

49 ARPANET combines the concept of the Internet as a network of networks hence the addition of ‘net’ to the abbreviated term.

50 Sputnik 1 was the first satellite to be launched into Earth’s Orbit in 1957 by the Soviet Union.
The predominant function of the computer network was to facilitate communication between the United States military and the Defence Department in the event of a nuclear attack. The computers (large mainframe size) within the network were controlled by the United States Government and predominantly used for military and defence purposes (Hollinger 1997).

Whilst a number of networks operated within the central framework where information travelled through to the military, the government also saw a need to develop the network for the growth of the computer science research community (Hardy 1996). ARPA extended the computer network and thus emerged the National Science Foundation Network (NSFNET) to allow scientists, American universities and government agencies to communicate and transfer information on an open network. Hardy (1996:6) notes that ‘ARPA’s computer science subcontractors ... formed the privileged group of the network’s first users’. This group predominantly used the network for sharing of data; however, it was not long after that individuals began to use the networks to transfer communication electronically for personal purposes (Hardy 1996; Zackon 1996). 51

The extension of participants to the computer network created the beginning of personal information flowing in the form of electronic mail (e-mail), which changed the nature of computer-mediated communications (CMC), by essentially commercialising its potential. A former scientist observed:

We in the ARPA community (and no doubt many others outside it) have come to realise that we have in our hands something very big, and possibly very important. It is now plain to all of us that message service over computer networks has enormous potential for changing the way communication is done in all sectors of our society: military, civilian, government, and private (Meyer and Dodds 1976:145 cited in Hardy 1996:24).

51 Scientists and researchers, who were part of the team which led the Internet’s commercial application, define the development of the computer network through four divergent processes: technological, operations and management, social, and commercial. First, ‘There is the technological evolution that began with early research on packet switching and the ARPANET (and related technologies), and where current research continues to expand the horizons of the infrastructure along several dimensions, such as scale, performance, and higher level functionality. There is the operations and management aspect of a global and complex operational infrastructure. There is the social aspect, which resulted in a broad community of Internauts working together to create and evolve the technology. And there is the commercialisation aspect, resulting in an extremely effective transition of research results into a broadly deployed and available information infrastructure’ (Leiner et al. 2000:1-2).
The potential commercial development of e-mail during the 1970s also elevated the opportunity for different forms of computer crime, such as the violation of privacy and security (Howard 1997). These offences occurred most commonly through e-mail but extended to information and data, which were considered sensitive. Importantly, the convergence of information technologies opened up opportunities for people to engage in criminal activities beyond previous forms of conventional crime. The opportunities for committing crime appeared to be made easier due to its open network and absence of guardianship.

In the early 1990s, the Internet surpassed initial expectations of resource and information distribution by expanding the computer network for commercial purposes, thus allowing access to the broader community. The Internet’s perceived potential has enabled access to local and global markets within a short space of time. This has meant that networks have sprung up all over the globe, merging communication via e-mail, chat rooms, peer-to-peer file sharing, and newsgroups through the Internet. Commercial transactions on the Internet, such as the sale and exchange of goods and services have also emerged and provided a global means for electronic commerce (e-commerce).

Today, the Internet constitutes an amalgam of interconnected networks where computer systems are linked to enable individuals, organisations, corporations, and government agencies a platform to communicate and exchange information in an open network. The Internet is used for a variety of purposes — education, research, commerce, communication, information, social interaction, entertainment, and criminal activity (Grabosky 2001b). The Internet’s largely unregulated network enables individuals to communicate and facilitate commercial transactions openly and anonymously.

Whilst it is important to acknowledge that cyberspace is a realm where legal transactions take place, a great number of illegal transactions also occur. The growth and take-up of the Internet appears to have contributed to the rise of cyber crime on a scale that was previously not physically achievable in such a short period of time. It was during the early stages of the development of computer networks, prior to the Internet, however, that different forms of computer crime emerged in the form of computer

52 Networks have also played a significant role in implementing and shaping virtual or wired communities on the Internet (see Rheingold 1993, 2000; Schuler 1996).
abuse. Despite its inception over half a century ago, only recent focus has brought to light the magnitude, diversity and impact of computer and cyber crimes. The next section will review the development and nature of computer crime over the past five decades.

4.4 THE NATURE OF COMPUTER CRIME – A REVIEW OF THE FOCAL PERIODS

The nature of computer crime and its subsequent development can be outlined through four focal periods: the Emergence of Computer Crime (1946-1976); the Criminalisation of Computer Crime (1977-87); the Changing Perception of Hackers (1988-92); and the Censorship Period (1993-present) (Hollinger 1997). The emergence of the Internet has generated greater opportunities to include an additional and quite significant period: the Emergence of Cyber Crime (1991-present). This review is important as it broadly demonstrates the historical development of computer crime and the historical convergence of crime and criminal behaviour through computers and later through cyberspace during the mid-to late twentieth century.

4.4.1 Computer Crime – a Fifty Year Journey

Each time an innovative technology, such as the electronic computer, has been introduced in society, usually both positive and negative consequences have resulted. While the beneficial contributions of the new technology are usually the first to be noticed, the less obvious, negative ramifications sometimes become apparent only much later (Hollinger 1997:xvii).

Hollinger’s (1997) remarks signify the subsequent challenges that have arisen from different forms of computer crime and its often hidden nature. It was previously argued that a definition of computer crime was not evident until the mid-twentieth century. The take-up of computers, which occurred at different times in different countries, meant that awareness of computer crime was not globally evident during these earlier periods. Moreover, the lack of a centralised reporting system meant that crime trends were difficult to discern. Whilst this has made it difficult to document the development,

---

53 It is important to note that the timing of these focal periods was initially based on American literature and empirical research; however, this chapter will incorporate data from a range of countries. The timing of these periods is, therefore, not universally applicable due to the development and take-up of computers, which vary from country to country (see Hollinger 1997).

Page 95
nature and trend of computer crime on a global scale, the following provides a brief overview of the development of computer crime over the past five decades.

1950s

In the 1950s, during the early period of computer networks, only few incidents of computer crime such as violation of privacy and security were recognised. Prior to this period, no accounts of computer crime were reported. According to Pergel (2002:1), "... the first criminal actions connected with computers happened before the end of the fifties (e.g. embezzlement in USA in 1959, committed with the help of punch cards). Howard (1997:43) notes that in the US, issues of computer security emerged when computers were used for classified information. This was also during the time when the military and defence were distributing information and data through computer networks. Secrecy was viewed as the predominant concern (see Howard 1997).

1960s

During the mid-1960s, the first documented case of computer crime in America was published in the *Minneapolis Tribune*, two decades after computers emerged. Upon further investigation of the report, *Computer Expert Accused of Fixing His Bank Balance*, Parker (1976:xi) published a paper on the incident as a warning to alert the broader computer community of the need to establish ethical standards for the use of computers. During this period, Parker (1976:12) also argued that computer crimes broadened to include fraud, theft, embezzlement, terrorism, larceny, extortion, malicious mischief, espionage, and sabotage.

There was scepticism surrounding the nature of computer abuse. The lack of evidence of computer crime and the questionable legitimacy of the original source of information contributed to the scepticism (Parker 1976). Parker argued that it was difficult to assess the validity of data relating to computer crimes due to the lack of reporting mechanisms and the number of undiscovered cases. This meant that reporting of criminal offences involving a computer was relatively infrequent. The lack of public awareness of computer crime also contributed to the low levels of reported computer incidents. Furthermore, the informal approach to reporting appeared to reflect the difficulty of assessing accurately the true nature and extent of computer abuse as well as the nature of offending. However, these concerns did not diminish and with additional networks
and the number of users increasing, crimes by computer also increased, broadening the nature of computer crime.

1970s

The 1970s highlighted the beginning of what emerged as empirical research on computer crime. McKnight’s publication, *Computer Crime*, in the early 1970s and Parker’s publication, *Crime by Computer*, in the mid-1970s, illustrated the development of computer crime as a potentially serious societal problem, by documenting its nature prior to the commercialisation of personal computers (see also Bequai 1978). Newspapers were the predominant source of unverified reports of computer abuse, followed by the publication *Computerworld*, and also questionnaires (Parker 1976:24). These cases required investigation to verify whether computer abuse had occurred. The different sources of information reporting cases of computer crime highlighted the difficulties in confirming the occurrence of computer crime.

During this period empirical studies uncovered the extent of computer crime. Sieber (1998:19-20) provides an account of three different types of computer crime: the American Equity Funding fraud, which involved manipulations of 56,000 insurance claims with a sales value of at least US$30 million, the German Herstatt case, which involved speculative foreign exchange transactions totalling several billion dollars, and the Swedish Volvo Manipulations case. In these cases, the computer played a vital role in the commission of a broad range of crimes, which were essentially seen as white-collar in nature. However, during this period, not all countries were aware of computer crime. McKnight (1973:18) recalls a conversation with Scotland Yard’s Deputy Assistant Commissioner Jim Crane, who stated, ‘... in this country so far, such crime has been virtually non-existent. McKnight also notes that in the United Kingdom, few cases of computer crime had been identified prior to 1973.

1980s and Beyond

The 1980s marked the beginning of the personal computer boom for millions of users worldwide. The commercialisation of computer networks began in the early 1990s. There emerged a community of computer aficionados, which developed beyond the early days of ARPANET. In the 1980s, cases of computer crime grew on a global scale, where new forms of computer crime, such as hacking and viruses were recognised and
later criminalised in particular countries (see Stoll 1989; Hafner and Markoff 1995; Adamski 1998; Rogers 2001a). During this period, one of the central features chronicling the rise of computer crime was the inception of computer laws and the emergence of cyber crime. This meant that crimes were not only being committed through the use of a computer but also through networks such as the Internet and the World Wide Web (WWW).  

The following provides a snapshot of reported incidents of computer crime in the United States of America (US), Japan, Hong Kong, and Portugal. The reporting and documenting of computer crime varies greatly in different countries. Table 4.1 illustrates the number of incidents of computer crime from the US reported to the Computer Emergency Response Team (CERT) from 1988 until 2003 (CERT 2005:3).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents</td>
<td>6</td>
<td>132</td>
<td>252</td>
<td>406</td>
<td>773</td>
<td>1,334</td>
<td>2,340</td>
<td>2,412</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Incidents</td>
<td>2,573</td>
<td>2,134</td>
<td>3,734</td>
<td>9,859</td>
<td>21,756</td>
<td>52,658</td>
<td>82,094</td>
<td>137,529</td>
</tr>
</tbody>
</table>

Source: CERT 2005

One of the significant observations that can be made from the data is the exponential growth in the number of reported incidents of computer crime in the US, particularly

---

54 The WWW provides users with access to information with software using hypertext.

55 The information on countries referred to in this section is based on information available at the time of research.

56 In the United Kingdom, for example, Hyde-Bales et al. (2004:1) note that ‘... currently [there is] no formal recording of crimes that involve computers and the Internet’. Research carried out by Hyde-Bales et al. (2004) found that the majority of police forces in England and Wales are not consistent in incident reporting and identifying computer crime. According to Hyde-Bales et al. (2004:4) ‘such variety of record creation provides both opportunities and weaknesses for an effective computer crime policy’. The research provides an impetus for future standardised recording processes of computer crime in the United Kingdom and Wales.
during the period 1999-2003. It is assumed that this increase coincides with the increased take-up and popularity of the Internet (see Adamski 1998).\textsuperscript{57} This assumption may also be based on the increased awareness and media attention of computer crime such as the ‘ILoveYou’ virus (which may have prompted Internet users to report crime).

The growth in computer crime may also be attributed to the opportunities made available through the global access to the Internet. For example, the Internet’s global capabilities and range of services and information have increased the availability of suitable targets (these issues will be further explored in Chapters Five and Seven). Second, the Internet’s channels of open communication may present opportunities to like-minded people through chat rooms for the purpose of discussing criminal activities (Williams 2001). Third, the absence of capable guardians to police the Internet on a global scale and the lack of security measures on various websites and personal computers may further entice people to carry out crime.

Not all forms of computer and cyber crime have come to the attention of enforcement authorities, which makes it difficult to trace the trend of computer and cyber crime in most countries. Sieber (1998:22) comments that in the past, few cases of computer crime in Japan were reported to police. This appears to be demonstrated by a trend that indicates a rise in the reporting of cyber crime. Broadhurst (2003:9) notes that the arrest rates for computer-related crime in 1997 was 262 (31.7 per cent), 415 (29.9 per cent) in 1998, and 1039 (92.2 per cent) in 2002. The global nature of some forms of crime such as hacking and the unleashing of viruses, may have contributed to public awareness, thus leading to an increase in rates of reporting. In addition, the enactment of new laws criminalising computer-related crime may also account for the rise of reporting (see Broadhurst 2003).

\textsuperscript{57} See Internet World Stats (2004) for an estimated number of Internet users from all countries.
Table 4.2 Computer Related Crimes Reported in Hong Kong 1995-2003

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking/ Cracking³</td>
<td>4</td>
<td>4</td>
<td>7</td>
<td>13</td>
<td>238</td>
<td>275</td>
<td>114</td>
<td>164</td>
<td>325</td>
</tr>
<tr>
<td>Criminal Damage</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>15</td>
<td>27</td>
<td>16</td>
<td>14</td>
</tr>
<tr>
<td>Online Deception</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>18</td>
<td>29</td>
<td>65</td>
<td>64</td>
<td>84</td>
</tr>
<tr>
<td>E-Theft &amp; Other</td>
<td>8</td>
<td>13</td>
<td>8</td>
<td>17</td>
<td>57</td>
<td>49</td>
<td>29</td>
<td>30</td>
<td>29</td>
</tr>
<tr>
<td>All</td>
<td>14</td>
<td>21</td>
<td>20</td>
<td>34</td>
<td>317</td>
<td>365</td>
<td>235</td>
<td>272</td>
<td>454</td>
</tr>
</tbody>
</table>

Source: Technology Crime Unit HKP in Broadhurst 2003:10

The data in Table 4.2 highlight the continued growth of reported cases of computer-related crimes in Hong Kong.

The first computer crime statistics in Portugal appear to have been collected from 1991. As Parker (1976) described earlier, each case had to be evaluated for verification because of the different ways in which computer crime data was collected. A report by the Department of the Judiciary Policy of Portugal noted that an estimated 70 computer crime cases were recorded between 1991 and 1993. Between 1994 and the end of the first semester of 1998, 378 cases of computer crime were reported (Sieber 1998:5). Whilst these statistics represent a rise in the reporting of computer crime, the report expressed concern as to whether these figures were an accurate representation of the true extent of computer crime in Portugal. Part of the concern is due to the significant rise of crime in 1995, which recorded 167 cases in a single year (Sieber 1998:6).

While these figures of computer crime in some countries brought to light the relatively small number of computer crime cases during the 1980s and early 1990s, more importantly they highlighted the potential ‘dark figure’ of computer crime. One explanation may be due to the hidden nature of computer crime and the lack of public awareness of its extent and impact, because computer crime was only criminalised in most countries in the late 1980s and early 1990s. The following sub-section examines the historical development of computer law through six waves, each wave evolving at different times in different countries due to the varying levels of development of computer crime.
4.4.2 The Criminalisation of Computer Crime

During the 1950s and 1960s, incidents of computer crime were emerging and later expanding in different forms (see McKnight 1973; Parker 1976). Since the first incident of computer crime, traditional forms of crime have adapted to technological changes and new forms of crime have also developed.\(^\text{58}\) The different forms and ways of committing crime appear to have forced a re-evaluation of existing laws as new computer laws were established. The changing nature of criminalising computer crime can be evaluated through six waves (Sieber 1998). We can identify six basic types of development of cyber criminal law: Protection of Privacy, Economic Crimes, Intellectual Property Protection, Illegal and Harmful Content, Criminal Procedural Law, and Protection Measures and Legal Regulatory Processes. These six types form the basis for legal evolution, which started in the 1970s and continues today.

One of the indicators that computer crime impacted beyond individuals to organisations, corporations, institutions, and government was the enactment of various laws to address the different forms of criminal behaviour. During the 1970s and 1980s, the criminalisation of computer crime emerged during a period when computers were predominantly used to transmit and store personal information. The storage of personal information on computers and networks provided opportunities for its violation.

This first wave ensured the implementation of laws relating to breaches of privacy and the role of personal privacy protection such as the introduction of privacy acts. For example, the United States of America introduced the Privacy Act in 1974 and the Electronic Communication Privacy Act in 1986. The United Kingdom introduced the Data Protection Act in 1984 and in that same year Australia implemented the Privacy Act. The European Union has played a significant role in monitoring privacy violation by introducing the Privacy Protection Directories in 1995 and again in 2002.\(^\text{59}\)

\(^{58}\) Traditional forms of crime are simply old crimes, while new crimes refer to crimes that have emerged from the advancement of information technologies. In this thesis ‘traditional crimes’ refer to old crimes such as fraud and pornography, which are simply carried out in new ways utilising new technologies. The distinction between these forms of crimes is that ‘traditional crimes’ are aided by technology to perform the same type of crime whereas new forms of crime have developed out of computing technologies.

\(^{59}\) In addition, the OECD (1988, 2003) has been instrumental in the progress and process of global cooperation with the development of online privacy protection. The OECD’s publication, Privacy Online: OECD Guidance on Policy and Practice (2003) reflects the OECD’s commitment to building networks and encouraging cooperation between its members for ensuring protection of privacy and personal data.
During the 1980s, two further waves of computer law were evident. A second wave, which developed in the beginning of the 1980s, predominantly addressed different forms of economic crime that involved a computer. The most common forms of computer crime during this wave were traditional in nature – fraud and sabotage. However, new forms of computer crime, such as computer intrusion, hacking, and unauthorised manipulation of computer data also emerged. During this period, cases of computer hacking also stimulated the enactment of additional laws and inspired greater transnational co-operation (see Stoll 1989).

The central identifiable feature of this period was the continued increase in incidence and diversity of computer crime since the 1980s, which emerged at different times in different countries. For example, hacking was recognised as a crime in the 1980s in the USA while in Japan hacking was criminalised in the 1990s. While computer crimes were increasing and expanding, not all countries during the 1980s enacted laws at the same time to criminalise the different forms of economic crime. For example, the Computer Fraud and Abuse Act was enacted in the United States of America in 1986; in Australia the *Crimes Act 1914 (Cth)* Part VIA was extended in 1989 to cover State and Territory offences, and in the United Kingdom, the Computer Misuse Act was enacted in 1990.

During the mid-1980s, a third wave of computer law developed in the form of the protection of intellectual property in digital form. At the time, protection of intellectual property needed to embrace the role of the computer and a revision of existing legislation was required to address this issue (see Urbas 2000). The United States enacted the Computer Software Copyright Act in 1980 and the Semiconductor Chip Protection Act in 1984. Reforms to the protection of information law were also introduced in a number of countries during the 1980s. Amendments to reform are still predominant today due to the changing role information technologies play in the digital world.

---

60 It is important to note that intellectual property crimes include violations, such as copyright, trademark, and the unauthorised use of communications.
It became evident early on that not all computer crimes were legally recognised in all countries. A recent example to illustrate this involved Onel De Guzman, the perpetrator of the malicious worm, ‘ILoveYou’. From the Philippines, Guzman installed the worm which infected and disabled millions of computers worldwide. At the time, the Philippines did not have an appropriate law criminalising the release of malicious code and so could not prosecute. This was rectified within six weeks by the Philippines legislature, but only after the damage had been done (see Urbas 2005a).

A fourth wave of computer law focused on communication offences, such as illegal and harmful content and racist messages and statements. Sieber (1998:88) notes that in relation to the Internet, ‘... two legal issues have to be distinguished: The first one concerns the criminal liability of the author or the content provider of the respected statement. The second one is about the additional liability of the service-provider whose networks and/or servers are abused by third parties’. A number of these offences are traditional in nature but the sophistication of technology has allowed these crimes to be perpetrated in new ways and at times given new meaning.

Disseminating content deemed to be illegal, such as child pornography and racist statements, has been made easier by the Internet. Sieber (1998) has also raised the point that if one country recognises pornographic and racist statements as criminal, another country may not have appropriate laws to prosecute perpetrators (see Smith et al. 2004).

The fifth wave, criminal procedural law, addressed issues of search and seizure of digital evidence. The sixth and final wave entailed protection measures and legal regulatory processes such as the introduction of security law and state access to evidence that may exist in encrypted form. This wave emerged during the 1990s and continues to play a fundamental role today due to the changing capabilities and sophisticated methods criminals use in furtherance of criminal opportunities. Furthermore, as computer and cyber crimes extend into new territories, issues of regulation have become increasingly salient, given the need to keep apace with the changing nature of computing technologies and the role computers play in the commission of crime. Sieber (1998:14) argues that:

---

61 The recent introduction of hacking as a criminal offence in Japan and the Philippines illustrates this.
The possibility of manipulations in data networks has led to additional questions as to what extent legal regulations on security measures are necessary. Three different questions must be distinguished: (a) duties to implement protection measures, (b) prohibitions of certain protection measures, and (c) consequences of possible manipulations for the use of electronic contracts.

It is informative to analyze the changing perception of hackers and explore four generations of hackers.

4.4.3 The Changing Perception of Hackers

Hacking and hackers may be viewed as among the most contentious and debated of all computer crimes and computer criminals (for example; see Turkle 1984; Denning 1990, 1999; Dreyfus 1997, 1998; Hollinger 1997; Taylor 1999). This is largely attributed to the perception of its changing nature from a professional role (computer programmer) in the mid-twentieth century to a criminal role in the late-twentieth century (see Sterling 1992; Chandler 1996; Rogers 2000, 2001a, 2001b). At its simplest, hacking may be defined as the unauthorized access into computer programs and/or files. Since the early studies of computer crime, empirical research has focused on hacking and the motivation and behavior of hackers to gain greater insight into this phenomenon (see Turkle 1984; Stoll 1989; Denning 1990; Dreyfus 1997; Jordan and Taylor 1998; Taylor 1999; Rogers 2000; Kleen 2001).

The early concept of hacking has been somewhat challenged by the contemporary view and understanding of the computer hacker (see Weizenbaum 1976). This has led to various definitions and conceptualizations of the term ‘hacker’, which has evolved over the past five decades. Sterling (1992:53) argues that ‘the term hacker has an unfortunate history’. Levy (1992) describes this history as one that:

... can signify the free-wheeling intellectual exploration of the highest and deepest potential of computer systems. Hacking can describe the determination to make access to computers and information as free and open as possible. Hacking can involve the heartfelt conviction that beauty can be found in computers, that the fine aesthetic in a perfect program can liberate the mind and spirit (cited in Sterling 1992:53).

In traditional terms, Taylor (1999:xii) describes a hacker as ‘... someone who explored the full range of capabilities of both himself and his computer equipment’. Today, however, the term ‘hacker’ refers to someone who intrudes upon another’s computer
system to further his or her own, possibly criminal ends (Taylor 1999:xii). The changing nature of hackers may be aptly described through four generations (Levy 1984).

(a) **Four Generations of Hackers**

The first generation of hackers were labelled ‘hackers’ by virtue of being computer programmers where their primary motivation was the intellectual challenge (Levy 1984). These programmers were from the Massachusetts Institute of Technology (MIT) and the Stanford Artificial Institute Center (SAIC) during the 1950s and 1960s where their predominant role was to develop computer programs (see Weizenbaum 1976; Turkle 1984; Levy 1984). This generation of hackers led the way for significant research of computer programming (Levy 1984; Sterling 1992).

The second generation of hackers (during the 1960s and 1970s) were considered computer revolutionaries. Hafner and Markoff (1995:11) maintain that during this period:

... To be a computer hacker was to wear a badge of honor. It singled one out as an intellectually restless soul compelled to stay awake for forty hours at a stretch in order to refine a program until it could be refined no more.

Turkle (1984:216) discusses the role of MIT computer programmers during this period and maintains that computer programmers ‘... are addicted to playing with the issue of control. And playing with it means constantly walking that narrow line between having it and losing it. Computer programming offers this kind of play, and it is part of the hacker culture’. According to Levy (1984), only minor amounts of crime occurred during this period.

During the 1980s, the third generation of computer hackers constituted a significant departure from the computer explorers of the mid-twentieth century to a new group commonly identified as computer intruders or ‘electronic burglars’ (Hafner and Markoff 1995:11). In fact, many original hackers of the 1960s and 1970s used the term ‘crackers’ for the new generation of computer
CHAPTER 4: THE NEXT GENERATION – COMPUTER AND CYBER CRIME

intruders.\textsuperscript{62} Turkle’s (1984:241) interview with systems programmers give strength to this view by noting that "... the systems programmers I interviewed expressed dismay that their vocation has been tainted with the image of ‘computer crime’ ‘It gives hacking a bad name’.

The term ‘cracker’ was applied to people who participated in computer crime and hackers wanted to distinguish themselves from crackers. Traditionally,

Hackers generally like to think of themselves as an elite group of information seekers who are adept at exploring computer systems and networks. Although hacking into network computer systems is illegal, hackers believe it is ethically acceptable as long as a hacker does not commit theft, vandalism or breach any confidentiality ... [However] those who break into computer systems with malicious intent are known in the hacking world as crackers (PBS 1998:1).

The distinction between hacking and cracking is not often made in the mass media. On one hand, hacking is viewed as a form of skill, however, on the other hand it is now recognised by law as a criminal activity. According to Steele et al. (1983):

The word “hacker” has taken on many different meanings ranging from “a person who enjoys learning the details of computer systems and how to stretch their capabilities” to “a malicious or inquisitive meddler who tries to discover information by poking around ... possibly by deceptive or illegal means ...” (cited in Denning 1990:13).

The fourth generation of computer hackers emerged in the 1990s and has excelled to greater heights of criminal behaviour with the commercialisation of the Internet. Hackers are commonly recognised today as cyber criminals or Internet hackers. Lightning (1988), a contributing editor for the online magazine ‘Phrack’ discusses the changing nature of hacking with a former hacker:

When Mr. Slippery started hacking seven years ago he as [sic] an exception among pimply faced, curious kids whose computers were toys for cheap, and typically harmless thrills. For four years, he lived up to his alias, eventually penetrating top security government

\textsuperscript{62} The term ‘cracker’ is used to describe actors unauthorised breaking into computer systems for a range of illegitimate purposes (see Meyer 1988).
After approximately four years of hacking, Mr. Slippery recalls ‘... that an entirely new crowd had sprung up ... you now have the 14-year-olds who were running destroying things seeing how much trouble they could cause’.

Opportunities for criminal activity became apparent in the 1950s. This signified the broadening of traditional ways of committing crime via a computer and hence paved the way for the commission of new forms of computer crime such as hacking and denial of service (DoS) attacks.

**(b) A Chronology of Hacking Incidents**

A Berkeley astronomer discovered one of the earliest cases of hacking in the mid-to-late 1980s. Stoll’s (1989) book, The Cuckoo’s Egg – Tracking a Spy through the Maze of Computer Espionage, detailed an investigation into what initially emerged as a US$.75 cent discrepancy in a computer accounting system. At the time, two accounting systems were operating simultaneously, which meant that each total would match. This was not the case, and the discrepancy lead to an investigation where Stoll believed an intruder was operating in the computer network. Stoll retained records of the hacker’s activities and designed a program that allowed him to track the hacker’s movements simultaneously. Stoll also created various documents which appeared to be confidential information to attract the hacker in order to trace him.

Stoll continued his investigation of tracking the hacker after his initial attempts to gain assistance from telecommunication companies and various law enforcement agencies failed. It was not until much later that federal enforcement agencies became involved and later arrested the perpetrator, Markus Hess (known as ‘the Hanover Hacker’). It was alleged that Hess illegally entered computer systems and downloaded unauthorised information and had been paid by the KGB for secret information on the United States military. Hess’ actions were recognised as computer espionage and the Hanover Hacker became the first of a number of published cases that were recognised as hacking offences.
Kevin Mitnick, one of America’s most recognised cyber criminals, caused in excess of US$290 million dollars damage by hacking into a wide range of high-tech companies. Mitnick’s history of computer crime began in the 1980s when he was caught stealing a number of computer manuals from a telephone company (Power 2000:57). Mitnick has committed a broad range of computer crimes such as breaking into several different computer systems, monitoring e-mails, stealing software, committing computer and wire fraud, and damaging computers (Power 2000:58). Mitnick has served time in prison for multiple computer-related offences.

In 1988, Robert Tappan Morris, a 23 year-old graduate student at Cornell University released the Internet’s first worm that infected a large proportion of UNIX computer systems connected to the Internet (Hafner and Markoff 1995). In 1995, under the pseudonym of the ‘Black Baron’, Christopher Pile, the author of a virus tool kit Smeg and viruses Queeg and Pathogen, was the first person to be prosecuted in the United Kingdom for writing and distributing computer viruses. These programs were publicly and freely available on the Internet and through bulletin boards (Jackson 1995). Pile was sentenced to 18 months in prison, an indication of how seriously the crime was regarded.

In 1996, in one of the largest acts of computer sabotage, a former network administrator, Timothy Allen Lloyd was accused of writing and planting a software ‘bomb’ that deleted software operating Omega Engineering Corporation’s production programs. According to Hochberg (1998:1):

The sabotage occurred on or about July 30, 1996. Lloyd had been terminated from Omega on July 10, after working for the company for approximately 11 years. The Indictment also reflects that the sabotage resulted in a loss to Omega of at least [US]$10 million in sales and contracts.

Lloyd was convicted in 2000.

In 1999, two Chinese citizens, Hao Jing-Long and Hao Jing-Wen, were prosecuted for hacking. It was alleged that Hao Jing-Long conspired with his brother, Hao Jing-Wen, to break into the computer network of the Zhejiang branch of the China Industrial and Commercial Bank in furtherance of stealing funds. It was further alleged that Hao Jing-Long, an employee of the bank,
entered the bank and secretly connected a modem to the bank’s computer, which allowed his brother access to the network. This access led to Hao Jing-Wen transferring a total of 720,000 yuan into 16 different accounts set up by the two brothers (Hong Kong Voice of Democracy 1998:1). The two brothers were found guilty of hacking and sentenced to death. This case represents one of the harshest punishments against a computer hacker (Hong Kong Voice of Democracy 1998:1)

Over the past decade, a broad range of new worms and viruses have developed and as a result disrupted millions of computers worldwide. The level of sophistication of viruses and worms has increased. Techniques are being used to deceive users into opening attachments, which in some cases releases a virus or worm unbeknownst to the user. The ‘Anna Kournikova’ worm was a malicious program that purported to attach a photo of female tennis player, Anna Kournikova. Jan de Wit from the Netherlands released the worm, which was designed so the user believed the e-mail was from someone familiar and therefore considered legitimate. Through this method, it violated a level of trust between individuals who assumed it was from a legitimate source. However, once the attachment was opened, a worm spread, searching for particular files and causing disruption to computer systems and networks. The worm generated a large volume of information and congested e-mail servers. De Wit was convicted in the Netherlands and sentenced to 150 hours of community service or 75 days in prison.

David Smith was the author of the ‘Melissa’ virus, which struck over one million computers worldwide towards the end of March 1999. The virus which targeted e-mails, contained an infected word document as an attachment. Pethia (1999:6) makes the point that:

The Melissa Virus represents a new level of sophistication in the progression of computer viruses. Melissa’s impact is so great because it exploits, in a very simple and clever way, the power that has been built into the flexible and expressive technologies in use on the Internet today.

The impact and effect of the ‘Melissa’ virus was global in that by this stage, millions of users were connected to the Internet. The way the virus was designed meant that few individuals were aware of the true nature and extent of
the damage it would cause such as internal documents leaking to outside individuals or organisations (see Pethia 1999) and an estimated damage of over US$80 million to computers worldwide (Cleary 1999:1). Smith was prosecuted and sentenced to 18 months in prison and fined US$5000.

The infamous ‘ILoveYou’ worm, which was released by a former Filipino computer student, Onel de Guzman, in 2000, threatened millions of global users on the Internet and spread in a diverse number of ways: most commonly through e-mail, Usenet\(^{63}\) groups and window sharing. The worm was one of the most destructive to date, causing millions of dollars in damage. Katyal (2001) notes the damage of the worm was approximately eight times that of the Melissa virus.

The ‘W32.Blaster’ worm struck Internet users worldwide in August 2003. The worm exploited universal vulnerabilities in Microsoft 2000 and Windows XP computer systems. The worm attempted to download the msblast.exe file to execute the application. In addition, it attempted to perform DoS (denial of service) on the windows server (Knowles et al. 2003). Knowles et al. (2003:1) point out that the worm had a high geographical distribution although the threat containment and removal of this worm appeared to be moderately successful. The author of the worm, 19-year-old Jeffrey Lee Parson aka ‘Teenkid’ was arrested and has since been jailed for 18 months and is required to serve 10 months community service.

The W32.Sasser.Worm struck approximately 18 million Internet users in the beginning of May 2004 by attempting to exploit the vulnerability of Microsoft Windows 2000 and Windows XP systems. The worm shut down computer systems as it installed itself on computer hard drives and then transferred to the Internet giving users 30 seconds to log off before automatically shutting down. The police allege that the author of the worm, teenager Sven Jaschan, ‘... downloaded some basic virus code from a hacker’s website and started adding

\(^{63}\) There are many different ways to define USENET groups. Salzenberg (1993) defines Usenet as ‘... a world-wide distributed discussion system. It consists of a set of “newsgroups” with names that are classified hierarchically by subject. “Articles” or “messages” are “posted” to these newsgroups by people
strings of further code to it. Once he’d finished, it was about 15 screens long (Macalister Hall 2004:61). The implications of the worm were extensive with wide-reaching effects. Macalister Hall notes that targets of the worm included some computer systems at Rail Corp in Australia, a number of German banks and post offices, the postal service in Taiwan, and hospitals and government offices in Hong Kong.

The examples above show the disruption and malicious damage inflicted on computer systems and networks due to hacking’s global nature. In addition, it shows that the reporting and statistical data collected to analyse incidents of hacking have also advanced. This will no doubt provide useful information for policy and lawmakers and aid in understanding criminal behaviour of hackers.

Denial of Service (DoS) attacks have also caused malicious damage to computer systems and financially impacted upon individuals, communities, companies, and organisations. Such examples have occurred on various American websites. For example, in early 2000, a 15-year-old Canadian youth known as ‘Mafia Boy’ launched DoS attacks on four prominent American websites — Yahoo!, E*Trade, Amazon.com, and eBay. In these attacks, computers were instructed to bombard the designated ultimate target with irrelevant information. The target computers soon ran out of memory and were unable to respond to customer enquiries. As a result, the target site was temporarily unavailable, causing loss of potential business.

It is interesting to note that some hackers still view themselves as ‘doing good’ despite the criminalisation of hacking. For example, in 1999, an American high school student cracked into three US Government agency websites and defaced them. According to the student, the attacks were performed to alert ‘authorities’ of the lack of security protection on ‘their’ website (Kahney 1999). The student’s justification was to ensure that the government agencies’ websites were secure. According to the student:

---
on computers with the appropriate software — these articles are then broadcast to other interconnected computer systems via a wide variety of networks'.

Page 111
A lot of other countries are planning cyberwarfare on the US government. If other countries have malicious intent, how can we as US citizens feel safe? I did this to let them know they really have to prepare for these things (Kahney 1999:1).

Despite the attempted justification by the school student, this is a recognised criminal offence in the United States.

Indeed, some organisations employ hackers who have disseminated viruses and worms because of their skills and expertise. This view is supported by Mitchell (2003) who states that ‘... a hacker has more of an insight into the minds and workings of another hacker. Personally I think it would be a great asset to a company to have a hacker as a security consultant, or even as an administrator for security’ (cited in Sturgeon 2003:1). This meets the old adage, ‘use a thief to catch a thief’.

In summary, the term ‘hacking’ has changed in definition from its early meaning of computer programming to the contemporary connotation of criminality. Moreover, the examples mentioned here illustrate the vexatious nature of hackers, particularly over the past decade. The transnational nature of the Internet has made a number of crimes such as hacking more of a threat because it can be carried out in diverse and circuitous ways. While hacking is a new type of computer crime, the next section will demonstrate that it also plays a significant role in cyberspace due to the additional crimes that can be carried out as a result of hacking.

4.5 THE EMERGENCE OF CYBER CRIME

Since McKnight’s (1973) account of the broad nature of computer crime and Parker’s (1976) study of computer crime in the 1960s, crime has proliferated exponentially as a result of the different forms and the numerous ways it can be carried out (see also Grubosky and Smith 1998; Grubosky et al. 2001; Katyal 2001). This sub-section addresses criminogenic attributes on the Internet that give rise to cyber crime.44

---

44 Newman and Clarke (2003:61) apply this term to an analysis of criminogenic attributes of the computing environment.
4.5.1 Criminogenic Attributes of the Internet

The Internet has paved the way for individuals, groups of individuals, and organised networks to commit a broad range of crimes that would not have otherwise been possible. As such, it is argued here that criminogenic attributes specific to committing crime on the Internet allow criminals unprecedented opportunities that may be distinguished from the physical world: anonymity, multiplicity, and target exploration.

(a) Anonymity

Anonymity on the Internet provides users a degree of privacy to communicate information to other individuals or groups of individuals through e-mail, chat rooms, and news groups without being recognised or without revealing the origin of communication. There are a number of advantages of anonymous communication on the Internet: the promotion of freedom of expression, encouraging dialogue between certain people and groups in society to discuss issues of a sensitive and personal nature, and providing a means of reporting criminal activity without fear of reprisal. However, the open means of communication using re-mailer services provides perpetrators a place to conceal their identity for the purposes of committing different forms of crime and trading information in secrecy (see Levine 1996; Saxena 1998; Goldberg 2000; Grabosky et al. 2001; Newman and Clarke 2003; Nasheri 2005).

The number of crimes that may be carried out under anonymous conditions include defamation, fraud, extortion, copyright infringement, cyber stalking, harassment, spamming, destruction of trade secrets, denial of service attacks, copyright software, misuse of personal information, and the dissemination of child pornography. Anonymity also provides the mechanism to violate trust.

65 Clarke (1999) used an acronym to a situational crime prevention approach to theft; Newman and Clarke (2003:61) applied Clarke’s approach to e-commerce using the acronym SCAREM: Stealth, Challenge, Anonymity, Reconnaissance, Escape, and Multiplicity, to describe the situations which may present themselves that either provoke or tempt individuals to commit particular types of cyber crime.

66 Finkelhor et al. (2000:21) note in a survey Online Victimization: a Report of the Nation’s Youth, that ‘...youth have reported other threatening and offensive behaviour directed to them on the Internet, including threats to assault or harm the youth, their friends, family, or property as well as efforts to embarrass or humiliate them. Once again, the concern of parents and other officials is that anonymity of the Internet may make it a fertile territory for such behaviours’.

67 The production and dissemination of spam mail is not recognised as a crime in all countries.
According to Friedman and Papathomas (2000:38), ‘... anonymity can erode a climate of trust by making assessments of potential harm and good will of others more difficult’. In relation to pornography, Friedman and Papathomas (2000:40) maintain that ‘because of the anonymity – particularly if the messages are encrypted and the user's identity concealed – the Internet provides a particularly good way to distribute illegal pornography’. This was evident in the W0nderland Club where members accessed private bulletin boards and newsgroups to send images of children to other members and communicated through these channels in secrecy, thus making detection difficult through anonymity.

Anonymous re-mailer services also appear to provide the impetus to conduct criminal activity. For instance, information can be distributed via these services without the operator of the service intervening in the search for illegal activities and therefore it lends itself to a broad range of crimes. For example, denial of service (DoS) attacks can be carried out by individuals who disguise their tracks, by hiding their IP addresses, thus making detection difficult. Denning and Baugh (1999:270) note that ‘President Clinton, for example, has received e-mail death threats that were routed through anonymous re-mailers’. If re-mailers had the power to investigate suspect communication, the level of criminal activity may be reduced because the level of guardianship increases. In an example of extortion via re-mailers, an extortionist threatened to fly a model plane into another plane during take-off at an international airport and released this information through e-mail via an anonymous re-mailer (Denning and Baugh 1999:270).

Electronic tools such as encryption along with storage and communication devices allow information to be deleted, manipulated, and re-routed to prevent the detection of a crime and tracing a criminal’s pattern (see Denning and Baugh 1999). These tools create greater opportunities for motivated offenders to manipulate victims and different types of crime while concealing the perpetrator’s identity. For example, a terrorist group used encryption to conceal messages while carrying out attacks on businesses and state officials. Initially authorities conducted a traffic analysis because they were unable to decrypt the messages during interception. Eventually investigators were able to break
through layers of encryption and passwords to gain access to messages (Denning and Baugh 1999:255).

In one case that involved encrypted e-mail, a 37-year-old man, Carlos Salgado, Jr. (aka SMAK) illegally accessed three online sites, including the University of California at San Francisco, and obtained in excess of 80,000 credit card records. According to Power (2000:92), Salgado ‘... launched his attacks from a compromised account of an innocent individual, he conducted on-line negotiations using encrypted e-mail, and he received initial payments via anonymous Western Union wire transfer’. Salgado was arrested after attempting to sell the credit card records in exchange for money although unbeknownst to him, he was communicating with members of the FBI.

The ability repeatedly to test out targets and methods of intrusion while evading identification by authorities makes the Internet an attractive medium (Newman and Clarke 2003). This tool opens up possibilities to a range of motivated offenders including individuals, groups, and organised networks through the use of cyber cafes and other more sophisticated ways of Internet routing (Williams 2001).

(b) Target Exploration

The vast amount of data stored on computer networks along with the growth of Internet use presents would be criminals with more prospective targets. For example, Newman and Clarke (2003:62-3) point out that ‘the Internet makes it possible to scan thousands of web servers and even millions of personal computers that are connected to the web, looking for ‘holes’ or gaps in security through which the criminal can enter and carry out any aspect of his crime ...’. Other methods include software that automatically scans personal details and websites based on techniques such as phishing and pharming to dupe victims. The Internet has provided a more efficient way to carry out a myriad of scams where both the potential victims and the methods used are numerous.

(c) Multiplicity

The dramatic growth of the Internet in the late twentieth-century enabled the connection of millions of people instantaneously. Whilst the Internet has
bridged communication afar, it has also connected criminals, elevated crimes to a global platform, and created opportunities for criminals to commit a multitude of new crimes. Prior to the Internet, most frauds involved single outcomes where financial gain was minimised to avoid detection. It was difficult to defraud additional targets in the physical world with one transaction. The Internet has changed the nature of crimes as it facilitates the means for people to apply their skills and knowledge to commit a multiplicity of crimes with one transaction, enhancing the probability of financial gain. FBI (1992:13) statistics show that ‘... the average armed bank robbery nets [US]$3,177. The Data Processing Association reports that the average computer crime loss to banks may be as high as [US]$500,000’ (Nawrocki 1987:14-15 cited in Rosoff et al. 1998:370). This example underscores the magnitude of crime carried out on the Internet.

A hacker can scan multiple databases and explore numerous criminal possibilities (Newman and Clarke 2003). Multiplicity is one of the defining features that separate criminal transactions in the physical world because of its multi-dimensional nature. The Internet also provides anonymity to perpetrators, which can allow them to create multiple identities. Although this type of technique is carried out in the physical world, the Internet magnifies the opportunities available for people to take on different identities. Crimes where this may apply include the Nigerian fraud scams, securities fraud and auction fraud.

The three criminogenic attributes discussed here: anonymity, multiplicity, and target exploration, have shown how the Internet provides opportunities for committing a broad range of cyber crimes that may have been limited in the physical world, and as such opens the way for new types of crime and criminals.

4.6 DIVERSE FORMS OF CYBER CRIME – A TRADITIONAL AND NEW MODUS OPERANDI

This chapter argues that crimes of the twenty-first century involving the Internet are a combination of traditional forms of crime committed through new methods and new forms of crime committed using the technological sophistication of computing.
technologies. As such, the forms of cyber crime are broad and constitute various dimensions. Crimes committed on the Internet can also extend from the virtual world to the physical world such as damage to critical infrastructure and stalking. Collin (2000:2) argues that, ‘the physical and virtual worlds are inherently disparate worlds. It is now the intersection, the convergence, of these two worlds that forms the vehicle ...’ for a broad range of cyber crime to be carried out on a single platform.

Table 4.3  Traditional Crimes - Traditional and New Methods

<table>
<thead>
<tr>
<th>Traditional Crime - Traditional Method</th>
<th>Traditional Crime – New and Sophisticated Method</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Child Sexual Abuse</strong></td>
<td><strong>Internet Paedophiles</strong></td>
</tr>
<tr>
<td>Proximity to schools, local community and local amenities, such as pools, beaches, shopping centres and sports grounds.</td>
<td>Internet chat rooms, newsgroups, bulletin boards and anonymous re-mailers. The Internet also opens up the opportunity for Internet paedophiles to set up global networks and online communities.</td>
</tr>
<tr>
<td><strong>Fraud</strong></td>
<td><strong>Internet Fraud</strong></td>
</tr>
<tr>
<td>Manual processing such as physically stealing an individual’s credit card to commit credit card fraud or cheque fraud. Using the post to mail fraudulent scams such as pyramid scams and the Nigerian fraud scheme.</td>
<td>Global potential for victims and criminal networks to commit credit card fraud, share market manipulation, fraudulent solicitations, illicit funds transfer, and auction fraud on a global scale through chat rooms, unauthorised entry into computer systems and networks, key logging, e-mail, and through the use of fictitious websites. Targets are also more accessible given the diverse ways fraud can be carried out on the Internet.</td>
</tr>
<tr>
<td><strong>Stalking</strong></td>
<td><strong>Cyber Stalking</strong></td>
</tr>
<tr>
<td>Physical exposure through the workplace and recreational activities. Communication through traditional media such as the post and telephone.</td>
<td>Virtual communication through means, such as chat rooms, e-mail, anonymous re-mailers, and use-net groups. Hacking into targets computer or files as well as posting information on websites.</td>
</tr>
<tr>
<td><strong>Economic Espionage</strong></td>
<td><strong>Cyber Espionage</strong></td>
</tr>
<tr>
<td>Clandestine photography; ‘Dumpster Diving’.</td>
<td>Unauthorised entry to computer systems and networks.</td>
</tr>
</tbody>
</table>

---

68 Newsgroups are electronic noticeboards where individuals and groups of individuals communicate most commonly through the Internet.

69 Anonymous re-mailer is a conduit through which information is received anonymously.
Table 4.3 outlines four traditional forms of crime and demonstrates the methods used in their application to the Internet. Table 4.3 shows that opportunities for traditional forms of crime have expanded into cyberspace by the very nature of the technology.

The following sub-section examines four traditional forms of crime – cyber stalking, pornography, terrorism, and fraud, while the second sub-section examines three new forms of cyber crime: unauthorised access to computer programs and files, computer viruses and computer worms.

4.6.1 Cyber Stalking

Make no mistake: this kind of harassment can be as frightening and as real as being followed and watched in your neighbourhood or in your home (Gore 1999:1).

The United States Department of Justice defines cyber stalking as the ‘use of the Internet, e-mail or other electronic communications devices to stalk another person through threatening behaviour’ (Gore 1999:1). Stalking is a traditional form of behaviour that lends itself to digital technology. Ogilvie (2000a:2) observes that ‘cyber stalking thus entails the same general characteristics as traditional stalking, but in being transposed into the virtual environment it is fundamentally transformed’. It is transformed because it no longer requires the physical presence of an individual to harass or stalk another individual. In addition, the victim does not have to know anything about the individual who is stalking them. Reno (1999:4) highlighted major differences between online and offline stalking which showed that:

Electronic communications technologies make it much easier for a cyberstalker to encourage third parties to harass and/or threaten a victim ... Electronic communications technologies also lower the barriers to harassment and threats; a cyberstalker does not need to physically confront the victim.

The Internet opens up possibilities to harass or threaten other individuals on the Internet in a diverse number of ways, such as e-mail, through chat rooms and newsgroups. Internet stalkers also have greater opportunities to search for potential victims through a broad range of communication channels. According to Ogilvie (2000b:2), cyber stalking is conducted through three primary forms to solicit or exploit communication:

- E-mail stalking – ‘Direct communication through e-mail’.
CHAPTER 4: THE NEXT GENERATION – COMPUTER AND CYBER CRIME

- Internet stalking – ‘Global communication through the Internet’.
- Computer stalking – ‘Unauthorised control of another person’s computer’

Ogilvie (2000b:3) argues that ‘unsolicited e-mail is one of the most common forms of harassment …’ . Cyber stalkers may be motivated out of a desire to exert control or power over other victims for personal gratification. Parker (1976) notes that the motives for computer criminals also include the ‘… inability to recognise the harm done to others, [and through the] personification of computers (seeing computers as adversaries in a game) ...’.

Although many forms of stalking originate in the virtual world, this form of cyber crime can also extend to the physical world. One example that illustrates this involved the successful prosecution of a 50-year-old male security guard. After a 28-year-old female rejected romantic advances from the security guard, the defendant used the Internet to solicit the rape of the victim (Reno 1999). According to reports, ‘the defendant terrorised his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards …’ (Reno 1999:4). In addition, the defendant posted the victim’s contact details on the Internet, which led to a number of men visiting her at home with the alleged intent to rape.

The nature of cyber stalking also allows stalkers to remain anonymous while threatening or terrorising victims. This can have an enormous effect on the victim because the victim may be unaware of the location of the cyber stalker. An example that demonstrates the use of anonymity involved Trung Ngo, who in 1998, sent numerous anonymous e-mail messages, which were harassing in nature (at times in excess of 50 e-mails per day) to a senior supervisory-level Defence Department employee at the Defence Information Systems Agency (DISA). The US Department of Justice (1998:1) reported that three years earlier, the defendant worked as a telecommunications expert for the victim at DISA. In addition to the harassing e-mails, the victim was sent magazine subscriptions in Trung Ngo’s name without authorisation or knowledge, and a range of products.

The cases outlined above show the serious and criminal nature of cyber stalking and demonstrate that victims can be targeted specifically, or randomly chosen. Thus there
are diverse opportunities available on the Internet to carry out cyber stalking through various methods and techniques.

4.6.2 Internet Sex Crimes against Children and Youth

Internet sex crimes against children and youth are one of the fastest growing illicit activities on the Internet. This takes two basic forms:

- The distribution of erotic images of children; and

- The use of the Internet to lure children with the intent to abuse them.

The distribution of child pornographic images is not new; however, its methods of transfer on the Internet provide ease of access to a global market. In a report on the Scale of Internet Child Pornography in Australia, the Australian Bureau of Criminal Intelligence (ABCI) observe that ‘Child sex offenders have embraced emerging technology to transmit and receive pornography to network with other offenders and to access potential victims’ (ABCI 2001:16). The Internet also provides paedophiles and like-minded individuals the means to produce, collect, distribute, communicate and share images of child sexual abuse with others in a short space of time throughout the globe. Individuals also sell child pornographic images and videos via e-mail and illegal Internet websites.

The rise in Internet sex crimes against children and youth is reflected in the number of groups of individuals who have been investigated and prosecuted for the distribution or participation of child pornographic images on a global scale over the past few years.\(^\text{70}\) A recent example that supports this point involved the infiltration of an Internet paedophile ring identified as ‘Shadow Brotherhood’. According to reports:

... some members of the group sexually abused children and then posted the images on their Web site, which also provided advice on how to meet children in Internet chat rooms. They used sophisticated encryption techniques, sometimes hiding material in seemingly innocent files ... (The Guardian Newspaper 2002 cited in Save the Children Europe Group 2003:7).

\(^{70}\) See for example Akdeniz (1996-2003) for numerous cases and materials related to Internet child pornography. See also Congressional Statement Federal Bureau of Investigation on Internet Child Pornography (Heimbach 2002).
Shadow Brotherhood appeared to be a highly structured network that organised its members in groups where familiarity and trust played a significant role. According to Police:

... administrators operated a “star” system to rate members: after initial vetting, new members received a one-star rating, allowing them to view certain chat rooms, newsgroups and bulletin boards. To gain further stars they [the members] had to post images of child sex abuse on the group’s site; as they gained stars, they obtained greater access to restricted sites containing the most graphic material (The Guardian Newspaper 2002 cited in Save the Children Europe Group 2003:7).

This example highlights the complex and disturbing ways in which Internet paedophiles communicate, process, and distribute offensive sexual images of children.

As part of a global child pornography business, a husband and wife were arrested in 1999 for child exploitation. Tom and Janice Reedy operated a website that offered in excess of 2000 categories of child pornography, such as ‘children forced to porn’ and ‘child rape’. The images purportedly originated from Eastern Europe and different parts of Asia. The business amassed a subscription of at least 350,000 people from 60 countries (Coman 2003). Moore (2003) points out that ‘the database was a cross section of respectable society’, which included lawyers, doctors, and teachers (cited in Coman 2003).

The Internet greatly facilitates the dissemination of illicit images of children. The Internet also provides a new means for paedophiles and like-minded individuals to target, solicit, and groom children, as well as providing new ways to communicate with children and each other on a global scale. Furthermore, the Internet assists in concealing a paedophile’s activities through anonymity and by disguising the nature of their communication through chat rooms and anonymous re-mailer services.

---

71 Save the Children Europe Group (2003:3) note that ‘the grooming process is the strategy used by sexual abusers to manipulate the child, and potentially protective adults, so the abuse can take place in a situation where the abuser has total control over the victim. It is a process where the abuser gradually overcomes the child’s resistance through a sequence of psychologically manipulative acts. It is also used to silence the child after the abuse has taken place’.
4.6.3 Cyber Terrorism

The nature of terrorism has changed over the past decade as a result of computing and information technologies such as the Internet (See Denning 2000; Grabosky and Stohl 2003; Weimann 2004; Urbas 2005b). Cyber terrorism may be understood as ‘...unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives’ (Denning 2000:1).

The Internet creates opportunities for terrorists to further their objectives through ease of access, anonymity, and infinite potential audiences and sympathisers, efficient means of communication, speed of information, and lack of regulation (Weimann 2004). For an attack to be categorised as cyber terrorism, Denning (2000:1) explains that it ‘...should result in violence against persons or property, or at least cause enough harm to generate fear’. Examples of terrorism include attacks that lead to injury or death, plane crashes, explosions, and water contamination.

The use of a computer to disrupt technological infrastructures such as power supplies, road and air traffic control, and economic systems such as banks, financial institutions and stock markets also constitute examples of cyber terrorism. If power, for example, is shut down and not restored for a considerable length of time and people die as a result of it, this would therefore constitute cyber terrorism (Denning 2000:1). If cyber terrorists break into a road traffic control system and change the coordination of traffic lights, and cars collide resulting in death, this would also constitute cyber terrorism. Similarly, aeroplanes colliding as a result of disruption to an air traffic control system would also be considered an act of cyber terrorism when done to intimidate or coerce.

Terrorism is a traditional form of crime. The methods applied to carry out cyber terrorism, however, differ from methods used to carry out terrorism in the physical world. This is achieved through efficient, clandestine communication by terrorists, propaganda by terrorist groups, and carrying out attacks through computer networks. It is these methods that play an important role in planning and coordinating plans in furtherance of terrorist acts. Collin (2000:1) argues that ‘the intelligence systems, tactics, security procedures and equipment that were once expected to protect people, systems, and nations, are powerless against this new, and very devastating weapon’.
Terrorists use the Internet for efficient, clandestine communications. Messages can be sent and received surreptitiously via the Internet through sports chat rooms, pornographic bulletin boards, e-mail, and image files. The content of these messages may also be concealed through encryption and steganography (Grabosky 2004). Grabosky (2004:7) suggests that ‘the nature of the Internet and world wide web are ideally suited to communications across widely dispersed elements of a network’, thus providing an efficient and anonymous environment for terrorists to communicate with one another.

To advance their ideological and political agendas, the Internet provides terrorist organisations unparalleled opportunity to disseminate propaganda and gain publicity. Terrorist organisations have direct control over the content of information and messages on their websites, a stark contrast to the limited access afforded over other traditional forms of media (Weimann 2004). Weimann (2004:6) points out two issues that are most commonly used on websites for such purposes: ‘... the restrictions placed on freedom of expression and the plight of comrades who are now political prisoners’. These techniques by terrorist groups are applied to increase their support base and to appeal to sympathisers of their cause.

Propaganda can be disseminated via Internet websites created by terrorist group supporters. For example, Hamas supporters publish the group’s charter and additional information on their organisation. According to Weimann (2004:6), ‘... many terrorists now have direct control over the content of their message [which] offers further opportunities to shape how they are perceived by different target audiences and to manipulate their own image and the image of their enemies’. Other terrorist groups post video messages, create video footage of their activities on the Internet and record who has carried out attacks (Marcus 2004:1). These methods show that the Internet has furthered the means for terrorists to spread their messages on a global scale, thus increasing the potential audience base and increasing the means of communication between terrorists and Internet users.

4.6.4 Internet Fraud

While Chapter Three maintained that fraud is one of the most recognised forms of white-collar crime, Internet fraud is also one of the most common forms of cyber crime
According to the Federal Bureau of Investigation (FBI), Internet fraud constitutes:

... any fraudulent scheme in which one or more components of the Internet, such as Web sites, chat rooms, and e-mail, play a significant role in offering nonexistent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims' funds, access devices, or other items of value to the control of the scheme's perpetrators (IFCC 2001:1).

Fraud can be carried out in a diverse range of ways. In addition, the Internet provides a more efficient and effective means to reach millions of users at a relatively low cost.

The various forms of misleading and deceptive practices of Internet fraud can be categorised into four schemes:

- **Advance fee schemes**: these include pyramid schemes, Ponzi schemes, chain letters and bulk e-mail, business opportunity schemes, bogus auctions, and prizes and lotteries. One of the common elements of these schemes is that prospective victims are deceived into parting with funds with an understanding that they will financially gain as a result of an advanced payment (Grabosky et al. 2001). According to Grabosky et al. (2001:111), ‘... this type of fraudulent scheme usually entail enlisting the services of the prospective victim to assist in an activity of questionable legality, thus providing some assurance that the victim, once defrauded, would be unlikely to report the matter to the police’. The increasingly sophisticated nature of these schemes has also made it challenging to trace offenders, many of whom operate all over the globe, in countries where laws may be more relaxed and or investigation is too costly to pursue.

- **Non-delivery and defective products and services**: cover a range of areas, some of which may involve Internet services, cable decryption kits, computer products and services, sexual services, misleading credit and loan facilities, health and medical products, and educational qualifications. The non-physical nature of the Internet has increased the different ways these schemes are carried out. Grabosky et al. (2001:115-6) argue that ‘this problem is exacerbated in global commercial transactions where long-distance delivery of goods is involved, sometimes entailing customs clearance and the payment of importation taxes’. In other
examples, goods may never be received, and or faulty or incorrect goods may be
delivered, thus creating additional problems in solving payment transactions.

- Share market manipulation can occur through misinformation, rumour, and
hyperbole. The most common schemes include ‘pump and dump’ and ‘slur and
slump’. Opportunities to carry out these schemes have increased given the
different ways information is disseminated through online bulletin boards, news
groups, counterfeit websites, false press releases, and e-mail. The pool of
prospective victims has also increased, given that a number of individuals
involved have little or no financial experience.

The opportunity to create a faster and more efficient means to reach potential targets of
these schemes has been assisted by the Internet. In addition, the costs involved to set up
such schemes are considerably lower compared to traditional methods, thus increasing
the potential number of motivated offenders.

The Securities and Exchange Commission (SEC) has brought more than 150 Internet-

On September 6, 2000, the Commission announced 15 enforcement
actions against 33 companies and individuals who used the Internet to
defraud investors by engaging in pump-and-dump stock manipulations.
The perpetrators of these market manipulations “pumped” up the total
market capitalisation of those stocks involved by more than $1.7 billion.
The actions involved the stocks of more than 70 microcap companies
and illegal profits of more than $10 million. The case ... involves
individuals and small entities that spread false information through
electronic newsletters, websites, e-mail messages, and through posts on
Internet message boards.

In an example of Internet fraud examined by the Securities and Exchange Commission
(SEC), Jonathan G. Lebed, aged 15, used the Internet to conduct a stock manipulation
scheme that made total profits of US$272,826 (Long and Horowitz 2000). Lebed
purchased stock through brokerage accounts on the Internet. After purchasing the stock,
Lebed sent misleading e-mails to various message boards, which led to an increase in
the price of the stock. As a result, Lebed sold his shares for a profit (Long and Horowitz
2000).

Methods of payment and payment systems have also changed to accommodate the
growth of transactions via the Internet. Payment systems on the Internet have provided
further opportunities for people to use information in an unlawful manner, given the vulnerability to unauthorised access. These methods of payment appear to contribute to the growth of fraud because of the opportunities that are made available through the volume of data and personal information.

Table 4.4 Usage of Internet payment Systems in Four Countries - July 2000

<table>
<thead>
<tr>
<th>Payment Systems</th>
<th>England</th>
<th>France</th>
<th>Germany</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONLINE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit card online</td>
<td>81%</td>
<td>61%</td>
<td>20%</td>
<td>88%</td>
</tr>
<tr>
<td>Debit card online (PIN less)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1%</td>
</tr>
<tr>
<td>OFFLINE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct debit</td>
<td>-</td>
<td>-</td>
<td>19%</td>
<td>-</td>
</tr>
<tr>
<td>Phone/fax in credit</td>
<td>4%</td>
<td>-</td>
<td>-</td>
<td>5%</td>
</tr>
<tr>
<td>Cash on delivery</td>
<td>-</td>
<td>10%</td>
<td>16%</td>
<td>-</td>
</tr>
<tr>
<td>Billing existing acct</td>
<td>4%</td>
<td>4%</td>
<td>14%</td>
<td>2%</td>
</tr>
<tr>
<td>Check</td>
<td>-</td>
<td>12%</td>
<td>-</td>
<td>4%</td>
</tr>
<tr>
<td>OTHER</td>
<td>11%</td>
<td>13%</td>
<td>31%</td>
<td>-</td>
</tr>
</tbody>
</table>

Source: Gartner Group 2001

Table 4.4 shows that credit card usage on the Internet appears to be one of the dominant and preferred methods of payment. The reliance on credit cards for Internet transactions increases the opportunities for its exploitation. Matt (2002:1) describes an example of credit card fraud which involved two British citizens who gained unauthorised access into a number of websites based in the United Kingdom, USA, Canada, Japan, and Thailand, stealing credit card information on approximately 26,000 accounts. The information obtained was allegedly sold to cyber markets in the former Soviet Union. Credit card information stored on computer systems makes this type of fraud an attractive option for would-be offenders given the volume of information on the Internet and various methods to obtain it.

In summary, fraud is an age-old form of criminality that has been significantly enhanced by the advent of digital technology. Not only can traditional forms of fraud, such as
false advertising, be accomplished more efficiently, new methodologies such as phishing and web-jacking have enhanced the repertoire of fraud.

4.6.5 Unauthorised Access to Computer Programs and Files

One of the earliest forms of computer abuse detected was the unauthorised access to computer files, also commonly termed ‘hacking’ (see Parker 1976; Turkle 1984). Unauthorised access to programs or files occurs when an individual achieves entry into another’s computer system without permission. More recently it has become the first step in carrying out additional forms of cyber crime. Stoll’s (1989) account of tracking a hacker through the Berkeley computer network is one example in which unauthorised access was gained in order to commit computer espionage.

Denning (2000:4) describes a case which involved an ‘… act of sabotage against a critical infrastructure, [in which] a fired employee of Chevron’s emergency alert network disabled the firm’s alert system by hacking into computers in New York and San Jose, California, and reconfiguring them so they’d crash’. The authorised access to this computer network was paramount in committing sabotage against his former employer. In another example, a Brisbane man faced charges relating to hacking after it was alleged that he penetrated the computer system of Maroochy Shire Council to create the overflows of raw sewage on the Sunshine Coast (Denning 2000:4).

These three examples demonstrate the serious nature of unauthorised access into computer systems and networks. They also illustrate that these forms of crime can be carried out with a single computer anywhere around the globe, which has the potential to disrupt millions of computer users and systems. The transnational nature of these forms of crime means that any computer connected to the Internet could be affected.

4.6.6 Computer Viruses

Computer viruses are one of the most common forms of computer and cyber crime. Spafford et al. (1990:316) describes a computer virus as:

... a segment of machine code that will copy its code itself into one or more larger “host” programs when it is activated. When these infected programs are run, the vital code is executed and the virus spreads further ... Computer viruses cannot spread by infecting pure data: pure data files are not executed. However, some data, such as files with spreadsheet
input or text files for editing, may be interpreted by application programs.

As more and more individuals connect to the Internet through e-mail, the potential financial damage to organisations increases exponentially. This is supported by data from the ICSA Labs 8th Annual Computer Virus Prevalence Survey, which illustrated a growth in the number of corporations who had experienced at least one virus encounter in 2002 (Bridwell 2003:8).\textsuperscript{72}

\textbf{Figure 4.1 Virus Prevalence Survey 2002}

The ICSA Lab’s survey also reported that during this period, more than 1.2 million virus incidents were reported on more than 900,000 desktops, servers, and perimeter gateways to their organisation (Bridwell 2003:5).

Figure 4.1 also shows that e-mail attachments are an increasing source of viruses rather than through diskettes, which were linked to early forms of computer crime. For example, in 1988, e-mail attachments contributed to approximately 30 per cent of virus sources. However, in the period 2000-2002, this figure increased to over 80 per cent. In 1997, diskettes contributed to over 80 per cent of the source of virus while this figure dropped to less than 10 per cent over the past three years (Bridwell 2003). A change in

\textsuperscript{72} It is important to note that a number of the viruses illustrated in this survey are technically considered computer worms rather than viruses. Not all respondents are aware that there is a difference or understand what the difference is between worms and viruses.
target distribution from diskettes to e-mail indicates that e-mail is a much more efficient vector for viruses.

4.6.7 Computer Worms

A computer worm is a program that replicates itself across computer networks. Computer worms break into computer networks through vulnerabilities in the targeted computer's software or operating system (Princeton University 2003:2). Computer worms are commonly recognised as computer viruses; however, there is a difference as worms can also run independently of computer viruses (see Spafford et al. 1990). Spafford et al. (1990:317) argue that:

... unlike viruses, worms ... travel from machine to machine across network connections; worms may have portions of themselves running on many different machines. Worms do not change other programs, although they may carry other code that does, such as a true virus.

In 1998, Robert Morris launched an Internet worm infecting thousands of UNIX computer systems. The program penetrated the memory of computers resulting in the shut down of more than 5000 computers. Once Morris was aware of the impact his worm had created, he proceeded to repair the damage caused; however, this was not before thousands of computers were infected and disabled. The damage caused was not only the disabling of computers but also damage to computer hardware and the financial costs involved in fixing the computers and the subsequent loss of business. The Morris Worm was one of the first publicised cases of hacking in the United States. The conviction of Morris led to three years' probation, 400 hours of community service and over US$10,000 in fines (see Freeh 2000).

These three forms of crime – unauthorised access to computer programs and files, computer viruses, and computer worms – represent new forms of computer and cyber crime, which collectively impact economically on Internet users. Clarke and Newman (2003) point out:

The total worldwide cost of viruses, worms and other security problems amounted to US$45 billion in 2002 ... The 2003 cost will be much

---

73 Katyal (2001:9) points out that 'the infamous 'I Love You' bug shared elements of both viruses and worms. It resembled a virus because it bred on a host computer's hard drive, but was a worm because it reproduced without any additional human input over a network'.

Despite the enormous financial impact outlined by Clarke and Newman, more and more of these crimes are perpetrated for other reasons, as the example of cyber espionage shows. Most viruses and worms are executed on common programs such as Microsoft Windows, which means that more and more people will be affected by a virus or worm. The connection of computers through various networks all around the world also opens up the possibility for transnational implications for these three forms of crime.

4.7 SUMMARY

This chapter has observed that the Internet is one of the fastest evolving platforms in a space where crime is carried out on a scale previously limited by geographical boundaries. As a result, this chapter has shown that cyber crime poses significant risks to individuals, businesses, government agencies and other organisations that are reliant on the Internet for commerce and for the exchange of information, goods, and services (see MacGibbon 2003). We have seen that part of the nature of this phenomenon is diversity and innovation. The Internet’s virtual nature has meant that there is a strong reliance on trust relationships to ensure that commerce, information and goods and services are traded, exchanged, and received legitimately in order to reduce the level of criminal activities.

This chapter has set the framework to determine whether cyber crime can be explained by existing criminological theories, as illustrated in Chapter Three, or whether any theories require modification for greater applicability to explain different forms of cyber crime. Chapter Five will raise the question as to whether existing theories of criminal behaviour apply to cyber crime. If they do, we can then understand the motivations and aetiology of criminal behaviour. If this is not the case, however, it is important to determine what additional elements inform our understanding of the differences between crimes in the physical world and crimes in the virtual world.
CHAPTER 5: THEORIES OF CRIME AND CRIMINALITY AND THEIR RELATIONSHIP TO THE INTERNET

The history of criminological theory can be read as one of scholars developing general theories that have explanatory purchase in the areas they know, but limited explanatory power beyond those areas (Braithwaite 1991:45).

5.1 INTRODUCTION

The previous chapter showed that the Internet has facilitated the growth of crimes – old and new. The exploitation of technological applications for criminal purposes, however, is not new. The Internet has become a vehicle where a vast array of existing and new crime is facilitated as a result of sophisticated methods driven by technology. As Internet take-up increases around the globe, its traditional use has also changed from the purview of academics and scientists to the expansion of communication, information exchange, and entertainment, to criminal activities. Cyber crime has emerged as a scourge of the twenty-first century.

Crime on the Internet has opened up a significant area of criminology. This chapter extends the analysis from Chapter Three with the objective of placing emphasis on whether theories of criminal behaviour have ‘explanatory power’ (Braithwaite 1991) for crimes committed on the Internet. The objective of this chapter is to test the applicability of five substantive theories to a broad range of cyber crimes. Taking into account that a number of these theories were developed to explain juvenile offending and conventional crime, Chapter Three showed that a number of these theories could also apply to adult offenders and white-collar crime.

This chapter is organised into five main sections. Each section tests a different theory on five forms of cyber crime: hacking, piracy, sex crimes against children and youth, sharemarket manipulation, and fraud in the form of auction fraud, and/or phishing. There will also be additional forms of cyber crime examined in some sections to further demonstrate whether the theory is robust or limited in its applicability. Section 5.3 will examine Sutherland’s theory of differential association. Section 5.4 will analyse Merton’s strain theory through two modes of adaptation: innovation, and rebellion. Section 5.5 will explore Sykes and Matza’s techniques of neutralisation. Section 5.6
will examine Gottfredson and Hirschi’s general theory of crime, and lastly, section 6.4 will evaluate Cohen and Felson’s routine activity theory.

5.2 A CYBER PERSPECTIVE OF CRIMINAL BEHAVIOUR


It appears that these studies have continued the trend of criminology’s focus on social and ecological approaches, such as the early studies carried out by the Chicago school of sociology (Shaw and McKay 1931). While it may be argued that a number of different theories can explain criminal behaviour through opportunity, social learning, ecological influences, and violation of trust, the question remains, to what extent are these theories ‘... readily transposable to cyberspace’? (Brenner 2001:3). This chapter seeks to fill that gap through an examination of five theories of criminal behaviour across a broad range of cyber crimes.

5.3 DIFFERENTIAL ASSOCIATION THEORY

Chapter Three found that differential association does explain organisational deviance and certain forms of criminal behaviour identified with particular white-collar crimes, regardless of age. However, it also established that differential association theory had limitations in explaining street crime and white-collar crime through the same principles of behaviour as a general theory of crime. To examine differential association’s applicability to different forms of cyber crime, it is important to note that the theory’s
predominant explanatory mechanism is learned behaviour through association, largely intimate groups. Differential association theory is also based on the premise that there are definitions which conflict with appropriate behaviour in society that give rise to crime. Just how association with criminals can influence deviant behaviour of others through the learning of different techniques and skills is also important to explore.

Empirical research that has evaluated computer-mediated communication (CMC) through the Internet has positively shown the link between group association and social and delinquent behaviour (see Dreyfus 1997; Jordan and Taylor 1998; Meyer 1989; Douglas and McGarty 2001; Rogers 2001). If we take into account Sutherland’s nine principles (outlined in Chapter Three), a framework can be developed to ascertain the applicability of differential association theory to four different forms of cyber crime - hacking, Internet sex crimes against children and youth, Internet piracy, and Internet fraud (including auction and online securities fraud).

5.3.1 Hacking

It has been recognised that most individuals act alone in carrying out hacking (Rogers 2001) although recent examples demonstrate that a number of hackers have been identified by law enforcement agencies as part of hacking underground cultures or communities (see Jordan and Taylor 1998; Taylor 1999). According to Jordan and Taylor (1998:764):

> Hackers often hack in groups, both in the sense of physically being in the same room while hacking and of hacking separately but being in a group that physically meets, that frequents bulletin boards, on-line places to talk and exchanges information.

The dynamics of the hacker underground culture appear to primarily include intimate groups, where a ‘process of communication’ between hackers plays a central role.

---

74 For instance, Cyber worlds is a computer program that enables an individual’s access to log-on to numerous online communities where multiple users can interact and chat to other users.

75 Meyer (1989:25) defines a hacking underground ‘... as an individual, associated with the computer underground (CU), who specialises in obtaining unauthorised access to computer systems’.

76 Jordan and Taylor (1998:762-3) note that ‘community is ... understood as the collective identity that members of a social group construct or, in a related way, as the ‘collective imagination’ of a social group. Both a collective identity and imagination allow individuals to recognise in each other membership of the same community’.
Jordan and Taylor (1998:763) argue that ‘the computer underground, or at least the hacking part of it, can be in this way understood as a community that offers certain forms of identity through which membership and social norms are negotiated’. The different forms of identity within hacking groups are kept within the underground culture (see Tangent 1992-2003; Taylor 1999; Thompson 2004). The illicit nature of hacking and the secretive nature of the culture appear to contribute to the development and fostering of the underground community.

According to Taylor (1999:43):

The fact that hacker culture predominantly exists in an informational rather than a conventional physical environment means that, in the absence of the community qualities that come from shared physical space, articulations of what it is to hack and why people do it may have a disproportionate role to play in community formation within the computer underground and in influencing the perceptions of those external to the activity.

The informal nature of certain hacker cultures does not alter the correlation between group association and learned behaviour. Conversely, the more comfortable an individual is with like-minded individuals who view criminal activity such as hacking favourably, then Sutherland would argue, the more inclined an individual is to participate in criminal deviance. Jordan and Taylor (1998:764) cite an example of a member of the Zoetermeer hacking group, who states:

Hacking can be rewarding in itself, because it can give you a real kick sometimes. But it can give you a lot more satisfaction and recognition if you share your experiences with others ... Without this group I would never have spent so much time behind the terminals digging into the operating system.

This example demonstrates the influence of group association and membership on criminal behaviour. Furthermore, it certainly dispenses any misconception that hacking is solely the work of socially isolated ‘nerds’ (see also Taylor 1999; PlasmoId 1999; Rogers 2001a; Hacker Network Inc. 1999). Osgood et al. (1996:637) note that, ‘several studies suggest that individual offending is positively associated with time spent in unstructured socialising with peers in the absence of authority figures’ (see also Hirschi 1969; Riley 1987; Agnew and Peterson 1989). Hacking is one example of a criminal activity predominantly committed in unstructured settings ‘... in the absence of authority figures’ (Osgood et al. 1996:637) due to its illicit and underground nature.
Empirical evidence to support Sutherland's correlation between group association and criminal behaviour can be shown by Hollinger's (1993) study of the extent of hacking among university students, Meyer's (1989) study, which examined the social and organisational approach of hackers in a computer underground, and Schell et al.'s study (2002) of the psychological and social behavioural traits of hackers.

Hollinger's study was based on a survey of 1766 university students and a study of three who had been convicted of illegally entering the University of Florida's computer system and damaging files. Hollinger's study found that it was more likely for individuals to engage in criminal activity if they had friends who were also involved in the activity (see also Rogers 2001a). Hollinger's study shows that associations formed between individuals and the shared learned behaviour influences criminal behaviour of hackers.

Meyer (1989) concentrated on the social approach of the computer hacker and the daily experiences of hacking which are now criminalised. He concluded '... that the computer underground consists of a more sophisticated level of social organisation than has been generally recognised' (Meyer 1989:9). The social setting appears to make it easier for hackers to perform their activities. The point to be made is the influence of the hacking network, which is perceived as 'social' to perform activities that are considered illegal.

While Meyer's intention was to illustrate the social and organisational approach of hacking and the skills developed within it, his study established that group association fosters learning and can act as an influence to criminal behaviour within this environment. This behavioural learning is largely carried out through communication and through various techniques and skills learned and developed within this environment.

Schell et al. (2002) analysed Meyer's study against their study of hackers and revealed a number of findings that appear consistent with Meyer's findings. For example, the H2K and DefCon study indicates that approximately 25 per cent of hackers spend substantial time communicating with their colleagues (Schell et al. 2002:177); however, after communicating with their colleagues, approximately 57 per cent act alone in carrying out their acts, while the remaining 43 per cent tend to collaborate with others (Schell et
al. 2002:177). Trust is also an important issue because it appears to determine whom they collaborate with.

Communication plays a central role among hackers for two reasons: first, for the distribution of information, and second, through the various techniques and skills that are learned to carry out hacking as a criminal activity (Denning 1999). According to Sterling (1992:59):

> The way to win a solid reputation in the underground is by telling other hackers things that could have been learned only by exceptional cunning and stealth. Forbidden knowledge, therefore, is the basic currency of the digital underground ... hackers hoard this knowledge, and dwell upon it obsessively, and refine it, and bargain with it, and talk and talk about it.

DefCon, the annual gathering of hackers, is one forum that draws hackers together for the purpose of exchanging information, ideas, and techniques in an open forum (see Tangent 1992-2003; Denning 1999; Schell et al. 2002). Hackers at DefCon also have the opportunity to compete for prize money in hacking contests (Wible 2003). Similarly, the annual security conference, Black Hat, attracts hackers who compete for prize money in the attempt to hack into computer servers to test out new computer programs. According to Wible (2003:1591) ‘... the hacking competitions sponsored by security firms promise large rewards, but the hackers who participate stress that their aim is to improve programming by exposing deficiencies in code’. In fact, rewards in excess of US$100,000 are offered to those hackers who break the code.

Over the past two years, Australia has hosted a hacking conference, Ruxcon, which is organised by hackers and attracts a range of people from IT specialists to security professionals, students, and law enforcement personnel. According to Spencer (2004:6), an organiser of Ruxcon, ‘we wanted to have a local conference where people could showcase their skills. It was also designed to encourage new people into this field and find people who didn’t know about who had interesting things to talk about’ (cited in Gray 2004:6). These conferences also provide the impetus for hackers to discuss recent exploits and develop associations with other hackers. In addition, the presence of law enforcement agencies provides an opportunity for them to learn about the hacking culture and keep apace with the changing developments.
Communication within the computer underground can occur through bulletin boards, e-mail, bridges,\footnote{77 Meyer (1989:48) points out that ‘a “bridge” is a technical name for what is commonly known as a “chat line” or “conference system”.’} loop lines,\footnote{78 Meyer (1989:50) notes that ‘loop lines are actually telephone company test lines … [which] allows for individuals to hold private conversations without divulging their location or identity by exchanging telephone numbers’.} voice mailboxes, and conferences such as DefCon and Black Hat. These modes continue to provide reliable methods of communication on the Internet for members to exchange knowledge and techniques. Furthermore, communicating and sharing information through these modes allows greater anonymity between members of the underground and a greater sense of association within a group. Meyer (1989:75) made the following observation:

Hackers have adopted existing methods of communication, consistent with their skills in high technology, to form a social network/community that allows for the exchange of information, the socialisation of new members, socialising with others ... performing the “deviant” act itself via these means.

Meyer maintains that these groups are social despite the acknowledgement of unlawful activity taking place (see also Denning 1999; Schell et al. 2002). Meyer (1989:54) notes:

... that the computer underground has established an extensive social network for the exchange of resources and mutual support. The characteristics of the [computer underground] CU varies according to the goals of the participants, but the presence of mutual association is consistent.

The social approach of the underground hacking culture provides a means to develop an organisational structure between the members. Meyer’s (1989:75-76) study observes that the ‘subcultural adaptation of language, expectations of normative conduct, and status stratification based on mastery of cultural knowledge and skill, all indicate that the computer underground is, at the very least a social organisation of colleagues’. Some of the roles performed in this group and the organisational structure of the culture reinforce Sutherland’s point that the ‘... specific direction of motives and drives is learned from definitions of the legal codes as favourable or unfavourable’ (Sutherland and Cressey 1974:75). In this case, it illustrates acceptance of illegal behaviour based on
the social and organisational dynamic and the criminal activities carried out as part of the hacking culture.

Although hackers may carry out their activities separately, Meyer’s research also points out that shared resources and information are part of the culture of unauthorised entry into computer systems. Clearly, the techniques adopted by the underground hacking culture and the skills learned within the group lend support to Sutherland’s point that criminal behaviour is learned in association with others in a process of communication. For example, Meyer (1989:39) argues that:

In order for the communication to be organised and available to participants in many time zones and “working” under different schedules, centralised points of information distribution are required ... [such as] computer bulletin boards, voice mail boxes, “chat” lines, and telephone bridges/loops — have been adopted by the CU for use as communication points.

The hacking culture maintains these communication structures discretely to carry out illegal activities and to retain a sense of anonymity within the group. Part of building this association, therefore, requires a level of trust among the hackers while they communicate in cyberspace.

Trust is considered an essential part of group association and of knowledge and information sharing in the hacking culture (Meyer 1989; Denning 1999; Taylor 1999; Luzwick 2002; Schell et al. 2002). Luzwick (2002:15) emphasises the point by stating that ‘the key to knowledge sharing ... between hackers is trust’. A high level of trust among hackers allows for greater communication to discuss techniques and recent exploits, such as the latest computer network intrusion. Trust also breaks down barriers between the hackers, which can lead to new ways of learning deviant behaviour in association with others.

While trust appears implicit in many hacking groups, links between the individuals of the hacking underground, as Meyer (1989) observed, are not always strong, and as a result trust may be violated. Taylor (1999:29) provides an example of a hacker who was betrayed by another and points out that, ‘true hackers depend upon secrecy, and trust each other not to act in any way that might incur a clamp down from the law enforcement agencies’. Meyer (1989:53) maintains that:
Loyalty between individuals seems rare, as the CU is replete with tales of ... hackers who, when apprehended, expose identities or "trade secrets" in order to avoid prosecution. These weak collegial ties may be fostered by the anonymity of the CU communication methods and the fact that all CU actors are, to some extent in competition with each other.

The 'weak collegial ties' that Meyer identifies are consistent with Sutherland's argument that, as part of the process of communication, techniques of committing the crime are sometimes complicated, sometimes simple, and as a result, the dangers of participating in illegal behaviour can be exposed through these means. For example, communicating various hacking activities via a chat room or on bulletin boards[79] may pose risks, such as being caught by enforcement agencies. Luzwick (2002:15) also makes the point:

With hackers an online relationship is established, sometimes reinforced by face_to_face [sic] meetings like Defcon or in clubs like CHAOS. If a hacker hoards information, doesn't share on a reasonable quid pro quo basis, or sends inaccurate information more than a couple of times, the hacker community at large will ostracise him.

The issue of trust discussed above appears to show that the drives and motivations of hackers are very different from each other because the level of trust varies. This may be dependent on the likelihood of an individual being investigated and prosecuted by law enforcement agencies. Without a strong association of trust, the underground culture may not operate as a cohesive network, and behaviour may not be encouraged or fostered to the extent to which Meyer's study indicated.

Meyer's (1989) study suggests that individuals within a hacking underground foster criminal behaviour due to the contact with other individuals who share criminal patterns which are part of their culture. Jordan and Taylor (1998:768) argue that "... peer recognition from other hackers or friends is a reward and goal for many hackers, signifying acceptance into the community and offering places in a hierarchy of more advanced hackers'. My argument is that the underground hacking culture provides a

[79] Computer Bulletin Board Systems (BBS) allow users to log on and leave messages, download files and programs. Meyer (1989:31) points out that 'computer underground BBS are generally owned and operated by a single person ... BBS in general are transitory in nature, and CU boards are no exception to this. Since they are operated by private individuals, they are often set up and closed down at the whim of the operator'.
forum where techniques can be discussed and skills learned in association with others to commit deviant behaviour.

Turkle’s (1984) study of the hacking culture in the 1960s and 1970s has shown little difference in the relationship between the hackers of that time and what currently exists today in hacking underground cultures. For example, communication and the exchange of techniques and languages remain an important aspect, as well as trust and secrecy among the hackers. What differentiates the hackers of the 1960s and 1970s and hackers in the early twenty-first century is the explicit criminal motivation of many contemporary hackers.

The study by Meyer (1989) showed that hackers influenced each other. In the words of Meyer (1989:52), ‘It is impossible to be part of the social network of the computer underground and be a loner’, hence the importance of group association in the hacking underground culture. In a recent case, it was reported that the author of the sasser worm, Sven Jaschan ‘... apparently succumbed to peer pressure, writing and releasing at least four different versions of the virus to impress school mates’ (Lowe 2004:16). In Austria, Thompson’s (2004) interview with a number of hackers who were part of a hacker underground and members of an international ‘virus-writers’ group known as the Ready Rangers Liberation Front appear to lend support to the role that networks play and the associations formed between individuals to influence behaviour.

These examples demonstrate that opportunities to develop social networks through newsgroups, bulletin boards, private chat rooms, and e-mail have assisted the growth of hacking. They also show the vulnerabilities associated with communicating with members across the globe as violation of trust was identified. While the analysis suggests that group association influences the behaviour of hacking groups, most hackers act alone and are not influenced by association with others. The following section will test the applicability of differential association theory to Internet piracy.

5.3.2 Internet Piracy

Internet piracy is defined as the unauthorised use of copyrighted music, software, and motion pictures downloaded via the Internet. There are three ways in which piracy is carried out on the Internet:
• Pirate websites that make software available for free download or in exchange for uploaded programs;

• Internet auction sites that offer counterfeit, out-of-channel, infringing copyright software;

• Peer-to-Peer networks that enable unauthorised transfer of copyrighted programs (BSA 2002:1).

The study of software piracy has been an area of increased interest with several studies examining the motivation and offender characteristics of pirates (Hollinger 1993; Glass and Wood 1996; Skinner and Fream 1997; Seale et al. 1998, Kini et al. 2003; Higgins and Makin 2004). These studies have predominantly focused on individuals (largely students) rather than groups who participate in Internet piracy. However, several studies have found a positive correlation between software piracy and association with peers (Hollinger 1993; Skinner and Fream 1997; Higgins and Makin 2004) and that favourable attitudes toward software piracy are significant in the process of deviant behaviour (Logsdon et al. 1994; Skinner and Fream 1997; Rahim et al. 2001).

Hollinger’s (1993) study of university students at the University of Florida provides one of the first empirical studies of Internet piracy. The study, based on the response of 1766 university students, was conducted over a 15-week semester and examined whether students provided or received pirated computer software. The findings revealed that 10 per cent of the respondents had breached copyright laws on computer software (Skinner and Fream 1997:497). However, if these figures were applied to the remaining student body, Hollinger estimated that in excess of 3000 offences of piracy per semester would be carried out (Skinner and Fream 1997:497).

Although the study carried out by Hollinger was limited to one American university and conducted over a 15-week period, it nevertheless demonstrated that a friend’s involvement increased the likelihood of software piracy. For example, ‘... when more than half of the students’ best friends had occasionally committed piracy, almost 40 per cent had committed the act themselves’ (cited in Skinner and Fream 1997:497). Although it was difficult to ascertain the extent of learned behaviour from the study,
these figures suggest that association within this environment can influence involvement of software piracy among university students.

Skinner and Frem (1997) conducted a survey of undergraduate college students in the United States. The aim was to test the applicability of social learning theory to explain the behaviour of those participating in computer crime. Skinner and Frem hypothesised that learning about computer crime and associating with peers and teachers in this environment increases the likelihood of engaging in criminal behaviour. A questionnaire given to 581 undergraduate students across a range of disciplines and levels of study (e.g. freshman, junior, and graduate) revealed some interesting findings.

The survey found that software piracy was the most common form of computer crime amongst the students (37 per cent). Skinner and Frem (1997:506) reveal that of the students surveyed ‘at least once in their lives, 41.3 per cent ... had knowingly used, copied, or given to another person a copy of pirated software; 33.9 per cent had pirated software in the past year; 12.4 per cent had done so within the past month’. Second, learning about criminal activities from friends and family members positively correlates with software piracy. The results concluded that ‘differentially associating with friends who participate in computer crime is the strongest predictor of piracy ...’. Although the survey was carried out at one United States institution, it showed the influence of association and learned behaviour of software piracy amongst a controlled group of individuals.

The activities and organisational structure of Internet software piracy rings, such as DrinkOrDie (DoD), Razor 1911 and City Morgue, may provide an understanding of whether association and learned behaviour correlates with Internet piracy. A number of Internet software piracy rings are recognised as underground communities and organised networks due to the illicit nature of their activities and the associations

---

80 Piracy groups such as DrinkOrDie and Razor 1911 are termed “Release” Warez Groups. According to Downing (2003:3) there are three forms of Warez groups: first, ‘Organised groups engaging in distribution, reproduction, and trading of pirated software via Internet, [second], “Release” groups: specialize in “cracking” (i.e., removal or circumventing embedded software protections) and being the FIRST to distribute new software to the Warez scene, [and third], “Courier” groups: specialize in transferring or trading software among FTP sites, earning credit/points’.

81 “City Morgue” was an Internet based software piracy ring with in excess of 70 members engaged in Internet software piracy.
formed between members. In fact, it has been recognised that a number of Internet software piracy rings are linked to organised crime (IFPI 2001:2). The nature of Internet software piracy rings also appears to encourage association between members for the purposes of copying and distributing software illegally.

The piracy ring, DrinkOrDie, was formed in Russia in 1993 and involved approximately 65 group members from around the globe for the purpose of distributing pirated computer software and games (McNulty 2002a). A number of DrinkOrDie’s members have been prosecuted in the United States for their involvement under the intellectual property statute 18 U.S.C. §§2318, 2319, and 2320 (see CCIPS 2005).  

Figure 5.1  DrinkOrDie’s Organisational Structure

**Leader**

![Organisational Structure Diagram]

Figure 5.1 shows that DoD’s organisational structure classified group members in four categories in order of importance and responsibility (McNulty 2002a:1). Each member’s status within the group (on a social and organisational level) appeared to contribute to the learning and association of behaviour. This was significant to the

---

82 The extradition of an Australian-based member of DrinkOrDie, Hew Raymond Griffiths is one of the first cases in which United States authorities have sought extradition of a suspected Internet copyright infringer.

83 “Pre-ers” is a term used to describe members of Internet piracy rings who are responsible for preparing pirated products for final release prior to distribution to release sites.
overall global success of the piracy ring, which consisted of the distribution and supply of software and the disabling of copyright protection for broader use (see McNulty 2002a). Many members of DoD were students and white-collar workers, including executives in the software industry.

Communication also played a major role in the operation, which largely occurred through secure Internet chat sites. These methods of communication provided a degree of anonymity between the members and a sense of trust in concealing their activities from law enforcement authorities. The issue of trust also lies central to the organisational structure and organised nature of the network because violation of trust can lead to a fragmentation and breakdown of the operation.

More recently, a leader of the online software piracy ring, Razor 1911, was sentenced for his role in the distribution of illegal computer and console game software. McNulty (2003a:1) describes that:

Since the early 1990’s, Razor 1911 sought to achieve a reputation in the underground Internet piracy community ... the group prided itself on cracking and illegally distributing the most popular software games, usually before their public release date ...

It has been noted that a number of piracy rings within the Warez community, such as DoD and Razor 1911 compete against each other to achieve recognition and the reputation as the fastest and largest provider of free pirated computer software (usinfostate.gov 2001). This type of activity may increase the opportunity for members within the group to learn the various techniques of committing software piracy as well as fostering the drives, motivations, and criminal knowledge learned from members within a group environment.

By contrast to the examples examined above, LaMacchia, a Massachusetts Institute of Technology (MIT) student (United States v. LaMacchia) (871 F. Supp. 535 (D. Mass. 1994)), set up a bulletin board in 1994 for people to access and exchange copies of software applications and computer games free of charge on the Internet. LaMacchia operated the bulletin board on an MIT computer for approximately six weeks before it was shut down. Despite the estimated value of the software at US$1 million, LaMacchia operated alone and did not profit from his activity.
Jeffrey Levy, a 22-year-old college student, was sentenced to two years probation after pleading guilty to operating a website that allowed third parties access to thousands of software programs, songs, games, and movies. Similarly, 21-year-old Brian Baltutat operated a website that offered in excess of 140 software programs to third parties. Baltutat pled guilty and was sentenced to three years probation and required to adhere to a range of restrictions (Goldman and Gladstone 2003:2). The examples of LaMacchia, Levy, and Baltutat reflect individual rather than group activity.

In summary, the organised structure of piracy rings appears to foster association of members as an important element in the continuation of their illegal activities.64 Furthermore, it has established that association and positive attitudes towards piracy influence the proliferation of piracy. It is important to note that individuals also carry out piracy without the association of intimate groups and learned behaviour.

5.3.3 Internet Sex Crimes against Children and Youth

The Internet has furthered the development and ways sex crimes against children and youth are carried out. The National Center for Missing & Exploited Children (Wolak et al. 2003:3) note that Internet sex offences can include ‘... completed and attempted sexual assaults; illegal use of the Internet to transmit sexual material and to solicit minors; and the possession, distribution, and production of child pornography’. Although there is no universally recognised law on Internet sex crimes against children and youth, there have been and continue to be investigations and prosecutions of people involved in these activities.

The distribution of child pornographic images is not new. The way in which images are produced, collected, disseminated, transferred, and circulated on the Internet is new. Digital technology provides easy access to a global market, and communication channels to potential and like-minded individuals. Images of children and youth can be circulated on the Internet through a broad range of modes – chat rooms, news groups, e-mail, bulletin boards, e-groups, file servers, and anonymous re-mailer services.

64 A worldwide investigation by the Bureau of Immigration and Customs Enforcement and the United States Department of Homeland Security targeted in excess of 40 individuals who were members involved in a number of Internet piracy groups, such as DrinkOrDie, Request to Send (RTS), ShadowRealm, Live Warez, and POPZ (McNulty 2003a:1-2).
CHAPTER 5: THEORIES OF CRIME AND CRIMINALITY AND THEIR RELATIONSHIP TO THE INTERNET

Communication plays a central role among individuals who would exploit children beyond the simple exchange of illicit images. In a study conducted with the support of the Paedophile Investigation team and the Western Australia Police Service, Graycar (1998:1) notes that Internet ‘... paedophiles were using the World Wide Web (WWW) pages to proclaim their lifestyles, to disseminate information and to facilitate communication’ (cited in Forde and Patterson 1998:1). Forde and Patterson (1998:3) point out that, ‘many of the Internet links provided on WWW pages described anonymity and privacy techniques. E-mail messages sent to news groups took advantage of anonymity techniques’. This behaviour reinforces Sutherland’s (1947) point that ‘... deviance occurs when people define a certain human situation as the appropriate occasion for violating social norms or criminal laws’ (Sutherland and Cressey 1947 cited in Pfohl 1985:245). This enables the individuals to have a sense of secrecy and to foster criminal behaviour that was deemed acceptable within a tolerant group environment.

There is strong evidence to support the correlation between group association, learned behaviour and the distribution of child pornography. For example, the W0nderland [sic] Club was the first group of online offenders to be prosecuted for Internet child pornography; Operation Candyman involved an estimated 7200 members; Magneta was the US–European Child Pornography Ring; and Operation Starburst was an international paedophile ring that distributed graphic pictures of child pornography (Akdeniz 1997:229 cited in Edwards and Waelde 1997). According to Heimbach (2002:2), the offenders involved in Operation Candyman, ‘... included a school bus driver, a foster parent, a mentor for underprivileged children, a member of the armed forces, a delivery person, a landscaper, a prison case worker, a janitor, an office manager, a security guard and his wife’. This suggests that the type and status of the offender has little significance for the type of crime perpetrated on the Internet. Moreover, it shows the global power of the Internet to act as a conduit to communicate, produce, collect and distribute images of sexually abused children.85

85 In the United Kingdom, it was reported that ‘Police officers simultaneously raided 75 addresses and arrested dozens of people ... [in an] operation, codenamed Magneta [which], took six months ... [and] focused on paedophiles who used Internet chat rooms to advertise and exchange images of children being abused [sic]’ (Left 2002). In late 2000, Graff (2000:1) noted that ‘Russian police, working with British and American colleagues, arrested two suspects accused of selling child pornography over the Internet in
One of the most recognised Internet pornography rings in the early twenty-first century was the W0nderland Club. The W0nderland Club members shared an interest in images of sexually abused children. The Internet provided the means to develop a network of like-minded individuals to expand their illegal activities through on-going electronic communication. Members of the W0nderland Club operated around the globe and largely constituted males, from all social classes and a wide range of occupations. 10,000 images were required for an individual to gain private membership into the W0nderland Club: the chat room. The investigation culminated in the seizure of ‘... 750,000 pornographic images and 1,800 pornographic videos of children ...’ (Hunter 2001 cited in Stanley 2001).

Hines (2001:5), a key member of the W0nderland Club, points out the attraction of the Internet:

... it's so fast. Everything is moving. There's always a software update you need for some of the programmes on your computer or something and there's always a new game that you've got from somewhere or new pictures to trade or ... It's wonderful. It draws you in, it sucks you in. It's a whole world in itself and it moves so fast. That's part of the attraction of it for me (cited in Corbin 2001).

Group association was intrinsic to the development and proliferation of the W0nderland Club and illustrated the fact that criminal behaviour may be ‘... learned in interaction with other persons in a process of communication’ (Sutherland 1974: 75-6). Hines remarked that, ‘talking was great. You’d make friends, and you’d say ‘oh, I found this new picture, this great new picture’ and they would say ‘oh what’s it called’ and you’d tell them and if they had it they’d say ‘oh we’ve got that one’, but if they didn’t then they’d say ‘oh send it and we’ll have a look’” (cited in Corbin 2001:2). The activity was fostered through this environment as if it were acceptable behaviour.

The operation of the W0nderland Club supports Sutherland’s (1939) theory that individuals who display criminal patterns are more likely to become deviant by association with others who possess similar attitudes. Corbin (2001:2) notes that, ‘the Internet gave [x] access to like-minded people who supported his perverse desires’.

---

Europe and the United States ... In October, a prosecutor in Italy charged 1,491 people with sending and receiving child pornography from a web site ...’. Italian Police reported that the Members of the ring
Corbin (2001:1) also points out that '... some [members] even preyed on young children to satisfy the demands of their friends'. Membership was, therefore, not only based on the distribution of indecent sexual images of children but a solid communication between members, which occurred through Internet Relay Chat (IRC) channels.

The nature of the W0nderland Club meant that images of sexually abused children derived from a range of sources, and that members were influenced by their propensity to communicate and discuss with other members their various exploits including the latest images of children regardless of the violation of trust of the victims. Webber (2001:2), a computer consultant, noted that:

> The main purpose of the club was the exchange of paedophile materials, pictures, movies, information and most appalling of all - sounds, terrible, terrible sounds. But while they were exchanging the pictures they could sit inside this chat room and exchange information (cited in Corbin 2001:2).

Central to this perspective is the idea that criminal behaviour was facilitated through group association. Forde and Patterson (1998:3) note in an exploratory observation of paedophile Internet activity that ‘paedophiles appeared eager to demonstrate their prowess to their peers ... [through presentations which] appeared to provide peer group status’.

The techniques used by members of the W0nderland Club may be viewed as complicated due to the high level of secrecy and trust between the members involved in transferring images of sexually abused children anonymously and with caution. Furthermore, as a highly organised group, trust and secrecy played a key role in the ongoing participation of individuals in the W0nderland Club (Forde and Patterson 1998), while a violation of trust was central to gaining access to pictures and images of children. However, the techniques to transmit and discuss images of sexually abused children appeared simple. This was due to the fact that once a person was accepted into the club, trading was much easier as it connected a member to potentially hundreds of other members worldwide, and there appeared to be a sense of community amongst the

from Russia ‘... kidnapped children from orphanages and filmed them being forced to have sex, sometimes raping them and torturing them to death on camera’ (Graff 2000:1-2).
members. The direction of motives also appeared to change due to the members’ acceptance in this group structure.

Heimbach (2002:3) argues:

Those who trade in child pornography participate in organised (like “candyman”) or informal (chat rooms, F-serves, news groups, bulletin boards, Web sites etc.) networks of like-minded individuals, which serve as support groups. That these individuals can easily find, identify with, correspond with, and trade child pornography with each other, gives them comfort in the fact that they are not alone and tends to validate their offending behaviour. They feel that they are part of a vast network of like-minded people who believe it is acceptable to engage in sexual fantasies about children ...

This appears certainly the case with members of the W0nderland Club’s online activities. These members appear to have been drawn together through their fascination with children as young as three years of age. The Internet provided the forum for these illegal activities to take place and the communication between these members was instrumental in the ongoing participation in this criminal behaviour.

The members of the W0nderland Club believed that the Internet would provide them with a sense of security, anonymity and a shield from law enforcement agencies. Jerry Jordan (2001:6), a US Customs officer, expressed the view that ‘...William Rosa would [not] have got involved in this had it not been for the Internet. The anonymity that he used, or thought he had, allowed him to cross that line and enter into this world hiding behind the fictitious name’ (cited in Corbin 2001). This sense of anonymity demonstrates that a high level of trust was significant for the distribution of images and for the continued association of the group, which would be under threat from law enforcement agencies due to the criminal nature of its activities.

While the examples of paedophile rings and associations of child pornography aficionados above show support for Sutherland’s theory, it is important to note that online exploitation of children does not always occur through group association and learned behaviour. The National Juvenile Online Victimisation (N-JOV) Study, which collected data on the characteristics and number of arrests for Internet sex crimes against children, revealed that 97 per cent of offenders acted alone (Wolak et al.
2003:xi). The arrest of a 64-year-old male, Lindsell, in the United Kingdom also shows that lone individuals carry out Internet sex crimes against children and youth. According to reports, Lindsell allegedly preyed on more than 70 young girls in Internet chat rooms across the globe and was apparently drawn to the Internet by the excitement of chat rooms (Morris 2003). Lindsell’s alleged behaviour led to a range of Internet sex crimes, such as attempted abduction, harassment and gross indecency to a 16-year-old child (Morris 2003:5).

In one case prosecuted in the United States, Bloom v. Commonwealth of Virginia (542 S.E.2d 18, 2001 Va. App. Lexis 91 (Ct.App. Va 2001)), the defendant, a 28-year-old male, was convicted of attempting to solicit a 13-year-old female over the Internet. Bloom contacted the young girl through a chat room and after communicating with her, arranged to meet in a public place. The young girl’s mother alerted authorities to the proposed arrangement, which led police to pose as the young girl and later led to Bloom’s arrest. The defendant was later charged and convicted. These two examples demonstrate that lone individuals do prey on young children on the Internet, which challenges the link between group association, learned behaviour and Internet sex crimes as a general theory.

5.3.4 Internet Fraud

Fraud is recognised as one of the most common forms of crime committed on the Internet due to the diverse ways in which it is carried out and the availability of a potential number of targets or victims (Grabosky et al. 2001; Smith and Urbas 2001; Newman and Clarke 2003; Beales 2004). According to Beales (2004:13), ‘Internet-related fraud complaints exceeded other fraud complaints for the first time last year, comprising 55% of all fraud complaints’. These statistics are consistent with The Federal Trade Commission’s report, which found that ‘... 2003 was the first year in which consumers reported that the Internet outstripped the telephone as the point of their first contact with a fraudulent scheme’ (Beales 2004:13). This suggests that the Internet has become a new medium for the commission of a broad range of frauds.

---

86 Wolak et al. (2003:7) defined offenders ‘... as alleged perpetrators of crimes who were arrested’.
Traditionally, lone individuals carry out most forms of electronic fraud (Grabosky et al. 2001); however, some forms of fraud may be carried out by groups. One of the first high-profile cases of computer fraud that involved group association occurred in the early 1990s. Vladimir Levin (R v Governor of Brixton Prison and Another Ex parte Levin [1997] QB 65), the leader of a Russian-based hacking group, gained unauthorised access to Citibank’s computer systems in the United States from his computer in St Petersburg for the purposes of obtaining illegal funds from Citibank accounts. Levin and his co-conspirators set up bank accounts in various countries to transfer $10 million from Citibank’s computer network for distribution into these accounts (Smith et al. 2004).

The Russian hacking group consisted of five members for whom communication and the exchange of information appeared crucial in carrying out the fraud. Levin’s co-conspirators travelled abroad to set up numerous bank accounts while Levin could monitor accounts of companies via his computer to transfer funds. It appeared that each member of the group provided skills and used techniques that were intrinsic to planning for the successful commission of the fraud. Communication, criminal knowledge, and motives of the members therefore supported their activities. This example of Levin and his accomplices illustrates support for differential association because criminal definitions were a common element among the members and as Sutherland (1947) would argue, people learn to be deviant around others who support norm violations. This example shows, however, that it is difficult to determine whether these members had criminogenic attributes prior to carrying out this fraud.

This thesis suggests that global access to the Internet provides unprecedented opportunities to develop networks through chat rooms and e-mail, which may increase the likelihood of being involved in Internet fraud. Williams (2001:1) argues that ‘...criminal organisations tend to be exceptionally good at identifying and seizing opportunities for new illegal enterprises and activities’. The Internet and the continuing growth of electronic commerce offer enormous prospects for illicit profits from fraud. Although the diverse variety of Internet fraud committed around the globe has made it challenging to track its changing nature and type of offender or network, there may be other forms of fraud that support Sutherland’s theory of group association and learned behaviour.
CHAPTER 5: THEORIES OF CRIME AND CRIMINALITY AND THEIR RELATIONSHIP TO THE INTERNET

(a) Internet Auction Fraud

Online auctions have become an increasingly popular form of e-commerce transactions since the mid-1990s. The popularity of online auctions equates to an increase in the number of transactions, which exceed 1 million per day and an increase in the number of participants to over 25 million worldwide. However, as the number of participants increases, it appears that criminal opportunities mirror this increase. Since 2001, auction fraud has been recognised as the most common type of Internet fraud involving consumer-to-consumer and business-to-consumer transactions (IC3 2004).

Most investigations of auction fraud have resulted in individual prosecutions with little available evidence suggesting group involvement and the influence of learned behaviour. A report on auction fraud found that in 2001 ‘... 84 per cent of the subjects are listed as individuals and the remaining 16 per cent are businesses’ (IFCC 2001:10). In the United States, a 43-year-old man from Ohio, Jeffrey P. Butcher was found guilty of multiple offences including wire fraud, identity theft, and credit card fraud. Butcher sold computer equipment through eBay, received payment from 43 successful bidders but failed to deliver the goods. The approximate losses from Butcher's fraudulent scheme totalled US$30,653.76. (White and Kern 2004:1). Butcher effectively deceived eBay customers because he knew the goods would never be delivered, although he continued to advertise them for the purpose of financial gain.

In United States v. Denlinger (No. 00CR573IEG, S.D. Cal. filed Feb.28, 2000), the defendant offered Beanie Babies for sale through online auction websites, however, after receiving payment from the purchasers, the goods were never received (Rusch 2001:2). In this example, the defendant acted alone and attempted to evade victims by using techniques that prevented victims from contacting him by constructing various aliases (Rusch 2001).

Two techniques commonly used to carry out online auction fraud both during and after the bidding process are bid shielding and shill bidding. Bid shielding involves collusion of bidders with the objective of increasing the value of the bids during an auction. For example, a person places a low bid and the co-
conspirator places a high bid with the intent of putting off other bidders from entering the auction. The high bid is withdrawn moments prior to close of auction thus allowing the low bidder the item (Albert 2002).

Shill bidding refers to the use of one or more false bids most commonly through a group of individuals with no intent of purchasing the item. The people involved most commonly adopt different user names for the purposes of bidding on co-conspirators items or their own item. This technique is used to drive up the price for the seller to gain financially from the transaction. Collusion in online auctions is difficult to investigate in a timely fashion given the huge volume of auctions occurring daily (Albert 2002). However, these techniques may demonstrate that learned behaviour and association influences criminal behaviour in online auctions.

Kenneth Walton along with two co-defendants, Scott Beach and Kenneth Fetterman, were charged with wire fraud and mail fraud in relation to shill bidding through an online auction. Walton, along with Beach and Fetterman, defrauded eBay users by misrepresenting the nature of the artwork auctioned. The defendants devised a plan that appeared to suggest to potential bidders that a well-known American artist painted the work. Further, the defendants created accounts that showed that bidders were in fact related to the artist. This technique was used to create the impression that the works were indeed original (USDOJ 2001b).

Techniques used by the defendants included: creating false identities to increase the auction price of the works, providing false information on eBay’s feedback form, and placing fraudulent bids. The defendants operated the scam over an 18-month period. This example demonstrates that groups can carry out auction fraud although in most cases, individuals act alone. Furthermore, it shows that differentially associating with others who have favourable attitudes to crime may influence one’s behaviour.

(b) Internet Securities Fraud

Share-market manipulation schemes are traditional forms of crime although the Internet has expanded the opportunities to reach new targets. This can be
achieved by creating new ways of manipulating the market through technology and the different way information is disseminated: e-mail, websites, bulletin boards, spam, hyperlinks, and new services. The most common type of share-market manipulation scheme is ‘pump and dump’. This scheme involves disseminating fraudulent and misleading information with the objective of driving up the price of the stocks of shell companies then immediately selling off their share of the stocks to gain from the financial transaction, prior to the stocks falling back to their usual level. People who purchase the stock during this period become unwitting victims of the scheme once the price falls (USDOJ 2001b:4). ‘Slur and slurp’ is a scheme used to talk down the value of the stocks while purchasing shares at the low end of the market thus increasing the opportunity for the stocks to rise and profit from the transaction. The use of these schemes often involves misinformation, rumour and hyperbole (Grabosky et al. 2001).

The Securities and Exchange Commission (SEC) conducts annual Internet sweeps, which have uncovered a myriad of online fraudulent transactions, involving individuals and small entities. For example, in SEC v. Thor Equity Group, LLC and George E. Mahfouz, Jr., (Civ. No. CIV 00-1699-PHX VAM (D. Ariz.)), the SEC alleges that Mahfouz, Jr, and his investor relations firm, Thor Equity Group, publicised securities of CancerOption.com, Inc. based on false financial projections and later sold a number of the stocks at inflated prices for financial gain. Analysts were provided with false information by CancerOption and Mahfouz Jr. and later that information was posted on CancerOption’s website. Furthermore, the SEC alleges that touters were hired to disseminate the false information to drive the price of the stocks up. The Chief Executive of CancerOption, Arnold C. Takemoto, was apparently aware of the false information in the reports and did not alter the information or the website.

In another case of ‘pump and dump’, a corporate insider, P. Joseph Verticci and Bruce Straughn, a stockbroker were alleged to have created and disseminated false information in order to sell shares for a profit of an unregistered company. The SEC alleges that the two defendants sold securities
of an American company, Interactive MultiMedia Publishers, Inc. (IMP) to the public, which were worthless. It was further alleged that the defendants arranged for material to be disseminated on the Internet to publicise the company in the hope of boosting the share price. Verticci and Straughn engaged touters who were paid compensation through shares. Once the shares rose, the defendants along with the touters sold their shares for a profit. The company ceased trading once the stock collapsed (SEC 1999:2).

This example demonstrates the ease with which criminal behaviour occurs through intimate groups, and the likelihood that positive attitudes towards cyber crime influence the behaviour of others. It is difficult, however, to establish whether criminal behaviour was learned in interaction with other persons in a process of communication or whether other variables could explain their involvement.

(c) Additional Forms of Internet Fraud

Italian police uncovered a major criminal network that involved online banking fraud with the arrest of 21 people in 2000. Willan (2000:1) reported that:

Members of a criminal group with links to Cosa Nostra allegedly succeeded in “cloning” an online branch of the Banco di Sicilia and were preparing to remove funds from an account belonging to the Sicilian regional government ...

Members of this criminal group involved bank and telecommunications staff. These individuals were central to the organisation and execution of the fraud because of its complexity and large-scale operation. This example shows the way the Internet can act as a conduit between members of a network using the means of communication and association to implement the fraud. Although this example does not illustrate learned behaviour, it emphasises the role of group association and criminal behaviour.87

---

87 There are many cases involving fraud where prior knowledge of the bank’s computer system has been central to the commission of the crime (R. v. Thompson [1984] 1 WLR 962; Director of Public Prosecutions v. Murdoch [1993] 1 VR 406).
Associations formed between members of the networks appear to be a central element in the commission of fraud. For instance, Madsen (2004:2) points out that ‘the fraudsters ... are aided and abetted by associates who have obtained employment in banks, post offices, and passport and taxation agencies’. This example supports Sutherland’s differential association theory and highlights the way the Internet is used to not only develop these associations but also maintain quick communication through e-mail.

Another type of Internet fraud that engages groups of individuals is the Nigerian advance fee scheme.\(^8\) The Nigerian advance fee scheme is often carried out on a global scale with the involvement of numerous individuals. Cells have been identified as operating around the globe, which rely on other individuals to carry out the fraud successfully. For instance, a process of communication appears intrinsic to the success of the fraud, that is, the communication between the potential victim and the offenders, such as overseeing the transfer of money and delivery of goods and payment between the members of the network. Sutherland’s (1947) point that ‘the principal part of the learning of criminal behaviour occurs within intimate groups’ may be difficult to apply to this example, however, because of the large scale and global dispersion of members involved.

An example that demonstrates the case with which people can be recruited to participate in Internet fraud involved students who were being paid to transfer funds to Internet bank accounts for an organised criminal network. According to police reports ‘... Sydney students have been recruited by criminals to steal money in an Internet banking scam which may have netted millions of dollars’ (ABC Online 2005:1). ABC Online (2005:1) reports that:

> Investigators say high school or TAFE students who are nick-named “money mules” are paid to illegally transfer money ... [According to detectives] the money is then transferred into the mule’s own

---

\(^8\) Smith et al. (1999:2) note that the nature of the advance fee scheme is that fraudsters ‘... generally describe the need to move funds out of Nigeria and seek the assistance of the victim in providing bank account details in an overseas country and administration fees needed to facilitate the transaction’. The victim is encouraged by the attraction of a commission.
account, withdrawn and sent to overseas crime syndicates which may have links to the Russian mafia.

These fraudulent transactions have targeted individuals and companies with an estimated amount of AUS$500,000 in the first series of offences. Detective Stirton maintains that 'just as the initial starting point of this investigation, we're aware of 61 individual victims and companies, however that is expanding almost on a daily basis' (ABC Online 2005:1). This example shows that the Internet has provided the means to recruit willing participants from around the globe in the hope of financial gain. Recruiting people from around the globe via the Internet may be a deliberate technique used to thwart investigators, given the time and resources required to investigate Internet fraud and the global cooperation from overseas counterparts that may be required.

The lack of successful prosecutions makes it difficult to know whether these individuals were linked to criminal activity prior to committing fraud on the Internet. Furthermore, the lack of empirical research on fraud networks also contributes to the difficulty of adequately assessing the applicability of differential association theory to a range of Internet frauds.

The Nigerian fee scheme does not always involve groups of people that are intimately connected and whose members learn behaviour from others within the scheme. Furthermore, not all forms of fraud are carried out by groups of people. According to Power (2000:16), the organisational characteristics of fraud can include small organised crime groups or those who act as loners. It is important to recognise that many other forms of fraud such as auction fraud and Internet securities fraud are also carried out by lone individuals and are less inherently social than hacking groups and paedophile rings, and therefore differential association could not be applied to all forms of fraud as a general theory.

5.4 STRAIN THEORY

Strain theory, as developed by Merton (1938), concentrates on a breakdown in the relationship between cultural goals and the legitimate means to achieve them.
Among the elements of social and cultural structure, two are important ... the first consists of culturally defined goals, purposes and interests and aspirations [these can include success, material possessions and prestige by legitimate means]. The second phase [institutional norms] ... defines, regulates, and controls the acceptable modes of achieving these goals (Merton 1938:672)

According to Merton the means to attain goals is usually through the family, education, and the workplace. Merton’s (1938) theory suggests that at times, however, there is a gap between the goals and the legitimate means of attainment, which can lead individuals to seek out goals through violation of the law. These modes of adaptation are inherently linked to the social structure, according to Merton who concentrated on economic activity and the link between wealth and success. Despite Merton’s emphasis on the lower classes, Chapter Three showed that in general, strain theory could apply to different types of white-collar crime.

The Internet, as discussed in Chapter Four, provides a plethora of opportunities for crime, regardless of age, class or status of the offender. This provides an ideal context to examine Merton’s theory. Empirical studies that have applied Merton’s theory to different forms of cyber crime include Rustad’s (2001) study, which analysed criminal activities in cyberspace, in particular, the hacking subculture, and Kern and Pfeiffer’s (2001) study, which analysed 860 USENET messages to explore what sociological theories may explain the behaviour of software pirates. In general, Rustad’s (2001) study showed support for Merton’s theory. Two of Merton’s modes of adaptation are reviewed here: innovation and rebellion.89

5.4.1 Innovation

Merton’s innovators accept the cultural goals of success and wealth although they reject the institutionalised or legitimate means of achieving them and attempt to attain the goals through illicit innovation (Merton 1938). Chapter Three showed that Merton’s concept of innovation could apply to crimes such as fraud, embezzlement, and espionage because the predominant goal is financial gain. This section will set out to demonstrate whether hacking, piracy, Internet pornography, Internet securities fraud,
and phishing are carried out by innovators to attain goals through illicit forms of innovation.

(a) Hacking

Traditionally, the term ‘hacker’ referred to computer enthusiasts who built and improved computer programs and systems in universities such as MIT and Stanford. However, as the concept changed over time, so too have the activities and motivations of hackers. Among the wide range of motivations of hackers, financial gain can be applied in the context of hacking.

A lone hacker, Markus Hess, who went by the code name ‘Hunter’, gained unauthorised access into the Lawrence Berkeley Laboratory’s computer system to obtain sensitive United States military and security information. Hess was funded by the KGB and reported information he illegally downloaded from the laboratory’s network. Hess used his technical knowledge as a hacker to obtain information in return for money and was rewarded according to the type of information he provided to the KGB and the techniques used. Stoll (1989:365) notes:

The deal was made around 30,000 Deutschmarks–$18,000–for printouts and passwords ... Even more important to the KGB was obtaining research data about Western technology, including integrated circuit design, computer-aided manufacturing, and especially, operating system software that was under United States export control. They offered 250,000 Deutschmarks for copies of Digital Equipment’s VMS operating system.

It appears that this presented an additional incentive for Hess as his activities were determined by the type of information he gathered at the expense of rejecting the legitimate institutionalised means of attainment. The activities of Hess illustrate the rejection of institutionalised means to attain information legally while accepting the cultural goals of wealth.

89 Merton’s (1938) three remaining adaptations; conformity, retreatism and ritualism are not examined in this section because they appear to be explanations of compliance or withdrawal rather than explanations of criminality.
In another example, Levin and his co-conspirators in the early 1990s appeared to accept the goals of wealth and success at the expense of hacking into Citibank’s computer systems for the purpose of transferring US$10 million to bank accounts set up by members of the group (see Smith et al. 2004). Levin and his co-conspirators clearly rejected the institutionalised means of attainment, by hacking into the bank’s servers with the prospect of gaining millions of dollars.

A citizen from Kazakhstan, Zezev, attempted to extort US$200,000 from the American corporation, Bloomberg L.P. along with his co-conspirator, Yarimaka. The two defendants planned to hack into the company’s computer network stealing confidential information for the purposes of extorting money and threatening to release the information to Bloomberg’s customers and to the media if the payment was not met (Smilon et al. 2003).

Zezev used his knowledge and position as chief information technology officer at Kazkommerts Securities to obtain access into Bloomberg’s network. According to evidence at trial, ‘… Bloomberg provided database services to Kazkommerts. As a result, Kazkommerts was provided with Bloomberg’s software needed to gain access to Bloomberg’s services over the Internet’ (Smilon et al. 2003:1-2). This provided the means for Zezev to manipulate Bloomberg’s software to obtain unauthorised access into their computer network and pave the way to plot the extortion (Smilon et al. 2003:2). Furthermore, it highlights the ease with which trust was violated in order to gain information in furtherance of committing extortion.

These examples demonstrate that hacking is used to achieve financial success illegitimately through different methods and crimes. It is difficult to ascertain whether strain influenced the decision to illegally access computer systems, however. While the illegal entry into computer systems provides an alternative means for innovators to carry out their crimes, not all hacking is carried out for financial gain. Denning (1999:46) cites an example of a hacker, Bevan, who penetrated the United States Air Force and NASA’s computer system, and who maintained that he was motivated by curiosity rather than financial gain. Sub
section 5.4.2.1 demonstrates that hackers are also motivated by revenge and the challenge, and carry out their crimes through protest.

(b) Internet Piracy

The situational and ethical factors and motivations of pirates have been an enduring topic of interest over the past decade (Glass and Wood 1996, Sims et al. 1996, Kern and Pfeiffer 2001, Rumbough 2001, Kini et al. 2003). The findings have uncovered a myriad of factors that influence people to engage in piracy: situational (such as low incidence rate of being caught, high cost of software, low level of punishment, and the perceived absence of clear codes of conduct) (Harrington 1989); association with peers who engage in piracy (Lodgson et al. 1994; Skinner and Fream 1997; Rahim et al. 2001); those that did not consider piracy as unethical behaviour were more likely to engage in it (Solomon and O’Brien 1990; Glass and Wood 1996); low self-control (Higgins and Makin 2004); and economic strain (Kern and Pfeiffer 2001).

Given that several studies have largely focused on the use of piracy among college students (Hollinger 1993; Sims et al. 1996), few have explored whether strain influences piracy. Kern and Pfeiffer’s (2001) study showed that economic strain can influence software piracy given the estimated value of programs and the limited financial means to access these programs legitimately. The data collected by Kern and Pfeiffer showed that approximately 18 per cent of programs have a value of US$500 and seven per cent have a value in excess of US$1000. According to Kern and Pfeiffer (2001:4) ‘in place of cost, this relative inaccessibility may also cause strain in conjunction with strong perceived pressures to acquire the program for personal use’. The relatively high levels of piracy among students may be partially explained by Merton’s theory.

The increase in piracy rings operating on the Internet has shown little evidence to suggest that strain plays a significant role in the proliferation of piracy. For example, it has been recognised that many white-collar workers, including executives, within the music industry appear to be major players in the piracy rings. According to the US Department of State (2001:5), ‘United States
Customs has identified members who are corporate executives, computer network administrators at major United States universities, [and] employees of large hi-tech companies ...'. This would appear to dismiss the likelihood that these individuals lack the legitimate means of attaining success and wealth.

It has also been established that members of piracy rings are motivated by factors other than financial gain, such as the challenge, recognition, the thrill, ego, and reputation. The US Department of State (2001:5) maintained that 'earning an online reputation as the fastest to steal, 'crack', and releas[ing] high-quality, pirated software over the Internet is most important to them'. This analysis suggests that strain is not a major variable in explaining the behaviour of Internet pirates although some examples do support it.

(c) Child Pornography

The Internet has furthered the availability of illicit images of children to a global market, which has resulted in a rise in the number of pornographic rings and individuals accessing and trading images of children. There are examples to demonstrate that individuals and groups of individuals reject the institutionalised or legitimate means of achieving wealth, but attempt to do so through illicit innovation of child pornography.

A United States investigation into a child pornography racket, dubbed Operation Avalanche, uncovered one of the largest illegal commercial enterprises involving child pornography on the Internet. Landslide Productions, Inc., engaged in advertising and distributing child pornography and offered subscriptions to in excess of 250 websites and collected 300,000 subscribers around the globe. Each customer was billed US$29.95 monthly to access these sites. Thomas and Janice Reedy, the masterminds behind the illegal ring collected approximately US$1.4 million per month from the enterprise (Weiss 2003), thus attaining the cultural goals of success and wealth through illicit innovation.

A 53-year-old man created and used misleading domain names for financial gain, which exposed young children to pornography. Approximately 6000 domain names were registered by the defendant as misspellings of popular
websites. Beales (2004:1) notes that, '... surfers who looked for a site, but misspelled its Web address, were taken to the defendant's sites'. The techniques the defendant used meant that children were logging into pornographic websites because he felt children were easier to target. The scam resulted in a financial gain of close to US$1 million because each time a person accidentally logged onto the website, the defendant received money (Keeley 2004).

Not all forms of child pornography on the Internet are motivated by greed. A number of child pornography rings trade pictures of children for sexual gratification and power. For example, access to the W0nderland Club was gained through private invitation or by providing 10,000 images of children to club members (Corbin 2001). It appeared through investigations that financial gain did not play a role in the motivation and ongoing participation of members of the club. Similarly, a global underground network of adults who traded in child pornography were motivated by sexual gratification rather than financial gain. According to reports, money was not exchanged for the pornographic material (Savino 2002). These examples show that innovative means are used to trade in child pornography; however, obtaining the material illegitimately for financial gain is limited because members of these groups are motivated by factors other than financial gain.

(d) Internet Securities Fraud

Low income is not the only indicator of strain. Middle class people who want more than they can afford with their legally obtained wealth are also 'strained'. People of all income levels use innovative methods because they can't gain wealth through legitimate investments.

The SEC (2000b) investigated a case of securities fraud against Christopher Hastings, who allegedly touted the stock of ten issuers. Hastings maintained a website that contained a free online newsletter of Internet tips and information on stocks and shares as well as posting misleading financial tips on bulletin boards and e-mail. The SEC (2000b:3) maintained that the misleading and false information included '... the track record of his stock picks, which he claimed
averaged a 410 percent increase after his touts ... [and] misrepresented his trading intentions ...'.' Furthermore, the SEC alleges that on two occasions, Hastings sold the touted stock he owned that resulted in a profit of US$70,309.

Hastings had no previous experience in the financial markets and was employed as a bus mechanic at the time of maintaining the website. This example demonstrates the ease in which people can set up a website on the Internet and provide false and misleading information for the purposes of financial gain. In addition, the opportunity to gain financially may have motivated Holdings to use the Internet as a means of financial gain illegitimately. Because 'no one knows you are a dog on the Internet', the Internet makes opportunities available for people to commit business crime who do not have stature in the business community.

A former chairman of a US company, Systems of Excellence, Inc. (SEXI) Charles Huttoe, SEXI's auditor, publisher, Theodore R. Melcher, Jr., along with three co-conspirators were charged as a result of their involvement in an Internet securities scam. It was alleged that Huttoe gave 250,000 shares of SEXI to Melcher, Jr., publisher of a stock tip Internet publication in exchange for touting the stocks of SEXI. Melcher Jr. promoted the stocks over a three-year period through the online newsletter and on bulletin boards (Kassler 2002). The scam resulted in more than US$10 million in illegal gains. The six individuals involved pled guilty to conspiracy to commit securities fraud. This example illustrates that this type of crime is not only committed by those among the lower classes.

The SEC's annual Internet sweeps reveal a number of interesting points. First, that a number of offenders of online securities fraud have little or no prior knowledge or expertise in the securities industry. For example, a number of individuals involved included a university student, driver, and bus mechanic. The lack of knowledge and expertise in the security industry appears to suggest that the Internet has opened up opportunities to create new and different ways to carry out traditional forms of securities fraud and that these individuals may be involved in groups in order to successfully carry out the crime. Second, a number of actions involved foreign individuals and entities reaching United
States investors through the Internet. This may suggest that the Internet has bridged communication between prospective investors and scammers, some of who may operate in countries where laws relating to online securities fraud may not exist.

(e) **Phishing**

‘Phishing’ is one of the techniques or methods used to trick users into revealing personal information, passwords, and credit card and account numbers through e-mail, spam, and most commonly through counterfeit websites for financial gain.\(^90\) Counterfeit or bogus websites imitate genuine websites for the purposes, inter alia, of gaining sensitive personal and financial information in furtherance of criminal activities such as fraud and extortion.\(^91\)

More recently, criminals have used their technical skills to transfer the legitimate webpage of a bank and input a box onto the main page to dupe victims into believing it is the legitimate site. Sullivan notes (2004:1) that ‘FBI officials suspect the [phishing] scammers’ growing skill is a sign not of a learning curve but of the introduction of more savvy and experienced criminals into the fraud schemes’. For example, it is not uncommon for criminals to replicate known websites such as banks using the same graphics and language.

Other techniques used include constructing a website to imitate another while providing links to the original legitimate bank site. This technique attempts to alleviate any suspicion on behalf of the customer by having the option to click onto a link, which allows them to be logged onto the legitimate site for a short period and then transfer back to the illegitimate site unbeknownst to the victim. Phishers also use misleading and false statements and claims to potential victims, which can create the impression that their personal information may be at risk or alternatively that their credit card information has been compromised.

---

\(^90\) The Federal Trade Commission (FTC) (FTC 2004) defines phishing as ‘… the use of spam directing consumers to update or validate their confidential payment information on copycat Web sites that appear identical to the sites of the legitimate companies with which they do business’ (cited in Beales 2004:5).

\(^91\) Grazioli and Jarvenpaa (2003) term this type of fraud “page-jacking”.
Papierniak, a 20-year-old college student was charged with wire fraud after applying phishing techniques to Internet users. Papierniak sent e-mail messages with an attached program that purported to be a security update from PayPal. The attached program secretly monitored information such as user names and passwords to the defendant, allowing him to collect in excess of US$30,000 from the scam (Hansell 2004).

Zachery Keith Hill, a 20-year-old male from the United States was sentenced to 46 months in prison for deceptive and unfair practices using the Internet. Hill used a range of phishing techniques to deceive America Online (AOL) and Paypal customers into providing personal and credit information for financial gain. For instance, messages were sent to consumers maintaining that their billing information relating to their AOL account needed to be updated or corrected. If consumers did not respond to the e-mail, the e-mail suggested that they risked possible termination of their AOL accounts. One of Hill’s messages stated:

... we have to ask all our members for updated/correct billing information. Please be advised that this is mandatory. If we do not get your updated billing information, your account will be revoked and put under review and may be cancelled (cited in Kovacic 2003:4-5)

As a result of the scam, Hill accessed 473 credit card numbers, 152 bank account numbers and 566 usernames and passwords for Internet accounts. More than US$45,000 was fraudulently obtained to purchase a range of goods and services (Kovacic 2003). These two cases support the view that innovation is applicable to phishing because the legitimate means of obtaining wealth is rejected.

In summary, the innovative mode appears to explain crimes of acquisition on the Internet. Examples to support innovation and Internet crime include those crimes where greed is one of the predominant motivations: hacking, Internet piracy rings, sale of pornography, securities fraud, and phishing.

Innovation does not explain all forms of cyber crime, such as the Morris worm, DDoS (Distributed Denial of Service) attacks and the piracy of LaMacchia,
because these forms of cyber crime appear to be motivated by intellectual curiosity or a sense of defiance rather than financial gain. Furthermore, it is difficult to demonstrate that individuals from the lower classes are most vulnerable to commit cyber crime. This appears to suggest that strain through innovative means may not be a dominant explanation of a range of cyber crimes.

5.4.2 Rebellion

Rebellion occurs where both the culturally held goals of success and wealth and the legitimate means of attaining them are rejected in favour of protest. Individuals who may be amenable to the rebellion mode of adaptation include those who use the Internet to develop strategies for criminal activities such as hackers (disgruntled employees who steal or vandalise), protesters against Microsoft, and Internet pirates.

(a) Hacking

Disgruntled employees who illegally gain access to computer networks for the purposes of stealing or damaging information or data are representative of this mode of adaptation. For example, Meydbray, a former IT Manager of a software company, illegally gained access to the computer network of his former employer intentionally causing damage to it. Meydbray was employed at Creative Explosions for approximately two years prior to the termination of his employment. It was alleged that less than two weeks after his termination, the defendant illegally gained access to the computer system of Creative Explosions, accessing e-mail accounts of the President of the company, changing passwords on e-mail accounts that resulted in the rejection of e-mails, and intentionally causing damage by deleting the company’s domain web page (Krotoski 2005). The case is currently before the US courts.

Patrick Angle, a former employee of high-tech company, Varian Semiconductor Equipment Associates, Inc. was charged with hacking and causing considerable damage to the company’s computer systems. It was

92 In the case of United States v. LaMacchia (871 F. Supp. at 535 (D. Mass. 1994)), LaMacchia’s case
alleged that Angle became disgruntled with his employment in September 2003 and was notified that his contract would be terminated 4 weeks later. On September 17, it was further alleged that Angle logged into the company’s computer network from his home and intentionally deleted the source code for software that he and others were developing. According to reports, Angle ‘... then covered his tracks by editing and deleting some of the computer logs of activity on the server and by changing the server’s root password to make it difficult for other Varian employees to log on to the server and assess and repair the damage’ (Sullivan 2004:1).

Hackers also target Microsoft Corporation in protest. Microsoft’s Windows operating system is one of the most targeted systems because it operates in excess of 90 per cent of personal computers around the globe, thereby increasing the impact and penetration (Bink 2003). The vulnerabilities in a number of the programs that run Microsoft create opportunities for its exploitation (Bink 2003). A number of viruses and worms that have been unleashed on computer systems over the past two years appear to be aimed at Microsoft’s Windows operating system.

The United States Government’s antitrust case against Microsoft may have also increased the risk for Microsoft as a target. Festa (2000:3) suggests that ‘the value of Windows source code has become an issue in the government’s antitrust case ...’. An intrusion into Microsoft’s computer system in 2000 revealed the vulnerability of its source code to theft. Reports suggested that those involved were based in St. Petersburg, Russia.

These examples demonstrate that the rebellion mode can be applied to disgruntled employees who intentionally cause damage to computer systems. The Internet has furthered the opportunities for disgruntled employees to reject the legitimate means to attain wealth and success and do so in protest. Substituting the production of logic with a logic bomb is a classic instance of Merton’s rebellion.

was dismissed and his actions led to the enactment of the No Electronic Theft Act.
(b) Internet Piracy

The example of LaMacchia (871 F.Supp. 535 (D.Mass. 1994)) who established a bulletin board for people to access and exchange copies of software applications and computer games free of charge is an example of rebellion. LaMacchia did not profit from his activities.

A number of Internet piracy rings reject the legitimate means of attaining software, instead stealing and releasing it on the Internet. Many of these piracy rings do not profit from their activities and as a means of protest against the large multinational companies distribute it freely over the Internet. The non-financial motivations to pirate vary: the challenge, thrill, reputation, ego, and peer recognition. While the behaviour of some pirates can be explained through the rebellion mode, others pirate software for financial gain. It is estimated that the global pirate music market in 2000 was US$4.3 billion (Berman 2002:2).

There are alternative motivations underlying criminal behaviour that are not predominantly explained by Merton's means of adaptation. This chapter has established that cyber crimes, such as hacking, piracy, and child pornography can be motivated by revenge, thrill seeking, peer recognition, and intellectual curiosity (see McDevitt et al. 2002; Cruise 2003). Thrill seekers are rejecting culturally approved success goals and replacing them with another goal. In addition, the rebellion mode of adaptation does not explain the role group processes play in deviant behaviour and the accessibility of crime. Accessibility can play a predominant role for different forms of crime committed on the Internet, such as fraud and money laundering.

5.5 TECHNIQUES OF NEUTRALISATION

Techniques of neutralisation proposed by Sykes and Matza (1957) are processes whereby offenders rationalise their conduct after the fact, or overcome any inhibition prior to committing an offence by justifying their behaviour. The following will analyse Sykes and Matza's five techniques of neutralisation to determine whether their theory can extend our understanding of criminal behaviour on the Internet.
5.5.1 Denial of Responsibility

If an offender lacks any responsibility for his or her actions, the effectiveness of self or others as a restraining influence is minimised (Sykes and Matza 1957:667). According to Sykes and Matza (1957:667), ‘the delinquent approaches a ‘billiard ball’ conception of himself in which he sees himself as hopelessly propelled into new situations’. This justification limits the ‘personal accountability’ of the offender by pursuing social forces as the primary cause of criminal behaviour rather than placing accountability on the offender. This technique allows offenders to excuse themselves from any culpability for their actions.

(a) Hacking

Some defendants may raise the issue of mental health problems such as computer and Internet addiction as mitigating factors that entail a denial of responsibility (Smith et al. 2004:140) (see also Dreyfus 1998; Guardianbooya 2001). Internet addiction was used as a defence in the Bedworth case. Bedworth, an Edinburgh University student, was charged in 1993 for gaining unauthorised access to various high-profile computer networks and systems and was acquitted by a jury ‘... on the grounds of a purported clinical addiction to hacking, which meant that he had not formed the requisite criminal intent’ (Smith et al. 2004:140). Mr Bedworth’s barrister argued that Mr Bedworth had grown up with computers and was affected by them. ‘When a kid’s best friend becomes a computer rather than a member of their family you are courting trouble’ (Harris 1993:1 cited in Taylor 1999:50).

Aaron Caffrey, a teenager from the UK was charged with launching a denial of service (DoS) attack against a Port of Houston computer network in Texas. Caffrey argued that he was not responsible for carrying out the attack from his personal computer by maintaining that it was hijacked by a rogue trader and used as the base for the attack (Jaani 2003:1). It was reported that prosecutors failed to establish a motive and intent for the attack although it was discussed that Aaron was a founding member of a British hacker league (Jaani 2003). Mr Caffrey’s barrister argued that his client insisted he ‘... was a victim of a criminal act rather than being a criminal himself’ (Jaani 2003:2). Caffrey
denied responsibility and his defence team successfully used the Trojan horse defence; a jury later acquitted him.

(b) Internet Piracy

Some Internet pirates may argue that the high price of music, software, and movies has forced people to download them illegally. Seale et al. (1998:29) suggest that ‘... people who report an inherent unfairness in the price or proportional value of software, maybe more likely to engage in piracy’. A US national online poll, which was conducted on 1183 youths aged 8-18 about their behaviour and attitudes towards copyrighted materials, found that just over half felt that it was okay to download the software because they did not have the money to pay for it. In addition, 19 per cent of respondents revealed that no one ever told them not to do it (Harris Interactive 2004:5). This behaviour excuses the youths of any responsibility by claiming that they were unaware of the legal implications.

Not all individuals deny responsibility for their acts. On the basis of a survey which explored the motivation to crack commercial software, Cruise (2003:78-79) found strong support that crackers accept full responsibility for their actions and the disapproval of others. The activities and actions of piracy rings such as DrinkOrDie and Razor 1911 also suggest that they pursue their activities for themselves regardless of the disapproval by corporations and the criminal nature of the offence. For example, some members of DrinkOrDie are executives within the music industry. A denial of responsibility provides only partial support for explaining the behaviour of Internet pirates as the motivation to pirate challenges this technique.

(c) Child Pornography

One of the first cases where a denial of responsibility has been used against the presence of images of child pornography on personal computers in the UK involved a 39-year-old communications engineer, Karl Schofield. It was alleged that Schofield possessed 14 images of child pornography on his computer. Experts testified that a Trojan could have been responsible for the presence of images. According to the alleged offender, ‘the specialist found the
day before the images were downloaded the program was implemented ... [and maintained] ... I had no clue about them' (Surrey & Berkshire Newspapers Limited 2003:1). Schofield was found not guilty.

In another case in the UK, it was alleged that Julian Green was in possession of 172 images of child pornography on his PC. Green’s defence argued that he had no knowledge of the images on his computer. The likelihood of this occurring on someone’s computer is possible according to Hogan, a senior manager at Symantec Security Response. ‘It is technically possible for a Trojan to set up someone’s computer as a proxy machine. So you see a folder on your desktop, double click it and it executes’ (in Kotadia 2003:1). Due to the presence of Trojans on his hard drive, Green was acquitted (Everett 2003a:1). The evidence suggests that some alleged offenders are using the justification of Trojan horses and computer viruses to deny responsibility for their behaviour.

(d) Internet Fraud

The presence of a computer virus has been used as a defence in the case of Alabama accountant, Eugene Pitts who was accused of underreporting one million dollars on his tax returns during 1997 and 1999. Pitts was acquitted on nine counts of tax evasion and filing fraudulent business and personal tax returns after his defence argued that a computer virus had caused the inaccuracies and falsification of information (Sophos Plc 2003:1).

Not all forms of fraud support a denial of responsibility. For example, Kim David Faithfull, a bank manager at the Commonwealth Bank of Australia (CBA) did not deny responsibility for his actions of defrauding the CBA. While managing the CBA Karratha branch in Western Australia, Faithfull established an Internet gambling account with IASBet from his work computer and gambled close to AUS$19 million dollars over a five-year period. Faithfull turned himself in to authorities and explained his actions to bank colleagues through a note expressing his guilt and remorse (Cornford and Cowan 2003:2). Faithfull was sentenced to 5 years jail.
5.5.2 Denial of Injury

A denial of injury occurs when an individual feels that nobody has been harmed by the deviant act or acts. The offender neutralises or ‘plays down’ their actions as harmless or explains that the victim could afford the loss.

(a) Hacking

A student registering to be a service provider on an Australian government website revealed that its site could allow other users to manipulate confidential information. According to the student:

... I was filling out my details and I noticed that I’d made an error, so I went back to edit it. In the process of that, I worked out pretty much how the site was working and it occurred to me that I could manipulate the site to reveal someone else’s details. I found that quite shocking, so I decided to send everyone who was affected an e-mail to tell them about that (K2 2000 cited in Torney 2000:1).

The purported rationalisation for the intrusion was that the student was alerting other providers to a security flaw that enabled intruders to view personal details with the potential of exposing them to risk. In this example, the individual felt that his or her actions had not caused any harm.

Rosoff et al. (1998) describe a case in which Sykes and Matza’s techniques of neutralisation provided a way for seven students to justify and excuse their illegal actions. In this case, seven high school students who went by the name ‘414’ erased sensitive and confidential data at New York’s Memorial Sloan-Kettering Cancer Center and illegally intruded into the Los Alamos, New Mexico, nuclear weapons facility (Driscoll 1983:2 cited in Rosoff et al. 1998:376). According to Rosoff et al. (1998:376), ‘when they were apprehended, they denied any criminality in their actions ... “We didn’t intend harm”’.

Hackers who are motivated by curiosity, exploration, or the challenge may argue that their actions are not wrong because there was no injury caused by exploring computer systems. Shaw et al.’s (1999:4) study found that in most cases, explorers’ actions ‘... reveal the organisation’s lack of adequate policies
and safeguards and expose the potential consequences of unauthorised access’. This is in contrast to hackers who intentionally damage a system.

Similarly, hackers who justify their intrusion into a computer system may argue that they were unaware that their actions contravened an offence. Shaw et al.’s (1999:4) study showed that hackers classified as ‘Good Samaritans’ ‘like to ‘save the day’ or show off their abilities’. They maintain that ‘Good Samaritans should not be confused with other perpetrators who disingenuously claim they were just ‘testing security’ when caught hacking the system’. An example of denial of victim involved a military technician who discovered a system failure in a military operated network identical to his own, although the facility was in a different location (Shaw et al. 1999). After the technician illegally entered the network to perform emergency repairs, the detection system was activated setting off the alarm system. Shaw et al. (1999:4) note that the technician was reprimanded although due to his benevolent intent no further action was taken.

(b) 5.5.2.2 Internet Piracy

An offender may justify his or her criminal activity by claiming that companies invite Internet piracy to be carried out because the record and software companies can afford the loss. According to Britton (2003:32):

... local record companies ... [must] drop CD prices if they want consumers to buy music ... copyright is a sanctioned monopoly, and when consumers are copying CDs, they are reacting to a market failure and high prices created by that monopoly (cited in Needham 2003:25-32).

This type of behaviour by the software pirates shifts attention from the individual’s actions to the behaviour of those who disapprove of their violations.

Skinner and Fream (1997:510) hypothesised that techniques of neutralisation may show a positive correlation with some forms of computer crime. A survey of 581 undergraduate college students on participation in computer crime showed partial support for the existence of neutralising techniques.
Skinner and Fream (1997:500) found that ‘college students who feel that companies and institutions should provide better security were more likely to guess passwords and browse accounts illegally than students not feeling this way’. In other words, the justification used by students meant that had computer systems been more secure, access would not have been available, thereby playing down their action as ‘harmless’. The findings of the survey also showed that ‘... when students felt that (1) software companies overpriced their product and (2) they would not report a friend who pirated software, they were more likely to pirate software and commit different types of computer crime than those not holding these attitudes’ (Skinner and Fream 1997:510-511). These findings suggest that individuals felt that companies could afford the loss because the software in their view was too costly.

Cruise’s (2003) study of people who crack commercial software revealed that ‘the majority of crackers accept that harm is caused by their actions, [although] a cluster of respondents did use the denial of injury to justify their actions’ (Cruise 2003:79). A number of members of Internet piracy groups claim that they are not causing injury to companies who produce music and games because the companies can afford it. The results from a US survey revealed that over half of the students surveyed felt that the technology industry is so prosperous that a few people using unlicensed software won’t make a difference (BSA 2003:14). The actions by pirates in this example diminish their culpability by not viewing their action as wrong.

A survey of Internet piracy on campus among 1000 American college and university students and 300 college and university educators, found that 88 per cent of students, 54 per cent of administrators, and 52 per cent of professors felt that it made no sense to be charged hundreds of dollars per user given the license vs. money ratio to reproduce the software (BSA 2003:14). In other words, the justification that companies can afford the loss excuses their behaviour as harmless.

Logsdon et al. (1994:855) conducted an exploratory study of the relationship between moral judgment and attitudes towards software piracy and revealed that those people who participate in the use of pirated software do not believe
that they are causing harm or injury to the software companies which are the authors of the software. According to Logsdon et al. (1994:855), ‘for software developers and companies, the implications of our study are serious, since even those who are capable of the most principled moral reasoning may engage in copying behaviour’.

(c) Child Pornography

In relation to accessing child pornography on the Internet, Quayle and Taylor’s (2002:340) study showed that:

The selection of images for sexual purposes was made according to some sort of “moral” or “ethical” code ... which allowed the viewer to believe that the children in the pictures were consenting and enjoyed being photographed.

The boundaries set by the individuals appear to justify any injury caused by the respondents. The following quotes by respondents are examples of the way they further legitimised their involvement:

Well there was definitely never any baby pictures believe you me ... I would have said there’s definitely nothing below ten on what I have on my system (T.S. cited in Quayle and Taylor 2002:340).


... just basically images of girls mainly. Girls actually having sex. And they had to look happy ... I mean I wasn’t looking for rape or anything (E.I. cited in Quayle and Taylor 2002:340).

These examples show that respondents denied any injury to the children, by claiming that the girls were happy and were indeed not hurt by the experience. Furthermore, Quayle and Taylor (2002:341) argue that ‘such pictures were often talked about in a very dispassionate way with no reference made to the fact that they were pictures of children’. They illustrate this justification with the following comments by respondents who appear to normalise their behaviour through comparing the collection of images to baseball cards and stamp collecting:

We were trading pictures ... it’s, as much as it pains me to say ... kinda like trading basketball cards (Q.H. cited in Quayle and Taylor 2002:342).
And there was also the thrill in collecting them. You wanted to get complete sets so it ... was a bit like stamp collecting as well (E.I. cited in Quayle and Taylor 2002:342).

These examples provide support to Sykes and Matza’s denial of injury through the various techniques used that normalise their activity (Quayle and Taylor 2002).

(d) Internet Fraud

A denial of injury may apply to perpetrators who carry out Internet fraud through what is termed the salami technique. This technique is applied by criminals who install a software program that enables the widespread deduction of small amounts of money from account holders. This high volume, low-value technique is used to reduce any suspicion by account holders that funds have been deducted. In 1993, four executives of a car rental franchise in Florida allegedly defrauded more than 47,000 customers by adjusting a computer billing program, which added extra litres to the car tank’s capacity. The scam operated over a three-year-period, which meant that customers who returned the hired car without filling up the petrol tank were charged inflated rates for an inflated total of petrol (Kabay 2002:2). Between US$2 to US$15 was charged per customer due to the scam. The rationalisation is that the victim is either unaware of the theft, or regards it as trivial.

A denial of injury may apply to offenders who defraud online bank customers through phishing and justify that their actions do not cause harm because banks can afford the loss. The lack of evidence to suggest that this occurs makes it difficult to provide support; however, evidence that phishers target legitimate financial institutions and companies may partially support this claim. The Anti-Phishing Working Group (APWG) (2005:3) reports that during the October 2004 – January 2005 period, the financial services sector averaged between 74 and 86 per cent of all hijacked brands. The number of phishing websites also increased during this period. In January 2005, 2560 phishing sites were recorded, an increase of close to 50 per cent from December 2004 (1740) (APWG 2005:2). Yearly profits recorded by banks across the globe may also justify to offenders that banks can afford the loss despite the financial harm
caused. Braue (2004:60) reports that estimations by research firm, Gartner, revealed global losses of US$1.2bn in 2003 by financial institutions through phishing. There is no evidence to sustain the argument that this technique is used by phishers.

5.5.3 Denial of the Victim

If an individual acknowledges the actions and accepts responsibility, he or she justifies the response made in view of the circumstances prevailing in the first place. Sykes and Matza (1957:668) argue:

> Even if the delinquent accepts the responsibility for his deviant actions and is willing to admit that his deviant actions involve an injury or hurt, the moral indignation of self and others may be neutralised by an insistence that the injury is not wrong in light of the circumstances.

(a) Hacking

Denial of victim may be applied to people who intrude into computer networks who are motivated by revenge or where they believe the victim had it coming. For example, George Parente, a former Forbes Inc. computer technician was charged with causing damage to the company’s computer network after his employment was terminated. It is alleged that Parente obtained access to the company’s network through a co-worker’s password, which resulted in numerous computer servers crashing and erasure of data (Freeh 2000:2). According to Freeh (2000:2), it ‘... appears to have been a vengeful act against the company and his supervisors ...’. Palente pleaded guilty and is awaiting sentence.

In another example, a disgruntled employee of Lance, Inc., John Michael Sullivan intentionally disrupted the company’s computer system by inserting part of a ‘logic bomb’ in the software that he was developing. According to reports, Sullivan’s role was to assist in developing a program that the company’s national sales staff could use to increase their efficiency (Williams and Williams 2001). On May 8, 1998, Sullivan was notified that he would be demoted citing poor performance, and on May 22, 1998 Sullivan resigned from the company. It was during this period that Sullivan inserted the ‘logic bomb’, which was released the day after his resignation, May 23 at noon. The release
of the bomb meant that the computers were inoperable (Williams and Williams 2001:1). These two examples show that the justification for the intrusions was made in light of their circumstances – termination of employment.

(b) Internet Piracy

Some Internet pirates may claim that companies deserve their products to be copied because the prices are unreasonable or that there is no real victim because a few people downloading their music or software won’t make a difference.93

The justification made by some pirates in Russia is that they cannot afford to purchase software, music or movies at legitimate prices. This view is echoed by Tanya, a 21-year-old who maintains ‘the prices are ridiculously high’. In Dima’s view, ‘... Russia piracy is not such a bad thing, since it compensates for our low incomes. At least it becomes possible for people to educate themselves about computer programs’. According to Antonova (2004:3), it costs approximately US$15 to purchase a newly released album and US$600 for computer programs such as Adobe Photoshop, this is in contrast to the average monthly income, which is approximately US$240. While Dima recognises that ‘It’s honourable to support domestic business ... [she suggests that] the whole system has to be changed in order for an average Russian to afford something other than pirated copies’ (cited in Antonova 2004:3). The justification is made that if the prices to purchase legitimate copies were made, that the injury is not wrong in light of the circumstances.

(c) Child Pornography

The use of virtual child pornography on the Internet has created the justification that there is no victim because there is no involvement of children. The difficulty with this justification is that it can be difficult to discern between real and virtual images, given the advanced ways images are created. In

93 Berman (2002:1) argues that victims include ‘... artists whose creativity gets no reward; governments who lose hundreds of millions of tax revenues; economies that are deprived of new investment;
reviewing the US Supreme Court’s decision on virtual child pornography, Walters (2005:2) comments that ‘... the rationale behind the existing child pornography laws was the protection of real children from sexual abuse ... If there are no children, there is no abuse, and therefore no crime’.

Bryan Sparks from the US was charged with child pornography offences after child pornographic material was found on his computer. It was reported that Sparks’ attorney acknowledged the difficulty of identifying whether the images on Sparks’ computer were real (Giffels 2004:1). A central part of the defence’s argument was that children are not victimised with the existence of virtual images. His defence team successfully argued that the images were virtual and did not use real children. (Giffels 2004:2). Sparks was acquitted of the charges.

(d) **Internet Fraud**

A denial of victim cannot be applied to this technique.

5.5.4 **Condemnation of the Condemners**

Condemnation of the condemners is a technique used by individuals who justify their actions to others who disapprove of their violations (Sykes and Matza 1957). According to Sykes and Matza (1957:668):

> The delinquent shifts the focus of attention from his own deviant acts to the motives and behaviour of those who disapprove of his violations. His condemners, he may claim, are hypocrites, deviants in disguise, or impelled by personal spite.

(a) **Hacking**

The hacker’s ethic, that all information should be free, is an example of condemnation of the condemners. According to Levy (1984:40-5), the hacker’s ethic includes the following:

- All information should be free’.

- ‘Mistrust Authority – Promote Decentralisation’.

consumers who get less diversity and less choice; and record producers who are forced to reduce their
• 'Hackers should be judged by their hacking, not by bogus criteria such as degrees, age, race, or position'.

• 'You can create art and beauty on a computer'.

• 'Computers can change your life for the better'.

The focus of attention on the behaviour of the hackers often shifts to a focus on the predominant motivations of those who disapprove of their violations.

Schell et al. (2002:244) explore the ideological contention of hackers and suggest that it comprises of the 'property paradigm' and the 'hacker paradigm'. Supporters of the property paradigm believe that the law protects the personal rights of property. In contrast, the hacker paradigm encompasses the ethos that all information should be free and knowledge and ideas be shared. Schell et al. (2002:244-5) provide an example of the hacker paradigm demonstrated by MIT.

In early 2001, MIT announced that over the next ten years material would be freely available on the Internet for most of the courses on offer. According to Charles M. Vent, President of MIT, 'open courseware combines two things: the traditional openness and outreach and democratising influence of American education and the ability of the Web to make vast amounts of information instantly available (MIT News 2001:2 cited in Schell et al. 2002:245). This initiative by MIT challenges the ethos of the property paradigm by shifting the focus to freely available information instead of exploring the legal rights of information in the digital age (Schell et al. 2002).

(b) Internet Piracy

Cruise's (2003:80) study found evidence to suggest that crackers condemn the condemners. For instance:

Respondents believe that a company's poor business practices lead to piracy, five respondents believe that over-pricing by the software companies leads to piracy, and two regarded the software industry as artist rosters because it is impossible to compete against theft'.
morally corrupt. Only two respondents regard the action and response of the software industry as appropriate ...

Some Internet pirates also adopt a pirate’s ethic that music and software should be free and available for users. According to Goldman (2005:2), ‘almost all warez traders believe software should be free, and they view themselves as technology liberators and benefactors of the oppressed’. Similar views have been expressed, that the oppressive methods industries use reinforce the position of warez traders that the industry is the enemy (Granade 2003). Jesiek (2003:1) points out that ‘the development of computer software and hardware in closed-source, corporate environments limits the extent to which technologies can be used to empower the marginalised and oppressed’. It appears that this position provides a further basis for condemnation of the condemners.

(c) Child Pornography

The North American Man/Boy Love Association is an example of condemnation of the condemners. The association supports the view that consensual sex between adults and boys (even below the US age of consent) should not be illegal and is appropriate behaviour. The mission of Man/Boy Love Association is ‘... to end the oppression of men and boys who have freely chosen, mutually consensual relationships’ (NAMBLA 2003). The Internet increases the exposure for members of NAMBLA to meet boys through chat rooms, e-mail, and news groups. Soto (2005:1) reports that ‘law enforcement officials and mental health professionals say that ... the group has a dangerous ripple effect through the Internet by sanctioning the behaviour of those who would abuse children’.

(d) Internet Fraud

It is difficult to apply an example of Internet fraud to this technique. As more and more cases of Internet fraud are investigated, future research may bring to light the applicability for this behaviour.
5.5.5 Appeal to Higher Loyalties

Some offenders will argue that the crime in question was necessary in order to prevent a greater evil or that loyalty to friends overrides that of others.

(a) Hacking

An example of appealing to higher loyalties involved a hacker (United States v. Bradley Joseph Steiger 318 F.3d 1039) claiming to be from Turkey, who anonymously alerted law enforcement authorities in the United States of America to a suspected individual whose computer contained images and was in receipt of child pornography (Goodwin 2003). The anonymous source sent an unsolicited e-mail to the Montgomery, Alabama Police Department and revealed:

I found a child molester on the net. I'm not sure if he is abusing his own child or a child he kidnapped ... As you see he is torturing the kid. She is 5-6 y.o. His face is seen clearly on some of the pictures. I know his name, internet account, home address and I can see when he is online ... (cited in Goodwin 2003).

The anonymous source declined to reveal his identity throughout the investigation due to his criminal actions. The justification for appealing to higher loyalties in this example was to prevent further sexual abuse against children by appealing to police to investigate. In fact the hacker also revealed that he had identified over 100 other suspected paedophiles.

A 25-year-old hacker, StRyKe, who was a member of the UK based Internet Combat Group (ICG) used his skills to fight against those involved in child pornography (Denning 1999:49). According to StRyKe, ‘I do think of myself as ‘moral’’. The Traditional image of a hacker is no longer a valid one. I don’t attack anyone who doesn’t deserve it. We are talking about people who deliberately harm minors’ (cited in Denning 1999:49). This example demonstrates that some hackers use their skill to appeal to higher loyalties and thus the crime in question was viewed as necessary in order to prevent paedophiles and pornographers on the Internet.

Ethical Hackers Against Child Pornography (EHAP) is another example of appealing to higher loyalties through hackers using their technical abilities and
skills to intrude into computer systems of suspected paedophiles with the goal of exposing them and their crimes. These hackers appear to justify their actions because of the serious nature of the crime and the broader consequences for the victims, community and users of the Internet. In fact, EHAP acknowledge that they use ‘... unconventional means to take down the worst, most unscrupulous criminals known’ (cited in Wall 1998:206). A sense of loyalty among hackers also provides support for appealing to higher loyalties through the sharing of information at the expense of legitimacy.

(b) Internet Piracy

Internet pirates may justify pirating materials because the loyalty to friends comes before corporations (Short and Zackheim 2002:87). Studies of piracy among university students show a positive correlation with file swapping and software piracy among peers. For instance, Moore’s (2004) study of peer-to-peer file sharing among university students found that it is prevalent among the majority surveyed. However, these results indicate that loyalty to friends has not motivated the piracy because Moore’s study revealed that few respondents believe that their actions are illegal.

(c) Child Pornography

The associations formed between members of the W0nderland Club suggest that loyalty to others within the group outweighed the illegal nature of their activities. The members communicated via private bulletin boards and their behaviour reinforced each other’s motivations due to the secretive nature of their activities and the trust established among members. The Internet provided the modus operandi for the global pornography ring despite the unlawful conduct carried out by members.

(d) Internet Fraud

The example of six individuals charged with Internet securities fraud, which included Huttoe, a former chairman of Systems of Excellence, Inc. (SEXI) and the company’s auditor Melcher, Jr., to promote the stocks of SEXI, may suggest that the illegal nature of their scam overrode the legitimate means to
achieve financial gain. In this example, loyalty to others may have given precedence over the law as the scam carried on for three years and resulted in gains of more than US$10 million dollars between those involved. However, the lack of evidence concludes that loyalty to others in this example is weak. It is difficult to provide empirical evidence because lone individuals carry out most frauds.

In summary, there is mixed support that techniques of neutralisation are used to justify the behaviour of cyber criminals. The analysis has shown strong support that denial of responsibility is used by hackers, pirates, and child pornographers. For example, each of the techniques used for hacking is positively correlated. Table 5.1 signifies support and partial support for the five techniques of neutralisation. It is important to note that while some types of crime show support there are additional motivations of cyber criminals that do not lend themselves to these techniques of neutralisation.

Table 5.1 Analysing the Applicability of Techniques of Neutralisation Against Cyber Crime

<table>
<thead>
<tr>
<th>Techniques of Neutralisation</th>
<th>Hacking</th>
<th>Piracy</th>
<th>Child Pornography</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of Responsibility</td>
<td>√</td>
<td>±</td>
<td>√</td>
<td>±</td>
</tr>
<tr>
<td>Denial of Injury</td>
<td>√</td>
<td>±</td>
<td>√</td>
<td>±</td>
</tr>
<tr>
<td>Denial of Victim</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>–</td>
</tr>
<tr>
<td>Condemning the Condemners</td>
<td>√</td>
<td>√</td>
<td>±</td>
<td>–</td>
</tr>
<tr>
<td>Appeal to Higher Loyalties</td>
<td>√</td>
<td>√</td>
<td>±</td>
<td>–</td>
</tr>
</tbody>
</table>

± Signifies partial support
√ Signifies support
– Signifies no support

5.6 GENERAL THEORY OF CRIME

Gottfredson and Hirschi (1990) proposed that their general theory of crime could apply to conventional and white-collar crime. Chapter Three showed mixed support for their
theory and, in general, found that it could not explain diverse forms of criminal behaviour.

5.6.1 Low Self-Control

Gottfredson and Hirschi examined low self-control as a key explanatory concept of the general theory of crime. Their theory claims that acts carried out are in general, simple and easy and are pursued for an individual’s own interest. Central to their theory of self-control is the concept of opportunity, which can determine an individual’s ability to resist temptation. If an individual’s resistance to temptation is diminished through opportunity, then they are seen to have low self-control.

(a) Hacking

Hacking is a form of cyber crime that can arise from low self-control. Although the motivations to hack vary, according to internal accounts, Taylor (1999:46) identifies three categories that can assist in lowering a hacker’s level of self-control:

- Feelings of addiction
- The urge of curiosity
- Enjoyment of feelings of power.

For instance, feelings of addiction can influence an individual’s propensity to commit hacking. Members of the hacker group, Toxic Shock (1990) maintained:

We are addicted to information and knowledge, and our drugs are withheld from us. We are forced to seek out precious information and knowledge elsewhere. We have to find challenge somewhere, somehow, or it tears our very souls apart. And we are, eventually, forced to enter someone’s computer (cited in Taylor 1999:47).

The urge of curiosity can develop into addictive behaviour and therefore a low level of self-control is established. According to Taylor (1999:46), ‘there seems to be a fine line between the levels of curiosity necessary for a competent hacker and the charge that such curiosity has stepped over the boundary into
addictive behaviour'. Taylor cites the Bedworth case to demonstrate the fine line between curiosity and addiction.

(b) Internet Piracy

The individual characteristics that Gottfredson and Hirschi identify with low self-control include impulsivity, insensitivity, and risk taking. The proliferation of Internet piracy rings on the Internet may increase the likelihood of low self-control because the opportunities appear much greater. Although little evidence is available to test this hypothesis, Higgins and Makin (2004) examined whether low self-control is positively correlated with Internet piracy among college students. Their study found support for Gottfredson and Hirschi’s proposition and showed that ‘... college students with low self control cannot resist the temptation of pirating software that they are interested in ...’ (Higgins and Makin 2004:13).

(c) Internet Sex Crimes against Children and Youth

The activities of the W0nderland Club showed that low self-control played a significant role in the distribution of sexual images of children among members. The W0nderland Club (discussed in section 5.3.2) illustrated that the Internet provides opportunities where an individual’s level of self-control is diminished because of the ease of access to images and the illusion of anonymity.

Authorities were alerted to evidence of child pornography on Ronald Scott Paul’s computer by a technician fixing the defendant’s computer (Tagle 2001:1). In fact, Paul’s background revealed that he had a prior offence involving child pornography in 1986. The behaviour of Paul appears to fit the interpretation that low self-control is a factor in Internet sex crimes against children, where the illusion of anonymity provided by the Internet makes it easier to commit the crime thereby diminishing self-control.

(d) Internet Fraud

The lack of available evidence has made it difficult to determine whether fraud can be explained because of low self-control. However, the examples of fraud
examined in this chapter suggest that the Internet has created opportunities for people to carry out a range of different forms of fraud, which may support Gottfredson and Hirschi’s proposition that if an individual’s resistance to temptation is diminished through opportunity, then they are seen to have low self-control.

5.6.2 The Correlation of Crime and Age

Gottfredson and Hirschi (1990) hypothesised that an individual’s involvement in crime reduces with advancement in age. It is important to note that generational differences in the take-up and literacy of Internet users are apparent. For example, in the early twenty-first century, children and young adults have grown up with the rapid development of technology and information technologies unlike older people who have had to learn after operating in an atomic world. With this in mind, it may be reasonable to assume that young adults may be more inclined to commit cyber crime because of the relative ease of access and technical expertise.

(a) Hacking

Traditionally, studies indicated that hackers predominantly consisted of teenagers (Meyer 1989; Denning 1999; Schell et al. 2002). This is consistent with their motivations, which are driven by the challenge, thrill, and adventure (Denning 1999). Accordingly, Denning (1999:44) notes that technologies such as the Internet "... offered endless opportunities for exploration and playing pranks ...". Although hackers are in their teens and early twenties, there is evidence to suggest that hackers also consist of older individuals. Denning (1999:50) notes:

Many hackers, perhaps most, do grow up, stopping at age 18 when they can be prosecuted as an adult. But others keep going, and some are not content with breaking locks, acquiring knowledge, and roaming the infobahn. They engage in serious acts of fraud and sabotage, and the entire underground culture supports their activities.

---

94 Common areas that provide Internet access include - cafes, airports, workplaces, libraries, schools, and tertiary institutions.
In general, most of the hacking related offences analysed in this chapter suggest that hackers range in age from teenagers to the middle aged. According to Maxfield (1998:5), a worrisome trend to emerge recently is the presence of adult computer hackers. ‘Some adults in the computer underground pose as Fagans, a character from a Charles Dickens novel who ran a crime ring of young boys, luring young hackers to their underground crime ring’ (cited in Lightning 1998). A number of factors which may indicate that hacking does not reduce with age include: the introduction of additional crimes that result from hacking (which may require a greater level of co-ordination and organisation), disgruntled employees who target their former employer’s computer network, and the proliferation and sophistication of organised criminal networks.

(b) Internet Piracy

Several studies on piracy have focused on college students who are among the largest demographic of pirates, with some suggesting that graduate rather than undergraduate students are among the largest category of students who pirate software (Skinner and Fream 1997). A study carried out by Ipsos (2002) revealed that of the respondents who admitted to pirating software, 30 per cent were males aged between 30-49, 21 per cent were males aged between 18-29, 20 per cent were females aged between 30-49, 19 per cent were men or women aged 50 +, and 11 per cent were women aged 18-29.

Members of Internet piracy rings, such as DrinkorDie and Razor 1911, included executives in record companies, computer network administrators, government employees, and university students. A number of Warez traders are older males rather than teenagers or students and work in the information technology industry (Goldman 2003:395). These findings suggest that Internet piracy is carried out by people of all ages. Whether patterns of desistance will be observable as we move further into the digital age remains to be seen.

(c) Internet Sex Crimes against Children and Youth

A US study, Internet Sex Crimes Against Minors (2000) (Finkelhor et al. 2000) revealed that over two thirds of Internet sexual perpetrators were male, 48 per
cent of perpetrators were younger than 18 years of age, 24 per cent were 18 and older, and 27 per cent were unknown (Finkelhor et al. 2000). This survey appears to dispel the myth that sexual offenders are older males, although the results are in stark contrast to more recent studies.

A study carried out by Wolak et al. (2003), *Internet Sex Crimes against Minors*, revealed that 41 per cent of perpetrators were aged 40 or older and 45 per cent were aged 29-35. These statistics appear to be consistent with data provided by the Queensland Crime Commission (QCC) and Queensland Police Service. For example, between 1994 and 1998, 97 per cent of child sexual offences reported to the police were perpetrated by males; the average age of a non-familial offender at the time of his first child sex offence was 30 years (Stanley 2001:4).

A three-year study (1997-2000) that profiled over 200 child sex offenders ranging in age from 13 to 65 found a mean of 35.7 and a median of 45 (McLaughlin 2001). The majority of offenders did not have prior contact with law enforcement prior to the Internet. This suggests that the Internet has opened up a market for people of all ages to engage in illegal activities, thus dismissing Gottfredson and Hirschi’s proposition that crime reduces with advancing age.

The case of Ronald Scott Paul (discussed above) also challenges Gottfredson and Hirschi’s claim that crime reduces with age because Paul was first convicted of possessing child pornography 15 years prior to his conviction of similar offences on the Internet. Similarly, details of Operation Ore, the British investigation of a child pornography ring revealed that perpetrators included more than 50 police officers, judges, two members of parliament, and doctors (Weiss 2003:4).

In summary, the Internet provides paedophiles with an additional medium for committing child pornography offences. The opportunity is greater; self-control is diminished with the illusion of anonymity; Internet services are readily accessible; and there are a number of like-minded individuals to communicate with regardless of age.
(d) Internet Fraud

Little available evidence demonstrates the age demographic of perpetrators of Internet fraud. However, the examples in this chapter show that perpetrators of a broad range of Internet fraud are committed by people of all ages. Given that fraudsters have become adept at exploiting the Internet's capabilities, the level of sophistication of Internet scams has also advanced.

The evidence presented here refutes the applicability of Gottfredson and Hirschi's theory as a general theory because not all crimes result from poor impulse control and age does not appear to constrain particular crimes committed on the Internet. This section has also shown the limits to Gottfredson and Hirschi's claim that crime reduces with age.

5.7 ROUTINE ACTIVITY THEORY

Routine activity theory places emphasis on the everyday routines and patterns of social interaction as contributing factors to criminal behaviour. Cohen and Felson's (1979) theory goes beyond focusing exclusively on the offender, instead concentrating on the opportunities that exist to commit crime within various structures. For a crime to be carried out, Cohen and Felson (1979) propose three pre-requisites:

- a supply of motivated offenders
- the availability of suitable targets
- the absence of capable guardian to prevent the crime from occurring.

Cohen and Felson (1979:590-591) did not envisage the exponential growth and global reach of technologies such as the Internet, although their explanation acknowledges that:

... technology and organisation affect the capacity of persons with criminal inclinations to overcome their targets, as well as affecting the ability of guardians to contend with potential offenders by using whatever protective tools, weapons and skills they have at their disposal.

Cohen and Felson (1979) illustrated this point with the automobile and telephone as examples of the way in which technology has enabled greater access and opportunity.
for crime to be committed. Some three decades later, the Internet provides one of the central areas for examining how this technology affects the capacity for motivated offenders to carry out different types of cyber crime. The following sub-section explores the three pre-requisites of routine activity theory prior to applying it to different forms of cyber crime.

5.7.1 A Supply of Motivated Offenders

It was illustrated in Chapter Three that a supply of motivated offenders can be categorised into three elements: the number of prospective offenders, the intensity of their motivation, and their proximity to the prospective target or victim. The Internet bridges barriers of physical distance through communication and the speed of transactions. It was shown in Chapter Three that cyber crimes can be carried out from anywhere in the world by anyone who has access to the Internet. The global Internet population has created opportunities for motivated offenders to seek criminal opportunities in the virtual world.

Second, the motives for committing crime on the Internet are analogous to motives in the physical world, although they can be aroused and intensified by the opportunities available on the Internet. Grabosky et al. (2001:2) state that ‘computer criminals are driven by time-honoured motives, the most obvious of which are greed, lust, power, revenge, adventure, and the desire to taste “forbidden fruit””.

It was noted in Chapter Five that greed is one of the motivations behind auction fraud, phishing, online securities fraud, and commercial Internet piracy rings. The goal of the offender in most of these crimes is to defraud the victim and financially benefit from the transaction. Similarly, information merchants trade information for money. The motivation for corporate espionage is usually profit, as the exchange of information is the key factor for the crime to be carried out (Thomas and Loader 2000; Nasheri 2005). It has been established in this chapter that the size of the offender pool is one of the significant factors in the growth of cyber crime.
All else being equal, the greater the number of Internet users, the greater the number of prospective offenders. Figure 5.2 shows that there were an estimated 280.86 million users worldwide (4.63 per cent of population) in February 2000, 455.55 million users (7.5 per cent of population) in February 2001, and 569.14 million Internet users (9.37 per cent of population) in February 2002. Over a two-year period, the number of users of the Internet has doubled (Nua Surveys 2002).

5.7.2 The Availability of Suitable Targets

The availability of suitable targets (or victims) on the Internet is growing exponentially due to its scale and global capability, thereby increasing the capacity and accessibility to reach millions of users. For instance, the availability of suitable targets can range from individuals to organisations, corporations and governments and of course information itself (see Newman and Clarke 2003). A recent CSI/FBI computer crime and security survey revealed that the Internet is increasingly being targeted (Richardson 2003).
Figure 5.3 illustrates the proliferation of targets. A DDoS attack or the unleashing of a virus or worm can mean that individuals, organisations, corporations, government and information can be the target or victim. Newman and Clarke (2003:46) note that ‘since information has become the key ingredient of e-commerce ... all of e-commerce becomes a target’. This certainly confirms that a suitable target is a pre-requisite for the commission of much cyber crime. The growth in connectivity and take-up of the Internet results in a greater number of prospective targets as well as victims.

There are many factors that demonstrate the growing availability of suitable targets on the Internet. Information technologies such as the Internet provide unprecedented capacity to accomplish things that have traditionally been difficult to achieve on a global scale and maintain in the physical world. For example, the Nigerian fee scheme that emerged over a decade ago relied on postal messages to reach millions of potential victims or targets. The cost to set-up, print and distribute letters would amount to hundreds if not thousands of dollars and in addition, the speed of response would be much slower than the Internet. Today, these letters can be produced through digital
technology at very little cost and reach millions of users instantaneously. The storage of valuable information by individuals, companies and government on the Internet increases the accessibility of the information to prospective offenders, and depending on the type of information available contributes to the attractiveness of the item as a target.

5.7.3 The Absence of Capable Guardianship

The Internet, a largely unregulated electronic domain, was initially based on trust (Fukuyama 1995). In the 1970s and early 1980s, the Internet community was relatively small and regulation was not viewed as an area of concern. However, this chapter has established that the Internet provides a unique means and is an inviting space to carry out a broad range of crimes. One of the attractions of various forms of crime on the Internet is the absence of capable guardians to monitor criminal behaviour.

As the Internet community grows wider, with improved ease of access and operability, it is lacking technological guardianship. In a much similar way in which people used to leave their front doors open (because it was presumed safe to do so), computer users leave computer passwords around or on computer terminals thus contributing to the absence of capable guardianship on the Internet.

Part of the attraction of the Internet to prospective criminals is its global reach and inadequate self-policing. The lack of guardianship on the Internet can also be attributed to the following factors:

- limited law enforcement to patrol the vast terrain of the Internet
- low security consciousness
- lack of self defence
- lack of willingness to report cyber crime
- vulnerable systems
- the lack of a central global control for cyber crime
- the Internet is multi-jurisdictional, and legal arbitrage leaves victims unguarded by law. Furthermore, it allows for some crimes to be recognised in one country and
not in another. Therefore, an individual may base himself or herself in a country where a crime is not illegal; however, the effects and impact may be in countries where it is illegal. The ‘ILoveYou’ virus was an example of this phenomenon

- the invisible nature of many different forms of crime such as identity theft and fraud makes it difficult for guardianship to work.

There are a number of ways in which security has been developed to guard and police the vast terrain of the Internet (this will also be explored in Chapter Seven). For instance, technological tools, such as firewalls and anti-virus software have increased the security of computer systems and networks. The 2003 Computer Crime and Security Survey (CCSS) revealed that 99 per cent of the organisations surveyed use anti-virus software while 98 per cent of organisations use firewalls to prevent attacks on their systems. The survey also highlighted that 91 per cent of organisations ‘... employ some kind of physical security to protect their computer and information assets and most [92 per cent] employ some measure of access control (Richardson 2003:4). Alternatively, Microsoft has established a ‘reward fund’ worth US$5 million dollars to pay bounties to those who trace and track down writers of malicious code in the hope of enlisting the expertise of the hacker communities to flush out virus writers (Regan 2003 cited in Frey 2003:15).

Guardianship can also be enhanced by market forces. For instance, Grabosky (2000c:10) suggests:

A market is currently emerging for internet service providers specialising in content suitable for family consumption, guaranteed to be free of sex, violence, and vilification. Market forces may also generate second-order controlling influences. As large organisations begin to appreciate their vulnerability to electronic theft or vandalism, they may be expected to insure against potential losses.

Other forms of guardianship include less formal methods of social control, such as private monitoring, parental supervision, auction escrow services, online watch groups such as cyberangels, and methods of surveillance (Grabosky 2000c). Nevertheless, this chapter has shown that despite efforts to increase security on the Internet, the absence of guardians on the Internet still allows the commission of a broad range of crimes. The following section will determine whether Cohen and Felson’s theory can explain different forms of cyber crime.
5.7.4 Testing Routine Activity Theory

(a) Hacking

The behaviour and motivation of hackers has been a growing area of empirical research (see Hollinger 1988; Denning 1990, 1999; Sterling 1992; Tangent 1992-2003; Adamski 1998; Jordan and Taylor 1998; Taylor 1999; Rogers 2000, 2001a; Schell et al. 2002). This is a departure from several studies that have focused on the victims of cyber crime and the financial costs associated with it.

Motivated Offenders: An examination of the motivations of hackers in Chapter Four revealed that hackers are motivated by excitement, curiosity, prestige, craftsmanship, peer reputation and recognition, celebrity, the thrill and the challenge (see also Denning 2000; Rogers 1999, 2000). Denning (1990:6) observes through one hacker, ‘hacking was the ultimate cerebral buzz for me. I would come home from another dull day at school, turn my computer on, and become a member of the hacker elite’. In the words of another hacker, ‘... much of the thrill comes from the dangers associated with the activity ... the technology just lends itself to cloak-and-dagger drama’ (cited in Denning 1990:7). In addition, more people online means more hackers online.

Post’s (1996) survey of hackers provided an analysis of individual behaviour characteristics such as self-perception and motivation. Post (1996:2) noted that hackers were motivated by the excitement to succeed, the challenge, and intellectual curiosity. Chantler’s (1996) study that examined the profile of hackers produced similar findings. The study involved 164 participants including hackers and people within the computer industry (cited in Rogers 2001a:52). Chantler’s study revealed that the motivations of the participants varied between different sub groups – the elite, neophytes, and the losers. The motivations of the elite included excitement and the challenge, a desire to achieve, and self-discovery. The motivations of the losers included vengeance, theft, and financial gain (cited in Rogers 2001a:53).
Dreyfus (1998:7) provides an insight into a number of hackers’ objectives based on the four motivations described above: excitement, curiosity, the thrill and the challenge:

- ‘The kick of getting into a system. It’s the ego boost from doing something well where other people try and fail. Once you are in, you very often get bored and may never call back. Because once you’ve gotten in, it’s a challenge over’. (Electron).

- ‘Once you get into the first system, it’s like, you get into the next one, and the next one, and the next one ... like forbidden fruit’. (Anthrax)

- ‘[At first it was] possibly the sheer lust for power or [the desire] to explore an intricate piece of technology. [Now] my first and foremost motivation is to learn’ (SkiMo)

- ‘It ain’t a malicious thing. It’s a challenge – the thrill of the chase. Sometimes I think I hack just to be able to say that I do something, like its a fad or something’ (Case).

Some hackers are also motivated by the desire for celebrity and peer recognition. ‘Mafiaboy’ was detected boasting about his exploits on the Internet (Yusuf 2004). This chapter has also noted that some hackers engage in additional forms of criminal behaviour such as fraud, extortion, and sabotage. In these cases hackers may also be motivated by greed and revenge.

**Availability of Suitable Targets:** The availability of suitable targets for hacking is broad and varied. The proliferation of connected computers – personal, commercial, and governmental means more computers are at risk.

**Absence of Capable Guardianship:** A number of hackers have succeeded in intruding into computer networks because of inadequate guardianship. For example, a 15-year-old Canadian teenager known as Mafiaboy intruded into a number of US university systems and released a malicious code. Mafiaboy targeted online websites such as Yahoo!, Dell, Amazon, eBay, and CNN and
carried out DDoS attacks, which prevented the websites from offering their services to Internet users.

Gary McKinnon, an unemployed computer systems administrator from the UK, illegally accessed 92 US military computer systems, two computer networks at the Pentagon, and a number of computers systems of private companies (McNulty 2002b). It was alleged that McKinnon installed copies of a commercial program, RemotelyAnywhere on the computer networks to access and remotely control another computer. Having obtained access to a number of computers, it was alleged that McKinnon installed a number of hacker tools, copied password files, deleted user accounts and confidential files and later used those computers to find the next target. McKinnon also caused a network to shut down for a number of days and a number of US military computer systems were rendered inoperable for one week (McNulty 2002b).

While the examples showed that these intrusions succeeded because of inadequate guardianship, awareness of cyber security issues appears to be on the increase. An online survey carried out between December 2004 and January 2005 to 850 members of the US Information Systems Security Association (ISSA) found an increase in the awareness of professionals and organisations about online computer security since late 2003 (PSB 2005). For example, in 2005, 93 per cent of companies wrote information security policies compared to 70 per cent in 2003, 91 per cent of companies had access controls compared to 69 per cent in 2003, and in 2005, 91 per cent of companies had a designated person responsible for information security compared to 78 per cent in 2003 (PSB 2005:11). An increase in awareness of cyber security issues and implementation of security policies increases a company’s defence capabilities against cyber crime. Security technologies have also been applied as a preventative measures against cyber crime, as Figure 5.4 demonstrates.
Figure 5.4  Security Technologies Used

Security Technologies Used

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>92</td>
<td>90</td>
<td>92</td>
<td>93</td>
<td></td>
</tr>
<tr>
<td>Biometrics</td>
<td>11</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted Files</td>
<td>56</td>
<td>54</td>
<td>51</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-virus Software</td>
<td>90</td>
<td>83</td>
<td>100</td>
<td>98</td>
<td></td>
</tr>
<tr>
<td>Reusable Passwords</td>
<td>48</td>
<td>46</td>
<td>61</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewalls</td>
<td>89</td>
<td>95</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted Login</td>
<td>56</td>
<td>53</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td>55</td>
<td>50</td>
<td></td>
<td>91</td>
<td>91</td>
</tr>
<tr>
<td>PCMCIA</td>
<td>39</td>
<td>39</td>
<td>39</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>59</td>
<td>50</td>
<td>61</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital IDs</td>
<td>34</td>
<td>42</td>
<td>42</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Computer Security Institute 2003
(b) Internet Piracy

Motivated Offenders: Internet pirates are motivated by a range of factors that include the thrill of the illicit, ego, the notion that information should be free, the challenge, reputation, and greed. The United States Department of State (2001:1) maintains that ‘earning an online reputation as the fastest to steal, “crack”, and release high-quality, pirated software over the Internet is most important to them’. The notion that software should be free is based on the idea that Warez traders are liberators and support the oppressed (Goldman 2003, 2005).

Availability of Suitable Targets: Suitable targets include software companies, music companies, universities, and local culture. The ubiquity of digital content vulnerable to piracy speaks for itself.

Absence of Capable Guardianship: Controlling Internet piracy is made more difficult by the continued increase in transmission speeds. An increase in transmission speeds equates to a greater number of files downloaded (that are considerably larger in size), therefore increasing the volume and accessibility. Making a product more user-friendly may make it more vulnerable to exploitation.

Companies and organisations continue to take steps to reduce the volume of Internet piracy by increasing the protection on the software making it more difficult to crack. Law enforcement has also played a significant role through a number of global operations which have resulted in thousands of arrests and imposed on a number of people involved in the global piracy ring, DrinkOrDie.

(c) Internet Sex Crimes against Children and Youth

Motivated Offenders: Those who solicit children on the Internet appear to be predominantly motivated by lust, power and the desire to taste ‘forbidden fruit’ (Grabosky 2001a). A plethora of opportunities exists on the Internet to communicate with children in the furtherance of other offences. The Internet has increased the pool of motivated offenders. A study conducted by children’s charity, NCH, revealed that child pornography through the use of computers
and the Internet has increased exponentially over the past 13 years. The study revealed that in the US 35 child pornography offenders were cautioned or charged in 1988 in comparison to 549 in 2001 (Reuters 2004 cited in ABC online 2004). According to NCH, ‘the scale of the problem has changed beyond recognition in just over a decade ... The increased demand has made child pornography into big business and the consequences for children in all parts of the world are horrifying’ (Reuters cited in ABC online 2004)

Availability of Suitable Targets: includes young children and youth who surf the Internet for recreational purposes. More kids are online than ever before. Figures by Neilsen/Netratings reveal that approximately 10.5 million Australians browse the Internet. The number one instant messaging service, MSN reaches 60 per cent of online users aged 12–17 years old (Baguley 2005:5). Children learning how to use computers and interact with other children at school extend these activities into the home environment. However, these experiences can lead to harassment. A Report on the Nation’s Youth: Online Victimisation in the US (Finkelhor et al. 2000) revealed the following findings:

- Approximately ‘one in five received a sexual solicitation or approach over the Internet in the last year’.
- Girls were targeted at almost twice the rate of boys (66% versus 34%).
- 97% of the perpetrators of the sexual solicitations ‘... were persons the youth originally met online’.
- One in four had an unwanted exposure to pictures of naked people or people having sex in the last year.
- One in seventeen was threatened or harassed.
- In 65% of incidents, the youth met the person who solicited them in a chat room.
10% of incidents, the perpetrators asked to meet the youth somewhere (Finkelhor et al. 2000:ix, 2-4).

This report underscores the prevalence of youth victimisation on the Internet. It also outlines the risk youth face in communicating with other individuals on the Internet, which constitutes a breach of trust, and can lead to distress, and potentially dangerous encounters. This is consistent with the United States Department of Justice (2001c:2), who maintain:

Traditionally, both intrafamilial offenders and strangers have found that young children and teenagers are perfect targets for criminal acts because they are often trusting, naive, curious, adventuresome, and eager for attention and affection. However, the most attractive factor to predators is that children and teenagers historically have not been viewed as credible witnesses.

The anonymity that the Internet provides predators makes it a more attractive place to prey on children and youth.

**Absence of Capable Guardianship:** The low levels of guardianship in chat rooms or by parents make detection difficult and can therefore increase the attraction for would-be offenders to communicate with and solicit children over the Internet. This challenges previous studies by Cantor and Land (1985) and Bennett (1991) who showed that guardianship does not play a role in explaining personal crimes. Due to the serious nature of Internet crimes against children, there have been measures taken to increase levels of guardianship on the Internet. These include online watch groups such as cyberangels, volunteer bands, such as Cyberarmy Paedophile Fighters, Predator-Hunter, and Soc-Umand, and individual vigilantes who actively monitor sexual predators in the hope of providing leads to police.

In one example to demonstrate online guardianship, a 37-year-old mother, Julie Posey\(^5\), actively engages in chat rooms and news groups in search of online sexual predators by posing as a 14-year-old. After exchanging graphic e-mails with one stranger for two weeks, Posey arranged to meet the stranger. This
appeared to be part of Posey’s motivation to pick up alleged predators. Posey notified police of the communication, which resulted in the ‘... arrest on suspicion of attempted sexual assault on a child’ (Leonard and Morin 2002:1). Leonard and Morin (2002:1) note that ‘as well as posing as an underage girl, Posey collects e-mail tips on child pornography that she passes on to local police’. The rise of private crusaders demonstrates an increase in the role of informal methods of policing and guardianship, which may be in response to the lack of resources and manpower to police the vast space of the Internet.⁹⁶

*(d)* Internet Securities Fraud

While traditional types of securities fraud can be carried out on the Internet – market manipulation, insider trading, and misrepresentation, the Internet abounds with unprecedented opportunities to carry out crimes through a myriad of investment frauds. Access to information has meant that the opportunities for new types of fraud appear endless as more and more users connect to the Internet. This access thereby increases the availability and attractiveness of targets and makes capable guardianship more challenging.

**Motivated Offenders:** Securities fraud on the Internet is largely motivated by greed although it can also be motivated by revenge. The means to profit can take the form of either positive or negative information, rumour or hyperbole (Grabosky et al. 2001:84). For example, a PairGain employee designed a counterfeit webpage to imitate the Bloomberg News Service page for the purpose of misleading shareholders and investors. The objective of the counterfeit page was to falsely announce that PairGain, a telecommunications equipment company, was to be obtained by an Israeli telecommunications company. The offender sent a message under the pseudonym, Stacey Lawson, about the takeover through Internet bulletin boards hosted by Yahoo! The

⁹⁵ Posey has set up a web site www.pedowatch.org that also provides information and tips to Internet users.

⁹⁶ It is important to note that there is an increase in concern as to the privacy of online users who may simply communicate to fantasise but not act out their fantasies in the physical world.
scheme also allowed users to click onto the counterfeit website to validate the initial news of the takeover. According to Painter (2001:2):

In just two hours, the false news triggered a buying spree - - [sic] PairGain stock rose over 31% on NASDAQ with ten times its normal volume. When the hoax was exposed the stock fell causing thousands of victims to lose substantial amounts of money.

Painter (2001:3) notes that ‘although Hoke intended to trade in PairGain stock, he got ‘cold feet’ and never capitalised on the hysteria he created’. Those who traded as a result of the press release stood to gain financially as the shares made a gain of US$46.5 million. Hoke pleaded guilty to securities fraud.

A number of cases demonstrate that share market manipulation is also motivated by revenge. The example of the disgruntled employee at UBS Paine Webber shows that the offender attempted to drive the stock price of the company’s shares down because the offender was dissatisfied with the company’s existing salary and bonus structure.

**Availability of Suitable Targets:** The number of targets or victims of online securities fraud has expanded given the numerous ways people communicate and exchange information on the Internet through chat rooms, news group and bulletin boards. Trading on the Internet, which can be carried out privately, thus bypassing intermediaries such as brokerage houses, allows investors to buy direct and have access to information previously managed by intermediaries. This open means of trading has created new opportunities for criminals to provide false and misleading information to other investors, however. According to Grabosky et al. (2001:89):

Those who use the Internet, however, have great difficulty in identifying those with whom they are communicating. Some organisations may intentionally disguise their identity through the use of re-mailing facilities in order to defraud individuals later and avoid detection.

These methods have meant that the fraudster can operate at a level that in the terrestrial world was limited by access to information. Furthermore, the means to disseminate information effectively at this speed was also difficult to envisage two decades ago.
Absence of Capable Guardianship: Posting messages on the Internet or creating fictitious websites to disseminate false and misleading information is easier in the absence of capable guardians. For instance, services are available that can allow people to set up e-mail accounts without validation of user information and web hosting services. According to Painter (2001:2), ‘Angelfire [an Internet web hosting service] is a free service that allows users to create their own web pages asking only that they provide subscriber information and an e-mail account so that a password can be e-mailed to the user’. This process allows people to create fictitious identities that make guardianship difficult.

Given the various ways people can invest on the Internet throughout the globe, challenges have arisen for law enforcement agencies to keep pace with criminal techniques. In the US, the FBI investigate criminal activity relating to securities fraud with the cooperation of the Securities and Exchange Commission (SEC), the National Association of Securities Dealers (NASD), the Commodities and Futures Trading Commission (CFTC), and related state agencies. Clandestine and overt investigative techniques by law enforcement agencies have been used to investigate a range of securities scams. The cooperation between these agencies is instrumental in information gathering, which has resulted in a number of successful prosecutions against fraudsters.

(e) Auction Fraud

Online auctions constitute a large number of Internet transactions between users. The largest online auction house, eBay, began trading on the Internet towards the end of 1995 as an online marketplace in which goods and services are sold worldwide. According to eBay’s business model, ‘buyers and sellers are brought together in a manner where sellers are permitted to list items for sale, buyers to bid on items for interest and all eBay users to browse through listed items in a fully automated way’ (Gomes-Casseres 2001:1). While this type of auction is not a traditional form of auction in the terrestrial world (as

---

97 Goldsborough (2003:45) notes that estimations of eBay’s market share are 85 per cent.
there are very few live auctions on the Internet), it provides users with information and access to goods and services in a marketplace environment while trading to prospective buyers around the globe.

In the case of eBay, MacGibbon (2004:1) states that ‘at any given time, there are more than 34 million items available on eBay worldwide, and more than 3.5 million new items ... added each day’. EBay lists in excess of one million items in over 50,000 categories and has 125 million registered users globally. Given the statistical picture outlined above, it is not surprising that auction fraud constitutes the largest type of fraud on the Internet (as shown in Chapters Three and Five).

**Motivated Offenders**: Offenders of online auction fraud are predominantly motivated by greed and financial gain. Given that ‘on an annualised basis, eBay users worldwide now trade more than US$1,060 worth of goods on the site every second’ (MacGibbon 2004:1), the potential financial outcomes provide incentives for potential fraudsters.

The number of victims who have paid for goods that have failed to be delivered also demonstrates financial gain as one of the primary motivations. Surveys carried out on auction fraud have also provided accounts that are consistent with this view. For example, the Internet Crime Complaint Centre (2005:3) (IC3) reports state that non-delivered merchandise and/or payment accounted for 31 per cent of complaints in 2002, 20.9 per cent of complaints in 2003, and 15.8 per cent of complaints in 2004. While these figures represent a decrease during the period 2003-2004, the figures also suggest that during the period 2002-2004 referred complaints have increased to 71.2 per cent from 46 per cent. These figures suggest that motivated offenders are seeking additional opportunities where the likelihood of financial gain may be greater. The IC3 (2005:3) suggest the highest median losses were found among other forms of Internet fraud such as cheque fraud and the Nigerian scam.

**Availability of Suitable Targets**: The availability and attractiveness of suitable targets is attributable to exponential growth of online auctions and the number of users participating in auctions globally. With 125 million registered
Internet users on eBay and over 50,000 items trading each day, targets can include information such as credit card details, buyers and sellers (individuals, organisations, and corporations). Potential victims can be induced into trading offline with the false hope of a better deal; however, as shown in Chapter Six, this appears to be simply a strategy used by the alleged offenders to defraud other legitimate users.

**Absence of Capable Guardianship:** The absence of capable guardianship contributes to the growth of Internet auction fraud. This is supported by statistical data from the Internet Crime Complaint Center (IC3), which provide evidence for the rise in auction fraud over the past three years. In Theurer’s (2003:1) view, ‘while “brick and mortar” auctioneers are regulated by states; the same laws, designed to protect consumers, are not applied to online auctioneers. The result of this lopsided application of governmental regulation has resulted in a high incidence of fraud through online auctions ...’. In particular, Theurer (2003:3) argues that the rise of online fraud is attributed to the ‘lax governmental oversight and the insistence of self-regulation among online auction companies ...’. To overcome the imbalance of capable guardianship, the United States National Auctioneers Association (NAA) has put forth recommendations to bridge the gap between online auction fraud and capable guardianship (which will be discussed under regulatory response).

The vigilance of online auction houses in monitoring suspicious transactions is important to providing a method of guardianship for Internet users. Auction houses alone will not control fraudulent transactions, however. Online presence of law enforcement officers assist in guardianship. Many agencies around the globe employ specialist officers that track fraud-related cases. For example, a US based company that trains law enforcement agencies to gain information and skills relevant to tracking online fraud has reportedly worked with 275 police departments across the country and more than 500 officers during 2002-2003 (Johnson 2003:3).

One example that successfully demonstrates law enforcement surveillance of auction fraud involved the Holliston Police Department in the US. A theft of 30 AlphaSmart 3000 word processors from Holliston High School led
investigators to the eBay website where in excess of 20 computers were tracked down through sales. According to reports, five students were arrested and faced charges of theft (Johnson 2003:2).

In another example officers from a US cyber crime enforcement unit scanned a number of auctions on eBay and came across a number of items of computer equipment that matched the description of some equipment reported stolen. After communicating with the alleged offender, reports noted that officers were able to convince the seller to meet in person, which later led to an arrest (Johnson 2003:3).

The recent arrest of a 27-year-old male from Sydney on charges of receiving and stealing car parts, wheels, and other valuables, which were later sold on eBay demonstrated that capable guardianship along with the presence of law enforcement can be an effective tool to reduce Internet fraud (AAP 2004:1). Indeed, Internet auctions can aid in detecting the sale of stolen goods. It is easier for law enforcers to monitor cyber networks than networks of fences.

(9)  

**Phishing**

**Motivated Offenders:** Offenders of this type of fraud are predominantly motivated by greed because the modus operandi is usually based on financial gain. The techniques used are most commonly applied through the appearance of trusted senders, such as banks, Internet service providers, online retailers, and credit card companies.

**Availability of Suitable Targets:** The increase in customers and the proliferation of Internet commerce, commercial websites, and online financial securities has brought about a dramatic increase in the number of suitable targets.

A recent report by the Anti-Phishing Working Group (APWG) found that the financial sector is the most highly targeted industry (Maier 2004). A number of legitimate and globally recognised companies have also been targeted. The second most attractive industry sector targeted by phishers is the retail industry and as the report suggests, this is primarily the online auction house eBay.
Table 5.2  Phishing Attacks by Targeted Company: December 2003 - May 2004

<table>
<thead>
<tr>
<th></th>
<th>May - 04</th>
<th>April - 04</th>
<th>Mar - 04</th>
<th>Feb - 04</th>
<th>Jan - 04</th>
<th>Dec - 03</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citibank</td>
<td>370</td>
<td>475</td>
<td>98</td>
<td>58</td>
<td>34</td>
<td>17</td>
</tr>
<tr>
<td>EBay</td>
<td>293</td>
<td>221</td>
<td>110</td>
<td>104</td>
<td>51</td>
<td>33</td>
</tr>
<tr>
<td>US Bank</td>
<td>167</td>
<td>62</td>
<td>4</td>
<td>0</td>
<td>22</td>
<td>0</td>
</tr>
<tr>
<td>Paypal</td>
<td>149</td>
<td>135</td>
<td>63</td>
<td>42</td>
<td>10</td>
<td>16</td>
</tr>
<tr>
<td>Fleet</td>
<td>33</td>
<td>28</td>
<td>23</td>
<td>9</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>VISA</td>
<td>21</td>
<td>0</td>
<td>7</td>
<td>8</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>AOL</td>
<td>17</td>
<td>9</td>
<td>10</td>
<td>10</td>
<td>35</td>
<td>4</td>
</tr>
<tr>
<td>Lloyds</td>
<td>17</td>
<td>15</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Barclays</td>
<td>15</td>
<td>31</td>
<td>11</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Westpac</td>
<td>12</td>
<td>17</td>
<td>10</td>
<td>0</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: Maier 2004:2

Table 5.2 shows the top ten companies most targeted by phishers from December 2003 until May 2004. The statistical data presented above also show that the incidence of phishing is increasing exponentially. This may coincide with estimates of increased Internet usage.

**Absence of Capable Guardianship:** Among the various forms of fraud that have extended to the Internet, phishing has emerged distinctly as a result of computer-mediated technologies. Like many forms of Internet fraud, the absence of capable guardianship contributes to its exponential growth; however, there are approaches in place to control this type of crime. For example, the Anti-Phishing Working Group is an organisation that documents trends in phishing, identifies targets and contributes to providing awareness and education to Internet users.
CHAPTER 5: THEORIES OF CRIME AND CRIMINALITY AND THEIR RELATIONSHIP TO THE INTERNET

5.8 SUMMARY

This chapter identified that few theories are robust and have explanatory power to a diverse range of cyber crimes. It has been demonstrated that differential association has partial support as an explanation of hacking, Internet piracy rings, and Internet paedophile rings because not all forms of criminal behaviour on the Internet are achieved through associations and learned behaviour. This was particularly evident through online auction and online securities fraud, which showed that many perpetrators act alone and are not influenced by others through association. Second, many people who are exposed to opportunities to participate in criminal behaviour on the Internet are law abiding. While a lot of evidence of social support for crime in cyberspace is apparent in the literature, the largely submerged nature of the phenomenon means we cannot be sure how much is the work of cyber-socially networked criminals and how much is the work of isolated individuals.

The analysis found that strain theory is limited in explaining cyber crime. Merton’s theory provides partial support for understanding hacking, piracy, and the sale of child pornography through innovation although much cyber crime is not committed in the pursuit of wealth. The analysis showed that Internet frauds are most amenable to this mode of adaptation although it was difficult to determine the extent to which strain influenced the decision to carry out these crimes. The rebellion mode was instructive for crimes such as hacking and offences by disgruntled employees in that the culturally held goals of success and wealth and legitimate means of achieving them were rejected in protest.

There was mixed support that techniques of neutralisation are used to justify the behaviour of cyber criminals. The analysis showed strong support that denial of responsibility is used by hackers and child pornographers but less so with piracy and fraud. The findings suggest that additional motivations are used to carry out crime that cannot be explained through techniques of neutralisation. Furthermore, some examples showed that there are cyber criminals who use other justifications for their behaviour that cannot be explained by this theory.

Gottfredson and Hirschi’s general theory explains only a limited range of cyber crimes. While the analysis found that low self-control is a better predictor for crimes such as
hacking, piracy, and Internet sex crimes against children, it was difficult to explain Internet fraud through low self-control. However, a predisposition to a low level of self-control may mean that the Internet provides further opportunities for offenders that are not limited to the physical world (Stanley 2001). Each of the crimes tested (hacking, Internet piracy, and sex crimes against children and youth, and Internet fraud) demonstrated that age is not a constraint. In fact, many users are first-time offenders in their thirties, forties, and fifties. However, it must be cautioned that few systematic age correlational data are available.

The most robust approach proved to be routine activity theory, which explains cyber crime as a result of three factors: a supply of motivated offenders, the availability and attractiveness of suitable targets, and an absence of capable guardianship. Its explanatory power was well sustained for hacking, piracy, Internet sex crimes against children, securities fraud, auction fraud, and phishing.

Many of the cases in this chapter suggest that trust should be viewed as an inherent element in analysing criminal behaviour on the Internet. The argument is not that individuals' levels of trust have changed, rather that the Internet has provided a means for trust to be abused in a number of different ways – from communication of individuals in a chat room to the facilitation of crime such as fraud, espionage, and hate crimes. The following chapter will consider the function of trust within the Internet environment and demonstrate how abuse of trust can lead to unlawful behaviour and the commission of diverse forms of crime on the Internet.
CHAPTER 6: CRIMINAL BEHAVIOUR ON THE INTERNET – THE USE OF TRUST

6.1 INTRODUCTION

Chapter Five distilled an important body of research about criminal use of the Internet. The most robust explanation proved to be routine activity theory, which explains cyber crime as the result of three factors: a supply of motivated offenders, the availability and attractiveness of suitable targets, and absence of capable guardianship. Chapter Five also showed that global access to the Internet facilitates communications between like-minded individuals through developing networks, association, and learned behaviour in furtherance of criminal opportunities. It found that this occurred most commonly through the hacking, communities and piracy, and child pornography rings. Chapter Five also identified the importance trust plays in establishing and developing networks and found that this is attributable to the Internet's anonymity, ease of access to a global audience and like-minded individuals, and borderless space.

This chapter will illuminate the strategies that cyber criminals use to establish and exploit trust on the Internet with a focus on Shapiro’s (1990) theory of trust violation. First, section 6.2 introduces Shapiro’s trust violation theory. Second, sections 6.3-6.6 applies four strategies that Shapiro identified as important precursors to trust violation (lying, self-dealing, corruption, and role conflict) to a broad range of cyber crimes.

6.2 TRUST VIOLATION THEORY

Shapiro (1990:350) was one of the first scholars to build on Sutherland’s use of the concept of trust by demonstrating ‘... how fiduciaries exploit the structural vulnerabilities of trust relationships through deception, self-interest, and, to a lesser extent, incompetence’. Shapiro’s research draws attention to the way norms of trust are violated by white-collar offenders. According to Shapiro (1990:350):

98 Chapter Three noted Cressy’s (1953) analysis of trust violation by embezzlers.
99 Shapiro (2002) carried out a study which explored conflict of interest in the private practice of law and the perceptions and attitudes of lawyers based in Illinois.
Instead of cultivating mechanical technology to break into a secured building, trustee "burglars" cultivate social technology to become trusted organisations or insiders in organisations rich with opportunity for exploiting their positions for personal or corporate advantage.

The strategies of trust violation applied successfully to analyse securities fraud and various other forms of white-collar crime were lying, self-dealing, corruption, and role conflict.

In an example of terrestrial self-dealing, Paik Won Ku abused his position of trust and responsibility as head of South Korea’s Securities Supervisory Board for financial gain. Shameen (1996:1) reports that:

… Paik Won Ku had the last word on which companies could go public or launch rights issues. That privilege made him a powerful man. Financing is relatively difficult to get in South Korea, especially for smaller firms, and when a company does get it, it is expensive. A long line exists, therefore, to raise money through the stock market. Not surprisingly, many businesspeople are willing to pay to jump the queue. According to the authorities, some did just that, and the people they paid off were Paik, 56, and a senior Finance Ministry official, Han Taik Soo, 46. In early June, police arrested the pair.

It has been estimated that Paik profited in excess of US$140,000 from ten companies. In addition, Taik was closely involved with one firm and received a substantial amount for facilitating their acquisitions (Shameen 1996:2) According to Shameen (1996:1):

Once the company goes public, the shares are sold at a huge profit. Companies such as Korea Data are given preferential treatment because their shares are quickly snapped up by in-vestors [sic].

Chapter Five underscored many ways in which trusted insiders exploit positions for personal advantage. Trust violation theory therefore provides a strong tool for analysing whether it has explanatory power for different forms of cyber crime. The following subsections apply strategies of lying, self-dealing, corruption, and role conflict to a broad range of cyber crimes.

6.3 LYING

Shapiro (1990) identified lying as one of the strategies that individuals use to establish and exploit trust. Shapiro (1990:350-351) asserts that "because of information asymmetries, virtually all types of fiduciary relationships are vulnerable to misrepresentation, deception, exaggeration, omission, distortion, fabrication, or
falsification of information by those in positions of trust'. Shapiro provides a range of examples to validate her theory: misrepresentation of the use of charitable funds to underdeveloped countries; fabrication of data for experiments; declaring a fictional account of a heroin addict to be a work of non-fiction (it was awarded a Pulitzer Prize); and falsification of test results by pharmaceutical companies.100

The various ways in which people lie in order to commit a crime on the Internet was briefly illustrated in Chapter Five: Internet predators who lie about their age in order to meet children off-line in furtherance of illegal activity; a Nigerian fraud scam which deceives people into parting with money or providing account details by falsely offering a fee for assistance in transferring funds; auction fraud which can involve money sent by the successful bidder to the seller while the goods are never received; misrepresenting true intentions when communicating in chat rooms as a prelude to harassment and cyber stalking; and deceiving investors by falsely declaring that a company is about to announce a new discovery, resulting in a company’s share price to rise.

This sub-section discusses five types of cyber crime: phishing, auction fraud, Internet sex crimes against children and youth, misuse of personal information, and cyber stalking to show whether these crimes entail the violation of trust.

6.3.1 Phishing

Counterfeit websites violate trust through deception and misrepresentation because in many cases the user believes that the website is legitimate and proceeds to input information and/or to complete transactions that may include disclosing credit card numbers and bank account details. Counterfeit websites can operate through the WWW or direct contact via e-mail in the form of hoax e-mails, or newsgroups. According to the Internet Fraud Watch (2000:1), ‘Web sites are the most common way that consumers are solicited for fraudulent Internet offers, but the statistics [also] reveal an increase in the number of initial contacts made by con artists in newsgroups’.

100 Braithwaite’s (1984) in-depth study into the pharmaceutical industry provides examples of this behaviour.
Attacks by phishers have targeted customers who have access to Internet banking facilities. For example, a message may indicate to the customer that their bank’s website is experiencing technical difficulties and instructs the customer to click on a link to a ‘temporary’ website and provide their account details or password. This method manipulates the customer into accessing a counterfeit website that exposes their personal and banking information, giving the perpetrator access to account details in furtherance of criminal activity.

The power of branding is likely to have a substantial effect on a user’s decision to conduct business on the Internet (see Newman and Clarke 2003). According to Maier (2004:2), organised syndicates are ‘... playing on the trust people already have in their banks, their (Internet Service Providers), [and] eBay ... They hijack the brand because people trust the brand. They trust e-mails they get from their bank’ (cited in Sullivan 2004:2).

Figure 6.1 shows a rise in the number of brands hijacked by e-mail phishing attacks in the US. Although these statistics only represent the number of reports made to the Anti-Phishing Working Group (APWG), they nevertheless underscore the fact that perpetrators identify with those global brands that users easily identify with and trust. Brand reputation and awareness of brands is an important factor in building initial trust on the Internet (Centeno 2002:24).

---

101 'The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating ... identity theft and fraud ... The organisation provides a forum to discuss phishing issues, define the scope of the phishing problem in terms of hard and soft costs, and share information and best practices for eliminating the problem' (www.antiphishing.org 2005:1).
In a recent example of a counterfeit website, an e-mail was sent to a company address with the following details:

From: "Westpac support" billing@westpac.com.au
To: <info@antiquesonline.com.au>
Sent: Sunday, January 25, 2004 2:17PM
Subject: Official notice to all Westpac users.

Dear Valued Westpac Customer!

Due to the increased fraudulent activity within our site we are undertaking a review of our member accounts. You are requested to visit our site by following the link given below. This is required for us to continue to offer you a safe and risk free environment to send and receive money online. Be sure to enter both Customer Account No & Password otherwise your account will not be verified and your access to the account will be blocked.

Thank You

http://olb.westpac.com.au

Copyright 2004 – Westpac Banking Corporation

ABN 33 007 457 141

(Source: Antiques Online 2004)

This e-mail was not legitimate. The sender of the e-mail attempted to represent it as legitimate by providing navigation to a (illegitimate) website to strengthen its...
authenticity, an Australian Business Number (ABN), by using language that replicates official messages, and by purporting to be from a reputable and legitimate source, in this case, Westpac Banking Corporation. According to APWG, 'by hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5 per cent of recipients to respond to them' (cited in Maier 2004:1).

In a recent case of phishing, one Helen Carr was indicted by a federal grand jury in the United States for participating in an Internet fraud. There were numerous ways in which Carr and her co-conspirators carried out the conspiracy, which operated over a 14-month period:

- The object of the conspirators' unlawful agreement was to steal and to obtain by fraudulent means unauthorised access devices, that is, credit card numbers, from persons using AOL as their Internet Service Provider (ISP).

- It was a part of the conspiracy to obtain by fraudulent means the screen names and passwords of AOL subscribers. For example, the conspirators sent fake 'InstaKiss' messages to AOL subscribers. These messages falsely told AOL subscribers that, to receive an InstaKiss from a secret admirer, they had to input their screen name and password into a form, which would later provide this information to the conspirators. The conspirators then used this information to log into AOL, where they then used spamming software to send false and fraudulent mass e-mails ('spam') to other AOL subscribers.

- It was further a part of the conspiracy to send mass e-mails to AOL subscribers through the United States. These false e-mails, purporting to be from AOL's Security Department, advised that AOL's last attempt to bill the subscriber's credit card was declined and that the subscriber needed to supply AOL with updated credit card and account information. To do so, the subscribers were directed to click upon an enclosed link in the e-mail message to visit an AOL web page.

102 According to Litan (2004), 'More than 1.4 million users have suffered from identity theft fraud, costing banks and card issuers $1.2 billion in direct losses in the past year'.
It was further a part of the conspiracy that AOL subscribers clicking upon the link were directed to a fictitious ‘AOL Billing Center’ web page prepared and uploaded by the conspirators to Internet sites providing free space for web pages. This fake AOL web page directed the subscribers to input their names, addresses, telephone numbers, screen names, passwords, and current and new credit card account information, in order to avoid having their AOL accounts terminated (United States of America v. Helen Carr. USDC Eastern Dist. Virginia, Case No. 1029 (b)(c) and 1029 (a)(3) (McNulty 2003b:2-3).

In order for the crime to be carried out successfully, the alleged conspirators relied heavily upon communicating with each other via telephone and the Internet as well as exchanging information, tools, and files (McNulty 2003b:2). While misrepresentation and lying were central to this type of fraud, it also showed that group association played a role in the organisation of the crime. Moreover, the perpetrators focused on a trusted and recognised brand such as AOL to deceive AOL customers through these strategies.

The FTC recently took action against a man who was involved in a fraud scam (FTC v. C.J., No. CIV-03-5275-GHK) (RZx) (C.D. Cal. July 24, 2003). According to the FTC, the defendant sent spam mail purporting to be from America On Line (AOL) ‘... that directed consumers to a “look alike” AOL website where the defendant obtained financial information used for his own online purchases’ (Beales 2004:5). In this example, the defendant deceived AOL customers and AOL for the purposes of financial gain. AOL customers trusted that the AOL site was legitimate and therefore provided personal information and account details.

Cella and Stark (1997:822) provide an account which demonstrates the way lying and misrepresentation are central to personal gain:

At very little cost, and from the privacy of a basement office or living room, the fraudster can produce a home page that looks better and more sophisticated than that of a Fortune 500 company. Thieves have many tools at their fingertips; even a link can serve as an aid for an investment ruse. Just like visiting a site, using a link is usually free, so the fraudster might even provide a link to the home page of the SEC next to a representation that a particular security has received “approval” from the SEC ...

In December 2002, it emerged that fraudsters set up a counterfeit website and mimicked the American online auction house eBay.com in order to steal credit card numbers from
previous eBay users. Thompson (2002:1) points out that ‘the recipients were told there had been a problem with billing and were asked to re-enter their card details at a site called ebayupdates.com’. Despite the website closing down within hours, this case demonstrates that the offenders misrepresented information to eBay users through deception for personal financial gain.

The strategies of misrepresentation, deception, and familiarity appear central to obtaining information and funds from people and companies by means of phishing. These examples have also shown that branding is a powerful mechanism used to deceive legitimate users who have traditionally placed trust in brands that can now be easily disguised through technology as illegitimate.

6.3.2 Auction Fraud

Auction fraud can be carried out in a diverse range of ways. Similarly, trust may be violated on online auctions in numerous ways. These can be identified as:

- Goods being paid for and not being delivered.\(^{103}\)
- Goods being received and not paid for.
- Deceiving the buyer of the true value and/or quality of the goods.
- Goods that are black-market goods, such as pirated copied software or CDs without warranty and imitation brands, sold as legitimate brands.
- Goods that are stolen property.
- The seller driving up bids to increase the price of the item or, alternatively, individuals using different aliases to drive up the bid, which can create discomfort for other bidders and therefore alienate other prospective buyers.
- Payments through fraudulent means, such as stolen credit card details or fraudulent cheques.

\(^{103}\) Mrozek (1999) reports of a case of ‘… Robert J. Guest [who] pleaded guilty in United States District Court in Los Angeles to charges of bilking people who bid on various items offered at auction on the
CHAPTER 6: CRIMINAL BEHAVIOUR ON THE INTERNET – THE USE OF TRUST

It is through these different methods that perpetrators violate trust (Snyder 2000). A survey conducted in 1998 by Commercenet identified lack of trust and concern regarding payment mechanisms as the top reasons for not purchasing on the web (Lombardi 1998 cited in Newman and Clarke 2003:35). These issues are still commonly identified despite recent developments by Internet auction houses to develop strategies to regulate online bidding processes and trust seals to increase confidence among consumers (see Snyder 2000; Wible 2003) (these issues will be further explored in the following chapter).

These techniques suggest that various strategies, such as lying, deception, distortion, fabrication, falsification of information, and stealing are used to defraud legitimate participants of online auctions (Snyder 2000; Newman and Clarke 2003). In a controlled experiment which examined the value of reputation on eBay, Resnick et al. (2002:2), noted ‘... the temptation to sellers to misrepresent products, e.g., exaggerate their quality or misrepresent their provenance, are great’. In the factors identified above, a level of trust was violated in the transaction between the prospective buyer and seller.

A recent example that demonstrates lying and deception involved a Sydney man bidding online for a laptop computer. Having identified a particular type of laptop computer to purchase on eBay, the individual was convinced by the seller to buy privately, as he had established a level of trust with the buyer. After initially communicating via the Internet followed by telephone communication, the buyer transferred the money for the computer into the seller’s account; however, the purchaser never received the laptop (Adams 2003).

In this case, a level of trust developed between the purchaser and seller during their communication via e-mail. The buyer revealed that the seller’s knowledge of the product convinced him to buy offline, and the seller offered him a reduced price for the computer if it was traded offline. A number of cases discussed below provide a glimpse into the ease with which fraudsters exploited trust through various strategies.

eBay Internet auction web site, taking approximately [US]$37,000 from consumers and never delivering the purchasing goods.

104 eBay.com is an online auction web site where individuals can buy, sell and trade goods in a global market on the Internet.
CHAPTER 6: CRIMINAL BEHAVIOUR ON THE INTERNET – THE USE OF TRUST

In the case of FTC v. Hare, the Federal Trade Commission (FTC) filed a civil suit on March 30, 1998 in the United States District Court alleging that Hare violated the FTC Act by offering merchandise through auction houses without delivering the advertised goods (No. 98-8194-CIV SD Fla. Sept. 8, 1998). It was reported:

Judge Daniel T.K. Hurley acted on a complaint filed by the Federal Trade Commission alleging that Craig Hare used online auction houses to offer new and used computers for sale. After “successful bidders” paid as much as $[US]$1,450 per computer, Hare provided them neither the computer nor a refund (FTC 1998:1).

The Federal Judge issued a temporary restraining order banning Hare from using the Internet to advertise, market, or sell any goods or services, and froze assets (FTC 1998:1).

In a similar example in the United States, 43-year-old Jeffrey P. Butcher, was found guilty of multiple offences, including wire fraud, identity theft, and credit card fraud. Butcher advertised a range of computer products for sale on eBay; however, he failed to deliver the items to more than 43 successful purchasers. Butcher deceived eBay customers because he was aware that the goods would not be delivered, although he continued to advertise the goods and accept payment, thus not fulfilling his obligations to the purchasers (White and Kern 2004).

Internet auction scams can also involve additional forms of fraud. Jeffrey L. Martin was convicted on theft charges. Martin assumed someone else’s identity to offer goods for sale via eBay and accepted payment for the goods; however, the defendant failed to deliver the goods. Approximately 50 people had fallen victim to Martin’s scam, which resulted in excess of US$9000 loss (Bethel 2000 cited in FTC 2000). Martin was sentenced to six years in prison, six years probation, was ordered to pay victim restitution, and was banned from using the Internet while on probation. In this example, Martin assumed the identity of another individual through falsification of information, misrepresented his intentions, and failed to deliver the goods.

These examples have shown that the Internet appears to have made it easier for offenders such as Butcher and Martin to deceive victims and gain financially from such

105 There appears to be an increase in the number of users persuaded to trade off line through deceptive strategies.
deceit through lying, deception, and misrepresentation. These examples also appear to show that eBay users trust eBay to provide ways that minimise their risk of becoming victim to fraud on the Internet. Clearly these examples underscore the trusted position of eBay to its customers.

6.3.3 Internet Sex Crimes against Children and Youth

Chapter Five demonstrated that Internet sex offenders violate norms of trust most commonly through lying and misrepresentation. In particular, sub-section 5.3.2 showed that offenders who communicate with children on the Internet may deceive them by misrepresenting their accurate age and at times their gender. In one example, a 47-year old male, Paul Brown Jr. posed as a 15-year-old male when exchanging e-mails with a 12-year-old female. Brown Jr. attempted to convince the young girl to make pornographic videos of herself. Brown Jr. was arrested and police discovered that he was applying techniques of deception to more than 10 other girls across the United States (Denning 1999:108). Individuals also use ‘truthful’ methods of electronic seduction that may not be viewed as criminal until they arrange to meet with a child in the physical world, harass, or send illicit images of children in furtherance of criminal activities.

Another example involved a 64-year-old father and postman from the United Kingdom, who was arrested in 2003 as one of the world’s most prolific Internet groomers (see Morris 2003). Kingston Crown Court heard that the accused was drawn in by the excitement of chat rooms. He posed as a young teenage boy, deceiving young girls and sending them naked photographs of him. In addition, he telephoned young girls, sent harassing messages and also told a number of girls that he wanted to rape them (Morris 2003). The Internet dramatically enhanced the capacity for the offender to lie, deceive, harass, and terrorise young girls and to elude law enforcement agencies for some time.

In a recent sting operation by detectives of Ada County, Idaho, in the US, nine men faced charges of enticing children in Internet chat rooms. It was alleged that nine men attempted to solicit sex from children and arranged to meet them offline in a disclosed location. The men were arrested when the detectives met the alleged offenders after
posing as teenagers in the chat room (Orr 2004:1). It was alleged that the men claimed that no harm would be done, as the objective was to only meet the teenagers (Orr 2004). In this example the police were the deceivers by posing as young children in the chat rooms.\footnote{107}

### 6.3.4 Misuse of Personal Information

Misuse of personal information takes many forms (Grabosky et al. 2001:159). Although misuse of personal information is not a new form of crime, the Internet’s global accessibility, the voluminous amounts of personal information accessible through it, the way it can be distributed and intercepted, and the ease with which criminals can manipulate and misappropriate information over a relatively short space of time, make this an attractive means in furtherance of criminal activities. Grabosky et al. (2001:160-8) examine various motives for theft of personal information, which include: social control, litigation, commercial exploitation, voyeurism, political protest or intimidation, stalking, harassment, and mistake. This section will focus on commercial exploitation to demonstrate the strategies used to establish and exploit trust.

(a) **Commercial Exploitation**

Of the many different strategies employed to establish and exploit trust for commercial gain, misappropriation and falsification of information is fairly common. In 2000, the FTC filed a suit against Toysmart.com, a web site which sells children’s toys (FTC v. Toysmart.com, LLC, No. 00-11341-RGS, (D. Mass. filed July 10, 2000, amended July 21, 2000)). According to the FTC (2000:1), Toysmart’s action included:

> ... misrepresenting to consumers that personal information would never be shared with third parties and then disclosing, selling, or offering that information for sale in violation of the company’s own privacy statement.

Information collected by Toysmart.com on customers was quite extensive and included names, family profiles, billing information, shopping preferences and e-mail addresses. The FTC (2000:2) note:

\footnote{106 Persons under the age of consent and undercover law enforcement officers may also misrepresent their ages.}

\footnote{107 This is recognised as a legitimate method of police investigation in some countries.}
Since September 1999, Toysmart has posted a privacy policy which states that information collected from customers will never be shared with third parties.

Toysmart.com experienced financial trouble and attempted to sell its database of information, however, the Web site’s policy indicated that it would never disclose personal information to third parties (FTC 2000). Toysmart.com clearly invaded the privacy of its customers and violated a level of trust, contrary to the company’s privacy policy. Although the FTC settled their charge against Toysmart.com, this example demonstrates the ease with which companies can misrepresent their privacy policies and abuse the trust of their customers who provided information on the basis that a privacy policy ensured privacy of information.

An example that demonstrates misuse of personal information for commercial exploitation involved a financial institution.

In 1999, the Attorney-General of Minnesota alleged that a bank sold customers’ private financial details to a telemarketing company for US$4 million plus commissions. The details were extensive and were reported to have included telephone and social security numbers, marital status, homeownership, bankruptcy status, credit card details, bank account balance and information on recent transactions (Grabosky et al. 2001:163-4).

In an example that demonstrates misrepresentation and deceptive spam, ‘ReverseAuction [which offers online auction services] allegedly agreed to comply with eBay’s User Agreement and Privacy Policy, only to harvest eBay users personally identifying information and spam eBay members with a message stating that their user ID’s “will EXPIRE soon”’ (FTC 2003). The FTC (2003) found that ReverseAuction obtained customer information through its competitor eBay to assist in the marketing and promotion of its new auction website illegitimately. The FTC (2003:1) found that:

ReverseAuction’s conduct ... has injured consumers throughout the United States by invading their privacy; using their e-mail addresses, eBay user IDs, and feedback ratings for purposes other than those consented to or relied upon by such consumers, including the purpose of sending them unsolicited commercial e-mail solicitations; causing them to believe, falsely, that their eBay user IDs were about to expire; and undermining their ability to avail themselves of the privacy protections promised by online companies. In agreeing to become registered eBay users and entrusting eBay with their e-mail addresses, user IDs, and feedback ratings, eBay's customers reasonably expected and relied upon the compliance of all eBay registered users, including ReverseAuction, with the terms and conditions of eBay's User Agreement.
CHAPTER 6: CRIMINAL BEHAVIOUR ON THE INTERNET — THE USE OF TRUST

ReverseAuction violated the eBay privacy agreement and moreover violated the privacy of eBay's members' personal information. It is important to point out that eBay provides assurances that personal details will be protected from theft by third parties, although this case highlights the vulnerabilities of their system to guard against such strategies in furtherance of criminal activities. The misuse of personal information also highlights the ease with which people can obtain access to personal information through strategies of deception and misrepresentation over the Internet.

6.3.5 Cyber Harassment and Stalking

Trust relationships can be formed on the Internet through e-mail, chat rooms, bulletin boards, and newsgroups. These methods of communication can also provide the means to exploit trust in furtherance of harassment or cyber stalking through misrepresentation. A number of techniques are used to identify and pursue victims: direct contact via e-mail; harassment abuses through live chat rooms; providing false information about the victim and posting it on news groups for wider distribution; establishing a web page on the victim with personal and spurious information; and assuming the victim's identity online in chat rooms. Many examples exist where individuals have fallen victim to this type of crime. According to Cyberangels (2000), approximately 63,000 Internet stalkers monitor the Internet stalking more than 470,000 targets (cited in USDOJ 2000:1).

As shown in Chapter Five, cyber stalking can extend from the virtual world into the physical world and the physical world to the virtual world. For example, in the US, a physical encounter between two individuals began in the physical world, which later led to harassment through the Internet and via e-mail. The victim was a prostitute and met the defendant while working. The defendant claimed that a personal relationship began (the victim maintained it was a professional relationship), which eventually led to harassment and stalking. It was alleged:

After this paid sexual encounter, the victim gave defendant her website address. During the next two or three months, defendant called the victim once or twice a day at her work. The victim also gave defendant her personal e-mail address and defendant began to e-mail her there ... [After another physical encounter and a meeting with the defendant] ... the victim was contacted by the administrator of the website and told her that the defendant was becoming a nuisance because of his constant calls and e-mails ... despite the restraining order, defendant e-mailed and telephoned the victim [which appeared to be threatening] ... defendant
was charged with stalking ... (The People, Plaintiff and Respondent, v. James Charles Koller 2003).

This example illustrates that trust was established through a professional or personal relationship and was continued by communication through e-mail. However, the perpetrator violated trust and exploited information for the purposes of harassment and stalking. Furthermore, it can be seen that the nature of the Internet can facilitate the exploitation of trusted relationships.

In summary, crimes such as fraud, identity theft, Internet sex crimes against children and youth, and cyber harassment and stalking are based on strategies of deception, lying, misrepresentation, and falsification of information. A number of the examples shown suggest that victims assumed a level of trust and familiarity, which allowed the offender to abuse their position and violate trust in order to carry out the crime. It is important to point out that trust is one of the central elements in these examples of cyber crime because in each case the offender used trust to exploit victims.

6.4 SELF-DEALING

Among the different types of strategies that individuals employ to violate norms of trust, self-dealing is used as a means for personal gain. Shapiro (1990:352) explored self-dealing as an element of stealing where she asserts the opportunities are vast. According to Shapiro (1990:352):

Agents are not merely the custodians of property; many are entrusted with discretionary responsibility for the disposition of property and the allocation of corporate largess. Some wayward trustees exercise this responsibility for personal benefit; they “self deal”.

Examples of self-dealing in the physical world include government officials directing business to firms in which they have an interest or are connected, the exchange of grades for sexual favours, and misuse of information for financial gain through insider trading or securities fraud (Shapiro 1990:352). The example of Simon Hannes (discussed in Chapter Three) is applicable to self-dealing as he used his knowledge of
insider information through his position as an executive of an investment bank to trade in shares from which he profited.\textsuperscript{108}

The following sub-section explores three forms of cyber crime that may explain self-dealing on the Internet: misuse of personal information, identity theft, and insider trading. It is important to note that such examples must involve violation of trusted relationships committed by insiders rather than outsiders.

6.4.1 Misuse of Personal Information

Two cases that exemplify misuse of personal information and self-dealing involved officers from the Metropolitan Police and in the second case, an employee of American Express. In the first case, two officers obtained personal information on a third party from the Police National Computer (PNC). It was alleged that the officers were seeking information on the name of a vehicle owner for private interest. Although the officers had authorised access to the PNC, the information was used for illegal purposes (DPP v Bignell (1998) 1 Cr.App. R. 1). The officers were convicted although they were successful on appeal. The courts debated on the issue of whether the officers’ actions contravened Section 1 of the Computer Misuse Act 1990 and the Crown argued that it did not and access was authorised.

In another case, one of the accused, an employee of American Express illegally obtained account information in furtherance of fraud and forgery. The accused was a credit analyst who had authority to access personal information only on accounts she was allocated. It was alleged however, that the accused exceeded authorisation by obtaining personal information on additional account holders from the database. Along with her co-accused, it was alleged that they conspired to defraud the victims by encoding forged credit cards and withdrawing substantial amounts of money from ATM machines (\textit{Regina v. Bow Street Stipendiary Magistrate, Ex parte Government of the United States of America} [2000] 2 AC216).

\textsuperscript{108} Similar examples may exist in the virtual world. Due to the anonymous nature of communication on the Internet and the ease with which criminals can hide their tracks, the identification of this type of strategy may be difficult to prove, however.
6.4.2 Identity Theft

Online identity theft has often been referred to as ‘the crime of the new millennium’ (Hoar 2001:1). Identity theft is not new. However, digital technology has opened up a plethora of opportunities for would-be identity fraudsters to apply their methods in new and sophisticated ways. Identity theft is most commonly recognised when an individual (criminal) uses another person’s personal information in order to take on that person’s identity; in many cases it is often committed to carry out an additional form of crime.

Identity theft occurs in diverse ways: ranging from the sharing of personal information, to intentional theft of purses, wallets, mail, or digital information, to door knocks, and individuals scanning rubbish to find personal identifiable information (Hoar 2001:2). Individuals can collate data from a range of sources on the Internet through unauthorised methods such as hacking, to e-mail scams, surveillance of chat rooms, news groups, relay-chat, and the use of Trojans and software programs. The Internet acts as a conduit for the collation and dissemination of personal identifiable information, which allows the perpetrator to move across the globe creating new victims and setting up new accounts at a rapid pace (Barnes 2000).

A number of identity theft cases involving the Internet have been prosecuted in the United States. However, only a few cases have involved individuals entrusted with discretionary responsibility and exploit trust relationships. A 34-year old United States Army Captain, Michael F. Kimble, who was sentenced in 2003 for identity theft, illegally accessed the names, birth dates and Social Security numbers of six people to open credit card and bank accounts in their name over the Internet (McNulty 2003d:1). A civilian serving under Kimble was one of the victims as Kimble used his access to obtain personal information from defence records. McNulty (2003d:1) notes that ‘to maintain control over the accounts, the defendant used a commercial mail drop ... as the address for the accounts ... [and] then transferred his own personal debts to the credit cards he had illegally obtained’. In excess of US$45,000 was transferred in the names of the victims. This example underscores Kimble’s abuse of trust through his position as Army Captain and misuse of personal information in furtherance of identity theft.

A recent case of identity theft and self-dealing involved an employee of a New York State Insurance Fund. The defendant, 38-year-old Valerie Schoffner was charged with accessing personal information from office files in furtherance of obtaining goods and
services, some of which were ordered over the Internet. It was alleged that the defendant obtained personal information such as names, addresses, and social security and telephone numbers of employees and customers of the Insurance Fund while working in administration for the company. In addition, personal information Schoffner illegally accessed was also provided to accomplices and later used to illegally obtain goods and services.

More than US$100,000 worth of goods and services stolen by the defendant and her accomplices have been identified by investigators (Comiskey 2001). In this case, Schoffner was willing to violate other employees’ and customers’ trust through her responsibility as a public employee, who misused personal information for criminal purposes. According to New York Attorney General, Eliot Spitzer (2001), the result is ‘... a shameful violation of trust by a public employee’ (cited in Comiskey 2001).

6.4.3 Insider Trading

The Securities and Exchange Commission (SEC) took action against a group of individuals who were allegedly involved in a global insider-trading scheme on the Internet. Although insider trading is not a new form of crime, this example highlights the ease with which the Internet facilitates communication between like-minded individuals for the purpose of criminal activities. This case also illustrates one form of abuse of trust by four of the defendants who were entrusted with discretionary responsibility through their position as ‘either principals or employees of firms that are registered with the Commission as broker-dealers’ (Swan 2000:3) and who used their insider knowledge to self-deal.

The SEC alleges:

In mid-1997, defendants John Freeman, James Cooper and Benton Erskine “met” in an internet chat room devoted to the performance of a stock in which all three had invested and lost money. In the course of their on-line communications, Freeman informed James Cooper and Erskine that he worked at Goldman Sachs & Co., Inc. (“Goldman Sachs”), a major international investment bank headquartered in New York. The three then agreed upon a plan to profit from any inside information Freeman could garner about merger and acquisition transactions being planned by Goldman Sachs’ clients (Swan 2000:2-3).

Over a two-year period, Freeman, Cooper, and Erskine, along with co-workers, friends, and associates, were involved in one of the most widespread networks of illegal trading
on the Internet. The trustee relationship was between the firm in which one of the
defendants was employed and their clients as the information about acquisitions was
used to provide insider information for the purpose of self-dealing. The SEC maintains
‘the defendants’ scheme grew to involve insider trading in the securities of over 20
different companies by dozens of individuals, who reaped illegal profits in excess of $8
million’ (Swan 2000:3).

These examples support Shapiro’s (1990) theory by demonstrating the ease with which
people in positions of trust engage in self-dealing on the Internet through misuse of
personal information, identity theft, and insider trading.

6.5 CORRUPTION

According to Shapiro (1990:352-3), corruption ‘... represents an alternative form of
theft, in which positions of trust are essentially rented or sold to outsiders’. Among the
various examples that Shapiro provides to demonstrate ways in which white-collar
offenders establish and exploit trust is ‘... access to inside information with which
fiduciaries are trusted’ (Shapiro 1990:352), which is an important part of corruption.
Corruption is rarely detected because neither party to the transaction is a victim.

6.5.1 Espionage

A former employee of Corning Incorporated, Xingkun Wu, was charged with violations
pertaining to Theft of Trade Secrets. It was alleged that in 2000, Wu downloaded
confidential information from Corning Incorporated prior to leaving for a new job with
SpectraSwitch. According to The United States Department of Justice (DOJ), the
Criminal Complaint alleges that ‘... Wu knowingly attempted to convert a trade secret to
the economic benefit of someone other than its owner, knowing that the offence would
injure Corning Incorporated as the owner of the trade secret (Ahearn 2001:1). It was
alleged that Wu may have intended to return to China, his native country. Wu’s insider
knowledge of the company gave him access to information which he misused for
personal gain.

The Federal Appellate Court upheld the criminal conviction (United States v. Camp and
conspired to steal trade secrets with Caryn Camp, an employee of Idexx, a rival
company. In 1997, Martin was unsuccessful in negotiating with Idexx to form a joint venture for research of the HIV and FIV viruses (Dilworth 2001:1). One year later, Camp applied for a position with Wyoming DNA Vaccine, which emerged as the beginning of e-mail exchanges between Martin and Camp. The correspondence between Martin and Camp began with discussions about their everyday lives but soon progressed. According to Dilworth (2001:1), ‘... Martin began e-mailing questions about IDEXX’s manufacturing methods, customer base, and pricing schedule’, which later involved e-mailing potential acquisitions’. However, the trading of secrets fell apart when Camp inadvertently misdirected an e-mail to an Idexx employee who exposed the deal. Martin was sentenced for his role in trading secrets to one year’s imprisonment, three years’ of supervised release, and US$7,500 restitution.

6.6 ROLE CONFLICT

Shapiro (1990:353) identified role conflict among the various strategies which white-collar offenders use to establish and exploit trust. Shapiro (1990:353) points out that ‘incumbents of positions of trust bring multiple interests and role obligations to fiduciary relationships’. Shapiro’s (1990:353) research was concerned with conflict of interest that ‘... represents an intrinsic vulnerability that gives rise to stealing’.

Nasheri and O’Hearn (1999:379) note the case of a researcher at the Mayo Clinic Laboratory. They report:

The FBI’s court documents allege that Iota downloaded several years’ worth of research information to magnetic-optical disks, photographed Mayo’s laboratory for research on cartilage and connective tissue, and took tissue samples, gene sequencing data and research books that were critical to the laboratory's work.

This case represents a conflict of interest that has given rise to stealing research data. Iota was in a position of trust as researcher and violated this position by recording and saving data and information that was the property of the laboratory. Nasheri and O’Hearn (1999:379) point out that, ‘it is unclear at this time whether this was motivated solely by personal gain or whether it had the sponsorship of either a governmental or private-sector entity in Japan’.

Page 232
6.6.1 Internet Piracy

Of the diverse types of crime committed on the Internet, Chapter Five noted that members of international piracy rings, and organised piracy networks can include executives or others in a relationship of trust with software and record companies. McNulty (2003c:2) notes that ‘the supply of such pre-release music was most often provided by music industry insiders, such as radio DJs or employees of music magazine publishers, who frequently receive advance copies of songs prior to their commercial release’. Although this statement by McNulty (2003c) does not suggest that executives are members of these rings, it does highlight a conflict of interest when these people become involved in the organisational structure and network of piracy rings.

Recent attention by law enforcement agencies has focused on the investigation and prosecution of International piracy rings, such as DrinkOrDie, which operate as organised criminal networks. These piracy rings distribute pirated software and games on a global level where part of their success has been demonstrated through the organised structure of the piracy ring (as shown in section 5.2.4). A number of members of DrinkOrDie were executives of software and record companies, thus having access to inside information on the distribution and operation of the illegal network (McNulty 2003c).

6.6.2 Espionage

An FBI Special Agent, Robert Philip Hanssen, sold classified national security information from the FBI, Central Intelligence Agency (CIA), National Security Agency (NSA), and the White House to the KGB in exchange for large amounts of money and jewellery (Melson 2001). The example of Hanssen characterises a different form of theft, in which his knowledge and access to confidential material as an FBI Special Agent was rented to the KGB in exchange for large amounts of money and jewellery.

Hanssen’s position enabled him to hold top-secret clearances. During the course of his employment, Hanssen made a pledge to ‘... never divulge information, in any form or any manner, to anyone who is not authorised to receive it, without prior written authorisation from an appropriate official of the United States Government’ (cited in Melson 2001:3). Hanssen used his position to gain access to confidential information
that related to US defence, provided information to the KGB/SVR based on his knowledge acquired during his employment at the FBI, and provided correspondence and information in the form of computer disks (Melson 2001).

Hanssen conspired with a number of agents and officers of the Russian Federation and the Union of Soviet Socialist Republics to engage in espionage between 1995 and 2001. Computer technology was used as an instrument of Hanssen’s activities. For example, Hanssen used a computer to store and save classified information on computer disks, a Palm III device to communicate and store information, and access to the FBI’s intranet to obtain confidential information and references on individuals relevant to the activities.

Hanssen provided the KGB with more than 20 disks containing hundreds of pages of classified information he obtained from the FBI. Encryption code was used on the disks as a security measure thus enabling only those with a code to gain access to the information. Communication between Hanssen and officers and agents of the KGB was also conducted on a computer micro bulletin board using encryption techniques (Pluta 2001:26). Hanssen also discussed the possibility of using a Palm to provide a more secure form of communication with the KGB. Hanssen states (2001:70):

I have a Palm III, which is actually a fairly capable computer. The VII version comes with wireless Internet capability built in. It can allow the rapid transmission of messages, which if used on an infrequent basis, could be quite effective in preventing confusions if the existence [sic] of the accounts could be appropriately hidden as well as the existence [sic] of the devices themselves. Such a device might even serve for rapid transmittal of substantial material in digital form (cited in Pluta 2001:70).

As an authorised user, Hanssen had access to the FBI’s Automated Case Support System (ACS), a database that contains information on investigative files and indices. According to Pluta (2001:87):

The main, and most extensive ACS database, is the Electronic Case File (ECF), which contains electronic communications and certain other documents relating to ongoing FBI investigations, programs, and issues, and the indices to those documents.

An audit of Hanssen’s use of the ACS found that searches of the ECF database were conducted in furtherance of his espionage activities (Pluta 2001).
Here it may be seen that computing technologies provide a more efficient way to carry out espionage: for example, by facilitating opportunities for people to discuss and send information relating to trade secrets and for the storage of confidential information through the computer without leaving the confines of the home or office. Furthermore, the use of sophisticated techniques of encryption makes detection of information more challenging for law enforcement investigators.

Dilworth (2001:1) points out the advantages of computing technology:

No longer does ... a competitor have to bribe an insider to deliver proprietary information. An unhappy employee or opportunistic licensee can abscond with a company’s most important trade secrets simply by downloading them onto a floppy disk ... [or] e-mail the information to a ready buyer.

The Internet allows individuals to gather information on companies abroad by illegally entering their computer systems and networks and downloading or copying classified information for the purposes of misusing information.

Timothy Kissane, a former release engineer at System Management Arts Incorporated (SMARTS) (which develops software programs that are customised and sold to companies), was sentenced to two years imprisonment for theft of trade secrets from his former employer SMARTS. According to Comey (2002:1), ‘... KISSANE signed an employment contract in which he agreed to “forever keep secret” confidential SMARTS information that he had access to, including “software codes”’. Nevertheless, over 12 months later, Kissane’s employment was terminated, which led to the beginning of the theft of trade secrets. The complainant (Comey 2002:1) alleges that:

Several weeks later, two of SMARTS’ competitors received e-mail messages from a “Joe Friday” at a Yahoo! e-mail account, offering SMARTS’ source code for sale. According to the Complaint, one of the e-mail messages stated that the sender possessed the “cvs repository of SMARTS InCharge code, from 11/20/01 as well as custom code for specific bug fixes and customer-requested enhancements”. The competitors brought these e-mail messages to the attention of SMARTS.

This example demonstrates the opportunities available to individuals to store and copy information while violating the trust relationship of their position.
6.7 SUMMARY

The chapter has exposed patterns in the various strategies that cyber criminals employ to establish and exploit trust through lying, self-dealing, corruption, and role-conflict. Of the various strategies used, lying can be applied to many different forms of crime. It also highlights that lying, deception, and misrepresentation is the most common method in use against victims. The acquisition of information became central to the applicability of self-dealing on the Internet with examples of misuse of personal information, identity theft, and insider trading.

Part of the ease with which people lie or deceive and self-deal appears to be due to the computer-mediated nature of communication and the cloak of anonymity afforded when communicating, providing, and disseminating information online. Corruption and role conflict showed less applicability to different types of cyber crime although it showed that access to information increases the opportunity for the commission of crime.

The following chapter concentrates on how the Internet could be made more trustworthy through a regulatory approach and examines whether regulatory processes are the way forward on the Internet to enable trust to increase methods of guardianship.
CHAPTER 7:  A SYNTHESIS OF CYBERSPACE – NETWORKS OF TRUST ON THE INTERNET

7.1  INTRODUCTION

The ease with which people commit crime on the Internet has become clear in Chapters Five and Six. It was argued in Chapter Six that violation of trust on the Internet forms an important aspect of criminal behaviour through lying, misrepresentation, role conflict, and perhaps corruption. This was demonstrated regardless of the type of crime, conventional or white-collar. In essence, the study of criminal behaviour as set out in the previous two chapters has found that the accelerated growth of cyber crime arises from a supply of motivated offenders, the availability of suitable targets or victims, an absence of capable guardianship, and a range of strategies used to establish and exploit trust.

The objective of this chapter is to demonstrate which regulatory responses are most effective in reducing criminal behaviour on the Internet. It is proposed that a ‘one model fits all’ regulatory approach will not provide effective outcomes to reduce all types of cyber crime. A broader objective is to review what the central themes are on trust and the Internet and explore what approaches have been taken to reduce trust violation on the Internet. First, section 7.2 explores how the concept of trust is defined and recognised in both the terrestrial and virtual worlds. Second, section 7.3 provides an empirical perspective on trust and the Internet. Third, section 7.4 outlines four regulatory approaches: self-regulation, market approaches, law enforcement, and global mutual cooperation prior to analysing their suitability to control three different types of cyber crime: online auctions, online securities fraud, and extortion. In this section emphasis is also placed on exploring the motivations of offenders, availability and attractiveness of suitable targets, absence of capable guardianship, and violation of trust.

7.2  THE CONCEPT OF TRUST

That honesty is the best policy, may be a good general rule, but is liable to many exceptions; and he, it may perhaps be thought, conducts himself with most wisdom, who observes the general rule, and takes advantage of all the exceptions (Hume [1737] 1975).
In identifying the strategies that are used to establish and exploit trust in furtherance of cyber crime, it is important to outline the relevance of trust for the Internet. It is important also to examine the role of trust in a regulatory response. This section provides a starting point for a discussion of trust on the Internet.

7.2.1 What is Trust?

Much like concepts of white-collar crime and cyber crime, there is no general consensus on the definition of trust (Misztal 1996; Wang and Emurian 2004). This is evident from the different conceptual analyses and studies of trust. For instance, dating back to the sixteenth, seventeenth and eighteenth centuries, influential philosophers, such as Hobbes (1588-1679), Hume (1711-1776), and Kant (1724-1804) recognised the importance of trust in human nature. Trusting relationships were an important element of Kant’s (1785) view on trust, human worth, and of his conceptions of an ideal moral community (Hills 2000). Thinking and research on trust have formed an important thread in the discipline of philosophy and in shaping understandings of its diversity and value in human nature, even though no clear distinction of its meaning is evident.

During the mid to late-twentieth century, a resurgence and proliferation of research on trust has led to multi-disciplinary perspectives exploring its concept and nature through psychology, political science, management, economics, and sociology (see Luhmann 1979; Barber 1983; Short 1984; Zucker 1986; Gambetta 1988, 1990; Putnam 1993; Fukuyama 1995; Glaeser et al. 2000; Braithwaite and Levi 1998; Job and Reinhart 2003). Fukuyama (1995:74) makes the point that, ‘it is striking, however, how different each discipline’s account of the origins of trust is’. According to Fukuyama (1995:74), ‘… this result reflects in part the different theoretical models of human behaviour underlying the different social sciences, but it is also a product of disciplinary insularity’. Within the discipline of sociology, for example, the concept of trust has focused on the role it plays in personal interactions, the community, government (see Job and Reinhart 2003), society, and more recently, the Internet.109

The Macquarie Dictionary (2003:158) defines trust in this way:

---

109 Aside from the conceptual debates about the concept of trust, Misztal (1996) points out that instead of focusing on the origins of trust, an examination of how trust functions may be more instructive.
1) Reliance on the integrity, justice, etc., of a person, or on some quality or attribute or thing; confidence. 2) Confident expectation of something; hope. 3) Confidence in the ability or intention of a person to pay at some future time for goods, etc.; credit: to sell goods on trust. 4) One on whom or that on which one relies. 5) The state of being relied on, or the state of one to whom something is entrusted.

Reliance and confidence, along with a degree of uncertainty, are important factors to consider when communicating with users and exchanging information on the Internet. It was shown in Chapter Five, for example, that the absence of face-to-face communication on the Internet can contribute to a lack of confidence in the marketplace. On the other hand, reliance is involved in trusting that a website in which individuals input personal information will not be used unlawfully. Confidence can be applied to the Internet through the expectation that someone will send monies owed or deliver goods as promised on the Internet. Similarly, there is confidence that the person with whom you are communicating on the Internet is who they say they are. This factor was commonly identified as a concern among individuals, particularly children and young adults, when communicating in chat rooms and news groups on the Internet.

A level of uncertainty is also linked with confidence within definitions of trust. Gambetta (1990:213-237), a sociologist, characterises trust as:

... a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action.

Gambetta’s definition focuses on three important elements. First, trust is subjective; second, the lack of monitoring (or guardianship) affects trust; and third, the level of trust is dependent upon the effect on one’s own actions of the agent’s actions. These three elements of Gambetta’s concept of trust may also be linked to Cohen and Felson’s three prerequisites: motivated offender, availability of suitable target, and the absence of a capable guardian to prevent the crime from occurring (this will be further explored in section 7.4 of this chapter).

Sociological research has identified and applied various concepts including confidence, trustworthiness and risk within the broader literature on trust. For example, Levi (2001) identifies trust as:
... relational, involving at least one individual making themself vulnerable to another individual, set of individuals, or institution that possesses the potential to do the harm or betray. Trust implies a judgement or risk in conditions of uncertainty. Moreover, trust is seldom unconditional; it is given over specific domains (cited in Levi and Braithwaite 2001).

This concept of trust also focuses on the implications of trust relationships, which can involve elements of risk\textsuperscript{110} or danger (which has been identified as a recurrent issue with various types of cyber crime as highlighted in Chapter Five). Morrison and Firmstone (2000:1) argue that ‘indeed, risk and trust are inseparable components in decision making. However, in talking of trust and risk, we are referring to peculiarly modern phenomenon’ (sic). If this is the case, as Morrison and Firmstone argue, increasing importance will be placed on the function of trust and its role in information technologies such as the Internet.

Whilst there are a number of different approaches to defining trust, this section acknowledges its value and breadth as an area of research and its applicability to the Internet. The various definitions of trust outlined in this section reflect to some degree the different theoretical traditions and frameworks from which the concept has emerged and evolved. However, it is important to consider, as Job and Reinhart (2003:61) point out, ‘trust is not an easy concept to define, and this difficulty has increased more recently with the growing secularisation in the range of conceptualisations of trust’.

Trust may therefore be viewed as multi-faceted, which forms our understanding of the concept, its nature and the way it has been applied to different contexts: individual, social and political, and is interlinked in sociological literature with concepts such as trustworthiness, confidence and risk (Luhmann 1979; Misztal 1996; Wang and Emurian 2004).\textsuperscript{111} While recognising the various ways the study of trust is applied in different disciplines, the next section focuses on whether there are distinctions between trust in the terrestrial world and trust in the virtual world.

\textsuperscript{110} Jackson et al. (2004:4) note ‘the word risk derives from the early Italian word *risicare*, which means to ‘dare’.

\textsuperscript{111} Misztal (1996:16) maintains: ‘the main difference between trust and confidence is connected with the degree of certainty that we attach to our expectations’.
7.2.2 Trust - A Terrestrial and Virtual Perspective

Trust forms an important factor in decision making processes i.e. whether to engage in personal and professional relationships or transactions both in the terrestrial and virtual worlds. Trust and distrust in the virtual world are defining features of establishing communication and developing relationships on the Internet. Indeed, chapters five and six showed that violation of trust lies at the core of many forms of criminal interactions in the virtual world which appear distinct from the terrestrial world (see Newman and Clarke 2003).

There are differences in trust between the terrestrial world and the virtual world. Grabosky (2001d:12) makes the point that ‘... in real life, trust is based on personal relationships, while online trust is based on confidence in processes’. An example that most effectively illustrates this distinction involved a buyer bidding for a laptop via an online auction (as discussed in section 5.5). During the processes of communication between the buyer and seller, the potential buyer of the laptop computer was persuaded to trade privately after being convinced by the seller’s knowledge of the product. Thus, the buyer of the laptop relied on confidence in processes of communication. Many factors have shaped the reliance on confidence in processes on the Internet. These can be identified through the absence of face-to-face interaction (which is also evident in many forms of transactions in the physical world), absence of physical proximity of Internet users, and anonymity.

In analysing the role of trust and its implications for e-commerce, Morrison and Firmstone (2000:8) found that ‘one of the new aspects about the Internet is that establishing trust in it entails a different set of semiotics to that witnessed in the past, or perhaps more accurately, requires new literary skills in managing risk through the formation of trust’. Based on Internet studies, Morrison and Firmstone identify four characteristics of the virtual world that create challenges (and are distinct from the

112 Luhmann (1979:72) argues that there is a ‘... strong incentive to begin a relationship with trust’.

113 Being convinced to trade offline is a strategy that some individuals employ to defraud victims online. Commonly recognised as the ‘grey area’ of online auction fraud, statistical data does not recognise transactions where users no longer engage in buying through Internet auction houses where the communication began.
terrestrial world) for establishing trust on the Internet: lack of accountability, lack of performance and familiarity, lack of closeness, and brand as reputation.

Lack of accountability refers to the challenges Internet users identify in their decision making process when conducting business on the Internet. Morrison and Firmstone highlight the absence of regulatory processes and the nebulous nature of the Internet as contributing factors to the lack of accountability. Furthermore, Morrison and Firmstone (2000:11) state that ‘the situation of mistrust is not helped by the current confusion surrounding what recompense consumers might seek should agreements failed [sic] to be honoured, or if services provided do not match expectations’. Although a lack of accountability also applies in the terrestrial world, one of the challenges of the Internet is the lack of transparency associated with transactions over the Internet. For instance, a user may be unsure when purchasing goods from a website whether it is the operator of the website who owns the goods or whether they act for others, how their information is used and where the goods are being stored. Should problems arise, the lack of a ‘one stop shop’ that allows consumers a place to follow up on transactions appears to contribute to an absence of confidence in processes.

Morrison and Firmstone (2000:12) identify lack of performance and familiarity as contributing to the absence of certainty in buying goods and services on the Internet. Based on an Internet study by future.com, Morrison and Firmstone make the point that if consumers lack certainty in purchasing goods over the Internet, the growth of the Internet may suffer. However, if trust on the Internet can be established and maintained, the growth of the Internet will provide benefits. Closely associated with a lack of performance is familiarity. Morrison and Firmstone (2000:13) argue that ‘... the problem the Internet faces, due to unfamiliarity, is that there may well be too much missing knowledge for trust to function as a bridge to action’. Again, the function of trust is important to the future success of the Internet (see Chapter Seven for ways in which knowledge can build networks of trust through cooperation).

Third, a lack of closeness of the Internet (which in the terrestrial world can be bridged through physical space and knowledge developed over time) presents new challenges to

\[114\] Wallace (2001) raised concern that physical signs such as body language and facial expressions are
Internet users. However, the lack of closeness can be overcome, as Morrison and Firmstone acknowledge, through third parties, such as Trust-E, trust seals, codes of practice, and different forms of regulation. Brands as reputation have been recurrently identified as an important factor in building trust on the Internet. Morrison and Firmstone (2000:15) argue that:

One does not simply trust a particular brand in terms of a specific product, but trust that which it represents without understanding the mechanisms of its production ... Thus, brands that have established themselves in the market of traditional exchange are to be trusted in the market of cyber exchange, and indeed, those with a pre-existing and established reputation will have advantage over those attempting to create a reputation by virtue of Internet presence alone.

Brands as reputation on the Internet are distinct from the terrestrial world due to the technological sophistication of cyber criminals who apply strategies to deceive Internet users through trusted brands. Recent attacks on trusted brands such as eBay and well recognised banking institutions such as Westpac and Citibank have highlighted the risks posed to trusted brands by violation of trust.

What is also distinctive about the Internet as opposed to the physical environment is its unprecedented access and as a repository of information. The unfettered access to the Internet (as Chapters Five and Six have shown) allows individuals to form not only social networks but also criminal networks through recruiting potential offenders across the globe anonymously. As Shapiro (1990:353) points out, ‘the social organisation of trust provides ample opportunity for deception’. Chapter Five highlighted the ease with which individuals and groups of individuals establish networks and apply strategies to violate trust for the purposes of criminal opportunities. The speed of communication and information via the Internet allows such networks to organise and execute crimes around the globe without having to leave the comfort of their homes or offices.

A five-year jail term imposed on an Internet scammer in Australia demonstrates the opportunities for establishing networks and building trust in furtherance of criminal opportunities. Nick Marinellis, a 40-year-old Australian, was involved in an Internet Nigerian scam amassing millions of dollars from victims around the globe. Lamont (2004:8) notes that according to police, Marinellis also operated with ‘... other syndicate

absent on the Internet and as such trust may be diminished.
members who perpetrate the scam from different ports around the globe, culminating in a final contact with [Marinellis] who is the Australian clearing house'. It appears that the Nigerian scammers rely upon strategies such as deception and lying to deceive their victims. Lamont (2004:8) described the scam:

Victims were led to believe NMFinance Network was a legitimate money handling company. Marinellis required money upfront to process the illusory millions the victims thought you would receive from lottery wins or business investment deals.

While this type of fraud emerged in the physical world, it appears that the Internet facilitated contact with like-minded individuals and potentially millions of victims. This access appears to have also increased the level of risk to potential victims through strategies used to violate trust. Furthermore, the sophistication of technology has allowed scammers to replicate official documents to such a high standard that they appear legitimate, thereby increasing the victim's confidence in the process.

This section has shown that vulnerabilities associated with trust on the Internet can be attributed to unprecedented access, familiarity, lack of accountability, absence of face-to-face interaction, and anonymity. A number of these characteristics are also present in old-fashioned mail order frauds and telemarketing frauds although the numbers of people who have access to information and ways to conceal their identity have been enhanced by digital technology. The following section explores what contributions have been made to the study of trust on the Internet.

### 7.3 TRUST AND THE INTERNET – AN EMPIRICAL PERSPECTIVE

As the Internet continues to reach more and more people around the globe, a growing interest in exploring the role of trust in computer-mediated communication (CMC) has emerged (see Jarvenpaa et al. 1999; Friedman et al. 2000; Dutton 2000; Corbitt et al. 2003; Corritore et al. 2003; Newman and Clarke 2003). This is also evident through a search on Google (2004) with the words ‘trust on the Internet’, which revealed an estimated 8,350,000 entries.\(^\text{115}\)

\(^{115}\) While this result includes newspaper pieces and editorials, it nevertheless highlights the interest and relevance of trust on the Internet.

Page 244
Empirical research and studies of trust and the Internet have focused on a range of issues: the criminalisation of anonymity (du Pont 2000), virtual communities (Rheingold 1993; Jones 1995; Davis 1999); trust and e-commerce (Birk 2000; Jarvenpaa et al. 2000; Dutton 2000; Grabosky et al. 2001; Van Den Berg and Van Lieshout 2001; Corbitt et al. 2003; Newman and Clarke 2003; Siala et al. 2004); trust and websites (Araujo and Araujo 2002; PSRA 2002; Corritore et al. 2003; Wang and Emurian 2004); privacy and security issues and Internet standards (Dutton 2000; Fox et al. 2000); consumer trust (Hoffman et al. 1999; Jarvenpaa et al. 2000); and elements of online trust (Corritore et al. 2003). This section will draw upon some of these studies to highlight the varying perspectives and findings on trust on the Internet.

Consumer perceptions and expectations of trust and websites is an area that has generated a growth of studies both in the private and public sectors (see also Hoffman et al. 1999). For example, a survey of 1500 adult online users, conducted by Princeton Survey Research Associates (PSRA 2002:5) showed that ‘only 29 per cent of users say they trust Web sites that sell products or services [while] … 33 per cent say they trust Web sites giving advice about such purchases’. These statistics are consistent with long-term Internet users (three years or more), which showed that within this group of users, 31 per cent trust e-commerce sites (PSRA 2002:5).

Corbitt et al.’s (2003) survey on consumer perceptions of trust and e-commerce revealed that trust is influenced by a number of sources, three of which include ‘... e-commerce reputation in general, the consumers, and the specific e-commerce web site’. The study also showed that the factors that influence individuals’ perception of e-commerce include ‘... technology trustworthiness and perceived risk ... [and a] customer’s experience with the Internet ...’ (Corbitt et al. 2003:12). The factors Corbitt et al. (2003) raise cannot be addressed by an individual Website but rather should be addressed at a collective or group level.

\[^{116}A\] A comparative analysis between web sites and other organisations showed that ‘68 percent of consumers trust small businesses, 58 percent trust newspapers and television news, and 55 percent trust financial companies, such as banks, insurance companies, and stock brokers’ (PSRA 2002:4).
Positive experiences associated with consumers’ perceptions and experiences appear to result in positive outcomes of trust on the Internet. However, in contrast to positive experiences of Websites, Freidman et al. (2000:35-6) note:

... not long ago, customers who regularly read Amazon.com’s online book recommendations assumed they were editorial content written by Amazon.com staff. A breach of trust resulted when it was revealed that publishers sometimes purchase spots for their books in this recommended system (Rosman 1999).

This example highlights the lack of transparency of processes on some Websites. However, more importantly, it also demonstrates the lack of trust in Website operators in a market which attempts to build levels of trust for consumers.

Dutton and Shepherd (2003) have drawn on the findings of the Oxford Internet Survey (OxIS) exploring trust in cyberspace. The survey was based on a random sample of more than 2000 people aged 14 years and over from the United Kingdom, Wales and Scotland, who were interviewed face-to-face.117 Of the 2030 respondents interviewed, 59 per cent use the Internet, with those in school and work comprising the majority of Internet users. According to Dutton and Shepherd (2003:1), these results suggest ‘... that there is sufficient trust to support the continued diffusion of this technology, despite a general awareness of the potential risks entailed in exposure to unwanted mail, viruses and other potential risks’.

Two elements of trust identified by Dutton and Shepherd (2003) that have arisen from the survey include ‘net-confidence’ and ‘net-risk’. According to Dutton and Shepherd (2003:2), ‘users of the Internet have more certainty and more confidence in the information and people they can access through the technology than do non-users ... [and that] greater proximity to the Internet tends to instil more trust, to some extent’. Despite the higher levels of trust experienced by the respondents, broad disparities in trustworthiness were identified in the public’s perception of trust on the Internet. The central issues that have arisen from the study suggest that trust is shaped by users’ experience of the Internet.

---

117 The survey showed that ‘the biggest difference between users and non-users is age. Among those still in school, 98% are Internet users and among people of working age, 67%. By contrast only 22% of retirees use the Internet’ (Dutton and Shepherd 2003).
CHAPTER 7: A SYNTHESIS OF CYBERSPACE – NETWORKS OF TRUST ON THE INTERNET

One of the factors that contribute to higher levels of trust, according to the OxIS survey, is experience. Yi et al.'s study (2002) found that experience is also closely associated with higher income levels. This is not surprising, given that those who traditionally had access to the technology are divided into those who can afford it and those who can't (further fuelling the debate on the digital divide). Interestingly, the survey also found that those with greater formal education tend to be more wary of the information published on the Internet. However, the study showed that the respondents appear to be less concerned with the risks involved with Internet use (Dutton and Shepherd 2003:2).

These findings by Yi et al. indicate that those with more formal education are less likely to become victims of crime, given that they are more wary. This correlation is somewhat spurious, given that the availability of suitable targets does not appear to be determined by such a factor. Yi et al.'s (2002:17) survey on trust and consumers found that respondents with higher education are more concerned about criminal exploitation and technological reliability. Given the findings that experience has been identified as an important factor in trust on the Internet, education and awareness are important elements in reducing the risks of becoming victims of cyber crime (an issue further explored in section 7.4).

In a study exploring Internet users' experiences, McKewen (2001:20) observed that '... there was a lack of honesty associated with communicating on the Web because people could never be sure the person they were 'talking' to was telling the truth' (cited Whitty and Gavin 2001). The study also showed that 'while many of the participants cited the lack of non-verbal content in their conversation as an obstacle to judging people's honesty effectively many also admitted to lying themselves' (McKewen 2001:20). This is consistent with examples provided in Chapter Five which highlighted the lengths to which individuals go to in order to deceive others online for the purpose of committing fraud. The study also revealed that '... lying was common amongst men and women, and young people were more likely to lie than older people, men in particular were lying about everything from gender to income, education and occupation' (McKewen 2001:20).

Wang and Emurian (2004) maintain that 'lack of trust has been repeatedly identified as one of the most formidable barriers to people for engaging in e-commerce, involving transactions in which financial and personal information is submitted to merchants via
the Internet’. Interestingly, while these statistics reveal a low level of trust in Websites, they also show that when consumers’ concerns are met, consumers appear to extend their level of trust to particular Websites. This is consistent with a study undertaken by Corbitt et al. (2003:203), which showed that ‘customer’s trust levels are likely to be influenced by the level of perceived market orientation, site quality, technical trustworthiness, and user’s Web experience’.

It has been established in this section that trust and the Internet is increasingly becoming a significant area of empirical research, and one that has profound effects on consumers and Internet users. However, studies on trust and the Internet have predominantly emanated from the United States of America, although recent studies have illustrated a British and Australian perspective (see Dutton and Shepherd 2003).118

While the studies outlined above demonstrate their broad application to the Internet, few in-depth studies of trust and the Internet have been available, and literature in this area tends to provide an incomplete picture of the nature of trust on the Internet. For example, it is difficult to validate the accuracy of online surveys due to the computer-mediated nature of communication and the difficulty of capturing a representative sample.

The various ways in which trust is applied across different disciplines does little to demonstrate the role and relationship between trust and criminal behaviour on the Internet. This is because, in general, literature on trust and computer-mediated communication appears to reflect the perspective of the Website operator or business and Internet user rather than the behaviour of the offender.119 One of the approaches in monitoring and controlling behaviour of users online is through regulation.

7.4 REGULATING THE INTERNET

Regulation has played a significant role throughout history in one form or another for thousands of years. Parker and Braithwaite (2003:119) state that regulation:

118 The study of trust and the Internet has been hampered by a lack of validated measurement instruments due to the broad and hidden nature and the ‘dark’ figure of crime on the Internet.
... is normally taken to include the enforcement of informal rules that are
not state laws as well as formal rules promulgated by supranational
bodies such as the World Trade Organisation or the European Union,
and subnational bodies such as professional associations ... Much
regulation is accomplished without recourse to rules of any kind. It is
secured by organising economic incentives to steer business behaviour,
by moral suasion, by shaming, and even by architecture. On this
broadest view, regulation means influencing the flow of events.

In a paper discussing regulatory conversations, Black (2002:163-4) recognises that the
study of regulation has been viewed through ‘... a kaleidoscope of lenses, notably
economics, cultural/anthropological theory, institutionalism, and systems theory ...’.
Black (2002:170) defines the concept of regulation as:

... a process involving the sustained and focused attempt to alter the
behaviour of others according to identified purposes with the intention
of producing a broadly identified outcome or outcomes which may
involve mechanisms of standard-setting, information-gathering and
behaviour-modification.

More recently, divergent approaches to regulation are being applied to new contexts
(see Weber 2002; Scott 2003; Jordana and Levi-Faur 2004), such as the Internet. The
Internet, as discussed in Chapter Four, constitutes an amalgam of networks connected
through the use of portable and open protocols. It was during the early 1990s when
ARPANET (a creation of the United States Department of Defence) transferred
responsibility for the backbone of the Internet to the National Science Foundation
Network (NSFNET), the research network of the Internet. Initially, the NSFNET
operated within United States academic and research based institutions but
communication soon spread to Canada and other parts of Europe to form global
networks (Frazer 1998:1). The open protocols meant that there were no secrets about the
operation of software; however, a greater level of trust was required by users of the
network to operate effectively and efficiently.

The growing interest in and uptake of the network by academics and researchers led to
pressures by the broader corporate community to expand it for commercial use. In 1995
the NSF opened up the network to commercial entities where it continued to operate as

---

119 The work of Newman and Clarke (2003), which explores trust and criminal behaviour through a
situational crime prevention approach, is an exception.
an unregulated network.\textsuperscript{120} It is widely acknowledged that because of its largely unregulated nature, the Internet is built upon trust between users and providers of information. Close to a decade on, usage of the Internet has expanded exponentially with recent figures estimating over 800 million users worldwide (Internet World Stats 2004) and close to 200 countries connected to the network (Westby 2003).

Despite the successes of users’ adoption of the Internet, the Internet has demonstrated its vulnerability to serious threats (see Chapter Four). The commercial inception of the Internet some years later proved that trust had diminished, as early signals of crime were on the increase. The growth in Internet take-up, followed by the subsequent proliferation of cyber crime, inspired a burgeoning of research on Internet regulation, governance, policing, and the law (see Post 1997; Drucker and Gumpert 1999; Grewlich 1999; Lessig 1999; Grabosky 2000b, 2001c; Marsden 2000; Biegel 2001; Broadhurst 2001, 2004; Grabosky et al. 2001; Scott 2002, 2004; Weber 2002; Newman and Clarke 2003; Westby 2003; Sideri 2004; Smith et al. 2004; Broadhurst and Grabosky 2005).\textsuperscript{121} As this thesis argues, given the Internet’s global and intangible nature, controlling online behaviour continues to form an important role in crime prevention and securing the future viability and success of the Internet.

There are many debates on Internet regulation. The broad nature of debate reflects the changing dynamics of the Internet: from an open network where behaviour was unregulated and information was free and available to all users, to its current platform where particular types of criminal behaviour and access to information are regulated. Parker and Braithwaite (2003:121) recognise the role of technological change and note that ‘... the rise of the regulatory state is that it is a response to new fears and tensions about our relationship to science and technology’. The various scholarly contributions to regulation on the Internet illuminate the various debates and local and global developments that have taken place over the past decade.

\textsuperscript{120} Frazer (1998:2) notes: ‘On April 30, 1995, the NSFNET was officially dissolved, although, returning to its roots, the NSF retained a core research network for research only use called the Very High Speed Backbone Network Service (vBNS), which went on to form the basis for the Internet2 project’.

\textsuperscript{121} Parker and Braithwaite (2003:119) point out ‘... the distinction between governance and regulation is narrowing as governments shed their responsibilities for service provision and shift more of their energies to regulating the service provision of other types of actors’.
These various approaches include: self-regulation (Daley and Irving 1997; Price and Verhulst 2000, 2004); state-enforced regulation through legal frameworks (Biegel 2001; Pocar 2004); international based regulation (Biegel 2001); cooperation and harmonisation between public and private sectors (Brenner 2003) and nations (Broadhurst 2003, Bullwinkel 2005); and architecture as crime control (Lessig 1999). Sideri (2004:61) notes that among the various discourses about Internet regulation, ‘the dominant view is that the role of law should be confined to putting in place the correct procedures to enable the participation of communities in the making of rules that affect them’. While growing interest is directed towards maintaining a self-regulatory environment, a shift from state-based control to international mutual cooperation is also emerging (see Pichler 2000).

Discourses about regulation on the Internet have moved beyond the need to regulate the Internet to how it is being regulated. Furthermore, discussions have been narrowed to focusing on specific types of cyber crime, such as privacy (Daley and Irving 1997; Crompton 2004); pornography and child pornography (see Akdeniz 1997); hacking (Duff and Gardiner 1996); harassment and stalking (Ellison and Akdeniz 1998); gambling (McMillen 2001); online investing (Bradley 2004; Condon 2004; Kingsford Smith 2004; Scott 2004); and fraud (Snyder 2000; Grabosky et al. 2001; Albert 2002; Huang Chua and Wareham 2004; Newman and Clarke 2003) in the hope of clearer guidelines, swift responses, and harmonisation. These developments have also given rise to cooperation between private and public sectors, governments, and nations. The following sub-sections will broadly outline the various forms of regulation on the Internet.

7.4.1 Self-Regulation

Although not a new concept, self-regulation is one of a number of approaches applied to regulate behaviour. Self-regulation has many components and, as Cunninghan and Rees (1997:364) point out, ‘... no single definition is entirely satisfactory’. According to

---

122 The area of regulation on the Internet and the growing body of research and scholarly literature is vast and is only touched on here.

The Internet is predominantly a self-regulated network,\textsuperscript{124} although it is also governed by enforcement components such as enforcement and laws. The findings of a study by the Programme in Comparative Media Law and Policy (PCMLP 2004) about self-regulatory codes of conduct revealed that ‘most successful self-regulatory activity has taken place where there is a key legal basis’ although the study also found that this approach is less successful ‘... in relation to trust of Internet content ... [and] child protection/harmful content’ (PCMLP 2004:2). A self-regulatory approach to the Internet has allowed individuals, organisations, businesses, associations, and corporations leverage to put in place mechanisms of self-governance to complement state-based regulation.

Some proponents may view self-regulation as a soft touch to regulating behaviour. According to Pichler (2000:98-9):

\textbf{Business very much liked the idea of running things on its own, adopting codes of conduct and other industry standards, and trying to avoid government regulations which were feared to be too constraining for the development of electronic commerce.}

Pichler highlights an important point, that the Internet presents a somewhat unique approach given the number of individuals, organisations and businesses conducting commerce on the Internet. While Pichler’s argument is based on businesses concerned with constraining commerce through government regulation, an environment based on

\textsuperscript{123} Post (1997:1) acknowledges that discussions on Internet governance include whether ‘...the transmission of ‘indecent’ material be banned, or otherwise regulated, on the Internet? ... What rules should govern anonymous communication in cyberspace?’ and discussions about copyright law.

\textsuperscript{124} Some countries such as China and Brazil impose stronger state-based enforcement on Internet users.
government regulation may not be as effective an approach to reducing criminal behaviour as other forms of regulation.

Self-regulation encompasses a broad range of approaches that include codes of conduct, online dispute resolution (ODR) mechanisms (Rule 2002), market approaches, formal private contracts, netiquette, and informal methods of social control. Self-regulation promotes cooperation between private and public sectors, thus forming a type of global self-regulation. Self-regulation also allows the private sector to implement new methods of guardianship to keep apace with the sophistication of criminal techniques and methods.

The Australian Government’s support for self-regulation is evident through promoting cooperative relationships between the private sector and industry associations. In a somewhat similar vein to the Australian Government’s position on self-regulation, the United States Government affirmed their support in a speech on the global electronic commerce environment by making the point that ‘governments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organisations to develop mechanisms to facilitate the successful operation of the Internet’ (Clinton and Gore 1997).

While it appears encouraging that government and state-based enforcement promote and support self-regulatory approaches, the PCMLP (2004) questions its sustainability. An analysis by PCMLP (2004:6-7) showed that self-regulatory approaches ‘... removes ... the spontaneity ... and raises the question of whether industry organisations or individual firms have the motivation to pursue self-regulation in the long term, when neither regulatory oversight nor financial support for self-regulation are in place’. These issues are important to consider given the growth in Internet take-up. Furthermore, if criminal activity on the Internet mirrors Internet take-up, pressures (psychological and financial) on businesses and organisations to secure networks may become more evident.

(a)  Codes of Conduct in Industry Associations

Codes of Conduct have emerged over the past decade as a popular approach to self-regulation with the predominant growth arising from Internet Service Providers (ISPs) and more recently from online chat rooms (PCMLP 2004).
ISPs continue to hold influence through their role in legislation, codes of conduct, and case decisions. Biegel (2001:5) asserts that ‘for the average person, Internet service providers (ISPs) continue to serve as gatekeepers to cyberspace’. This is demonstrated by the information and payment users provide ISPs to access the World Wide Web (WWW) and e-mail. ISPs have the power to remove a person as their provider through misuse and abuse. However, the role of ISPs continues to be debated where underlying issues are marked by the nature of their power in enforcing codes of conduct.

The Internet Industry Association (IIA) of Australia, for example, proposed an Internet Industry Code of Practice in 2002125 with a focus on self-regulation and cooperation with law enforcement agencies (IIA 2002). The objectives of the Code of Practice include:

- To establish a cooperative working environment for ISPs and LEAs’ in which there are clear policies and procedures relating to investigations into certain types of criminal and civil acts having regard to the Act – in other words, to describe standards of best practice in relation to these matters;

- To provide clear guidelines to the satisfaction of both industry and LEAs’ as to what constitutes ‘such help as is reasonably necessary’ and to ensure this term is defined having regard to standards of confidentiality and privacy afforded to users of the Internet under the Act and thereby establish confidence in and encourage the use of the Internet;

- To provide a transparent mechanism for the handling of LEAs’ investigations for the Internet industry and ensure that there is a clear understanding on both sides as to what the procedures are;

- To promote positive relations between the LEAs’ and the Internet industry.

125 The Internet Industry Code of Practice is currently in draft form.
126 LEA refers to Law Enforcement Agencies.
To give users of the Internet confidence that their privacy and the confidentiality of their transactions will be guarded from unlawful intrusion by LEAs (IIA 2002).

While the IIA Code of Practice has many benefits in the investigation of potential crimes (through promoting cooperation and positive relations between law enforcement agencies and the IIA), the Parliamentary Joint Committee on the Australian Crime Commission on Cyber Crime (PJCACC) (2004:17) noted its concern, in particular, the ‘... persuasive effect of the Code’. The PJCACC (2004:17) maintained that ‘if the Code of Conduct applies only to those who agree to be bound by it, there is still a potential for the problems ... as those who wish to operate free of sanctions will still be able to do so’. Furthermore, the IIA fails to highlight the value of trust in the electronic environment, which in turn can increase levels of confidence in the marketplace.

An analysis of ISP Codes of Conduct, carried out by PCMLP,127 showed variations in the comprehensiveness between countries. The variations relate to the different focus each country places on content. It is important to highlight that stricter codes of conduct do not necessarily result in a stricter regulatory environment (PCMLP 2004).

### Table 7.1 Concerns Covered in Different National Codes of Conduct in the European Union (EU)

<table>
<thead>
<tr>
<th>Country</th>
<th>ISP Coverage</th>
<th>Business Info</th>
<th>Illegal Activity</th>
<th>Material Harmful to Minors</th>
<th>Hate Speech</th>
<th>Bulk Email</th>
<th>Data Protection and Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>Belgium</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Denmark</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

127 The PCMLP (2004:48) note that ‘... the word stringent or comprehensive ... refer to codes that covered most of the areas of interest in self-regulation ...’.
### Table 7.1: Networks of Trust on the Internet

<table>
<thead>
<tr>
<th>Country</th>
<th>ISP Coverage</th>
<th>Business Info</th>
<th>Illegal Activity</th>
<th>Harmful to Minors</th>
<th>Material Speech</th>
<th>Bulk Email</th>
<th>Data Protect &amp; Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finland</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>France</td>
<td>×</td>
<td>×</td>
<td>√</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Greece</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ireland</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Italy</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>×</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Luxembourg</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td>×</td>
<td>√</td>
<td>√</td>
<td>×</td>
<td>×</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Norway</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>×</td>
<td>×</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td>Portugal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sweden</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK</td>
<td>×</td>
<td>√</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Germany</td>
<td>√</td>
<td>×</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>×</td>
<td>x</td>
</tr>
</tbody>
</table>

Source: PCMLP 2004

Table 7.1 illustrates a range of issues that have been adopted by different national ISP codes. The analysis by PCMLP found that the role of trust is important in establishing and maintaining codes of conduct. The study also found that a lack of trust can lead to challenges in implementing codes of conduct (PCMLP 2004:81). This was illustrated with the example of Italy, where ISP providers did not appear to have trust in the government in its push to implement a code of conduct for Internet content, in particular, for the protection of minors. As a result, the government’s attempt failed. In the case of Ireland, the PCMLP identified that high levels of participation from ISP
providers was attributed to the government’s unwavering commitment to self-regulation.

The ease with which ISPs can set up and sell Internet access may make self-regulation through codes of conduct difficult in its effectiveness as ISPs in Australia are unlicensed (APJCCC 2004:15). The report by the Australian Parliamentary Joint Committee on Cyber Crime (2004:16) noted its concern:

The resources of less reputable ISPs can become a storehouse for records of criminal activity. Further there is potential for ISP’s [sic] to obtain material from client addresses which is confidential, in addition to the credit card payment information which is supplied by the clients when they join the service.

The implementation of legislation to thwart criminal activity linked with ISPs has been discussed in the United Kingdom and may lead the way with other countries adopting a similar approach.

(b) Benefits of Self-Regulation

There are a number of benefits of self-regulation on the Internet. Self-regulatory approaches can tailor methods of guardianship and target testing to specific industries. Banking corporations, for example, can contact customers who bank online via e-mail alerting them that their personal details need to be changed in order for the system to be updated and made more secure. For those customers who reply giving the bank the information required, the bank would send another e-mail warning customers that had the e-mail not been legitimate their information would be compromised by potential cyber criminals. This form of target testing also allows businesses to keep pace with the sophisticated techniques and methods that cyber criminals employ to deceive legitimate users. Furthermore, it educates Internet users about the various techniques that criminals use in furtherance of criminal opportunities.

Self-regulation can be tailored to control criminal behaviour because rules can be changed at a faster pace than other forms of regulation and it reduces the levels of bureaucracy (Riegabauer 2004). In addition, self-regulation has an ability to build on a range of expertise and experiences of those involved in
industry and to keep apace with technological change. It also mobilises management creativity in problem solving.

(c) Limitations of Self-Regulation

Self-regulation can lead to unfair competitive practices. In particular, those companies with a monopoly may impose their rules on to those with less status and financial support (Riegabauer 2004). The study carried out by the PCMLP (2004:2) identified ‘... insufficient transparency and accountability in code production process; ... lack of sustainability of funding of self-regulatory initiatives ... [and] the difficult[ty] to evaluate the impact of self-regulatory activity on user experience, trust and perception’. Part of the challenge associated with evaluating the impact of self-regulatory activity relates to the lack of reliable data from Internet users and operators. Furthermore, the absence of a global self-regulatory Internet body to oversee general issues and future concerns may mean that such debates will continue.

The lack of internal enforceability may result in associations enforcing norms against particular members and sectors. However, if norms are not enforced, consumers may lack confidence, and decreasing levels of trust may affect purchasing online. Furthermore, leverage of association and industry groups may be limited due to the ease in which individuals and groups can open a shop front for criminal activities. Education and awareness is voluntary, therefore some organisations may weigh up the cost-benefit outcomes of educating their members. This leads to a potential lack of knowledge to members who are subject to the codes of conduct.

In summary, self-regulatory strategies can be an efficient approach to decreasing criminal behaviour on the Internet over other forms of regulation; however, limitations are inherent if self-regulatory strategies are not reviewed to keep apace with changes and methods of criminal activity.

7.4.2 Market Approaches

Given the numerous challenges of regulating and policing the Internet, market approaches may provide a way for Internet users and businesses to actively participate
in reducing the availability of targets and increasing methods of guardianship. Market approaches are in tune with the increased sophistication of cyber criminals by providing services that can reduce the risk of becoming a victim through filtering software programs, anti-virus, anti-spam and firewall software.

(a) **Filtering Software Programs**

In a submission to the APJCACC (2004:10), Symantec Australia noted:

If you look at the whole instant messaging or chat room space, ... there are a lot of third party solutions out there which you can bolt on to existing instant messaging and chat room technologies to record the conversations. It is just a matter of going out and finding the right bits that fit together and knowing how they work ...

Third parties also play an important role by providing self-regulatory strategies in reducing the availability of targets and increasing methods of guardianship through security. Third parties provide online security to businesses and organisations that may not have set up their own systems privately and can encourage networking between businesses and sectors. For example, the Trusted Computing Group (TCG) is an industry standards body, with members from various industry sectors such as computer manufacturers and software companies with an interest in enhancing security. According to TCG (2005:1), it is formed to:

... develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals, and devices. TCG specifications will enable more secure computing environments without compromising functional integrity, privacy, or individual rights. The primary goal is to help users protect their information assets (data, passwords, keys, etc.) from compromise due to external software attack and physical theft.

(b) **Anti-Virus Software**

Software and hardware companies are also moving to educate Internet users and businesses on security and the Internet. Microsoft, for example, encourages businesses and organisations to participate in security events organised by Microsoft. According to Microsoft Corporation (2004:1):

The security events are Microsoft's way of demonstrating its commitment to security. These days it's very important that both
developers and IT professionals know about and can identify different security threats. Therefore we will not only show you how the "Trustworthy Computing" initiative resulted in more secure products; we want to show you how you can anticipate to [sic] and overcome different security threats. These events are focused on delivering modularized content and offering prescriptive guidance around security for both developing applications and running the business' software.

Given the exponential growth in Internet fraud, payment intermediaries such as escrow services as well as trust seals are becoming an important service and market approach for users and businesses. Escrow services are one of the most commonly recognised market approaches and provide security in making payment for goods and services purchased via the Internet. Escrow services act as third parties to both buyers and sellers. This service provides users with a degree of assurance by holding payment until the purchaser can verify that the goods received were what the purchaser had bid for and upon confirmation the service forwards the money on to the seller.\textsuperscript{128} This type of service increases the level of trust because it acts as a third party and tracks the product purchased.

Trust seals or trust marks have emerged as an important self-regulatory tool for Internet content and e-commerce. Recognised trust seals or marks on Websites appear to provide added assurances to Internet users and may increase the consumer's level of trust as they are based on a common set of standards (which may take the form of codes of conduct). However, one of the challenges with this type of approach is that illegitimate Websites can also deceive consumers by reproducing trust seals or marks on their Website in the hope of attracting consumers. A report prepared by PCMLP notes that the challenges with trust seals derive from monitoring compliance and consumer awareness. This point was supported by research which showed that '...brand awareness of trustmark schemes is low. Particularly, where there is competition between trustmarks, the consumer is unlikely to recognise a truly Internet trustmark' (PCMLP 2004:47).

\textsuperscript{128} A fee is required to obtain escrow services.
EBay, an online auction marketplace, provides customers with the option to use their company-owned escrow service. The advantage of an eBay-owned escrow service is that it may limit or decrease the number of fraudulent transactions because of the details and personal information required to carry out the transaction. An increase in the guardianship of escrow services needs to be considered to increase levels of trust that Internet users need to effectively purchase goods online.

In summary, market approaches are an effective method of guardianship and self-control on the Internet although it is likely that market approaches alone will not control criminal behaviour. This view is echoed by a number of submissions to the APJCACC (2004:10-11) who noted that a number of

... parents rely on software filtering programs to protect their children from unsuitable content. These are varying degrees of usefulness, as the filter tends to eliminate material which appears to be objectionable but which is not. Filters can also do the opposite, and fail to filter very much content at all.

7.4.3 State-Based Regulation – Law Enforcement

Traditionally, law enforcement has played a central role in policing, investigation, detection, and prosecution of a broad range of conventional types of crime in the terrestrial world (see Burns et al. 2004). However, the transnational nature of cyber crime and the increased sophistication of criminals and criminal networks have forced a re-evaluation of the role of law enforcement and methods of policing. As such, traditional methods of law enforcement and policing have to be modified to take into account the changing landscape of the Internet (Brenner 2003). Brenner argues that factors such as proximity, scale, physical constraints, and patterns form the basis of how policing is carried out in the terrestrial world and that, because of the different configurations of the Internet, a law enforcement approach needs to take into account the changing structures.

While the Australian Government initially adopted a free-market approach to regulating behaviour on the Internet, the subsequent rise of cyber crime has prompted the establishment of a centralised enforcement agency sponsored by the Australian Federal Police (AFP): the Australian High-Tech Crime Centre (AHTCC). The AHTCC, which
was established in 2001 under the auspices of the Australian Federal Police, has a number of individuals seconded from the banking sector working closely with federal agents to detect and prevent online fraud. This is one of the first joint Internet initiatives between law enforcement and the private sector in Australia.

In addition, the Australian Crime Commission (ACC) assists in investigation by collecting and analysing information and intelligence (AJPACC 2004:11). In the Attorney-General’s Department submission, Schneider (2003:17) stated that:

The responsibilities of these organisations are diverse, and in most cases Cybercrime forms only a portion of their work. Each of these entities has different roles ranging from the development and coordination of policy, to policing and prosecution of crime.

The role of the AHTCC (2003:1) is to:

- Provide a national coordinated approach to combating serious, complex and multi-jurisdictional high tech crimes, especially those beyond the capability of single jurisdictions;

- Assist in improving the capacity of all jurisdictions to deal with high tech crime; and

- Support efforts to protect the National Information Infrastructure.

Cooperation between law enforcement agencies can also mean that costs and resources are shared (an issue that was identified in Chapter Five as one of the barriers to policing the Internet). The active involvement and online presence of enforcement agencies in e-commerce instils market confidence through combating cyber crime and identifying potential and future threats and thereby increases public confidence. Aggressive law enforcement can deter some people from offending and prevents a country from becoming a repository for criminal activity and data storage.

Research carried out by the UK Home Office explored responses to criminal threats and future challenges to crime on the Internet (Morris 2004). The report underscored the need to understand criminal behaviour on the Internet prior to devising strategies to overcome them. Morris (2004:12) suggests that reducing crime through law enforcement should involve ‘... a combination of technological surveillance and law
enforcement investigation expertise [which] can be combined to attempt to identify and potentially track offenders, who may be operating alone or as part of a wider network'. However, the respondents in the research identified that law enforcement should lead such initiatives rather than industry alone. This is important given the increased powers of law enforcement officers and agencies and the cooperative approach with their global counterparts.

Chapter Five identified that one of the major barriers to law enforcement on the Internet (identified in Chapter Four) is the lack of harmonised laws and criminal codes that provide a basis for investigating and prosecuting cyber criminals. One of the most notable examples that highlight the absence of harmonised laws was the global release of the 'ILoveYou' virus, which was allegedly carried out by a Filipino student. At the time that the virus was disseminated, the Philippines did not have laws against creating and disseminating viruses, which meant that the student could not be charged under the current laws despite the global destruction the virus created. Although the 'ILoveYou' virus prompted a change in laws across the globe it nevertheless highlights the jurisdictional challenges that a lack of unified laws pose for other types of crime.

The evolving nature of computer and information-based technologies also makes it challenging for law enforcement officers to detect and investigate cyber crime due to a range of factors. These include lack of resources (i.e. financial and personnel needed to equip officers to master and keep up with emerging technologies), lack of a centralised operational body to detect and investigate cyber crime, and the modus operandi, which prohibits the response of law enforcement as a reliable form of guardianship. In addition, the growth of criminal networks and organised crime syndicates on the Internet, which can be located in various countries around the globe, presents new challenges for law enforcement officers, such as time-zone differences, language barriers, cultural differences, lack of mutual assistance, not to mention legal challenges (see Westby 2003).

Westby (2003:5) identifies three fundamental challenges – technical, legal and operational, that law enforcement faces in relation to combating cyber crime:
• Technical challenges that are caused by (a) rapid changes in technology and the inability of law enforcement to stay current and (b) technical shortcomings that impair finding and prosecuting cyber criminals.

• Legal challenges that are caused by procedural barriers or hurdles and the inability of legal frameworks around the globe to keep up with technological capabilities and the changing business environment.

• Operational challenges that are caused by (a) a lack of equipment, training, and adequate organizational structures, and (b) the need to work with great speed despite time zone, language, and cultural differences.

While this section has highlighted some of the limitations of law enforcement, it nevertheless underscores the important role law enforcement plays in investigating and preventing cyber crime on a local, regional, and international level and as a regulatory response to cyber crime. One of the central themes running through this analysis is the importance of global and mutual cooperation. The following sub-section highlights the need to support such initiatives.

7.4.4 Global Cooperation

Towards the beginning of the twenty-first century, global efforts have been stepped up to address current challenges of policing and regulating the Internet and criminalising particular offences (see Grabosky 2001b; Broadhurst 2004). The exponential growth in crimes carried out on the Internet precipitates the need to look beyond local frameworks. This view is supported by the way that crimes are carried out on a local and global scale as well as the increased sophistication of individuals, businesses, and organised networks and syndicates in committing cyber crime.129

The preceding two chapters found that cyber crime presents one of the most complicated and highly challenging areas of law enforcement because of its global nature. One of the regulatory strategies to reduce the barriers of the global and

129 Research identifying organised networks and organised crime on the Internet is limited. One of the challenges lies in the lack of reliable data and the challenge with differentiating what proportion of Internet crime is organised (see Morris 2004:12).
transnational nature of cyber crime is the need for mutual global cooperation between communities, associations, industries, corporations, governments, and nations. Broadhurst (2004) argues that in order to control and combat cyber crime, regional and international cooperation plays a key role in bridging communication and information sharing between local, regional, and international enforcement agencies, government and countries.

For a regional and international cooperative approach to be effective in combating cyber crime, Broadhurst and Grabosky (2005:26) delineate six strategies:

- Improve security awareness by providing adequate resources to secure transactions and equip system operators and administrators;
- Improve coordination and collaboration by enabling systematic exchanges between the private sector and law enforcement including joint operations;
- Take steps to ensure that technology does not outpace the ability of law enforcement to investigate and enact substantive and procedural laws adequate to cope with current and anticipated manifestations of cyber-crime;
- Broadly criminalise the conduct (including juvenile offenders) and focus on all violators big and small;
- Strengthen international initiatives by updating existing treaties and agreements to recognise the existence, threats and transnational nature of high-tech computer-related crimes and strive for legal harmonisation;
- The development of forensic computing skills by law enforcement and investigative personnel and mechanisms for operational cooperation between law enforcement agencies from different countries, i.e. 24/7 points of contact for investigators.

Given the increasingly sophisticated and complex nature of crimes carried out on the Internet, the role of international agencies such as the United Nations and Interpol is more essential in this milieu than ever before (Broadhurst and Grabosky 2005). The recent global operation on child pornography, Operation Falcon in the United States of America and Operation Auxin in Australia, underscores this need and highlights the fact
that without mutual cooperation, efforts to control criminal behaviour on the Internet will be less effective.

The theme identified in a number of these approaches is the need to build networks of trust. Networks of trust are an important tool that provide the mechanism to build confidence in consumers and also allows information to be passed on to law enforcement agencies and businesses in the global effort to combat cyber crime.

7.5 EXAMPLES OF REGULATORY APPROACHES TO CONTROLLING BEHAVIOUR ON THE INTERNET

In the late-twentieth century, crimes in cyberspace marked the transition of a new understanding of deviance and criminal behaviour with the modernisation of information and computing technological networks such as the Internet and the World Wide Web. As previously argued, regulatory responses appear to contribute significantly to reducing and controlling criminal behaviour on the Internet.

This section suggests that reducing the supply of motivated offenders, decreasing the availability of suitable targets or victims, increasing methods of capable guardianship, understanding the various strategies used to establish and exploit trust, and illustrating an effective regulatory response can further assist in reducing criminal behaviour on the Internet. In the light of this, Cohen and Felson's three prerequisites — motivated offender, availability of suitable target, and absence of capable guardianship are applied as well as violation of trust and regulatory response to three types of cyber crime: auction fraud, Internet securities fraud, and extortion. The objective is to examine the applicability of these approaches to each crime.

7.5.1 Auction Fraud

With the growth in Internet auction fraud, regulatory responses have become an important mechanism to assist in thwarting would-be cyber criminals.130 EBay has become a market leader in developing self-regulatory strategies by decreasing the

---

130 A broad range of empirical studies has focused on eBay's feedback system (Bajari and Hortacsu 2000; McDonald and Slawson Jr. 2002; Melnik and Alm 2002; Resnick et al. 2002). The majority of these studies are not controlled experiments with the exception of Resnick et al. (2002).
availability of suitable targets or victims and increasing methods of guardianship through a variety of approaches. For example, the development of a feedback or reputation ratings system assists members in making decisions to purchase goods by viewing feedback from other purchasers by the same member on payment experience, interactions, speed of shipment and additional experiences. This form of feedback provides an opportunity for those who have been dissatisfied with their purchase to make other members aware and to alert prospective purchasers of their experience.131

According to eBay (2004:1), 'such member-to-member comments help the millions of buyers and sellers in the eBay community build trust and share their trading experiences with others'. It is important to note that potential criminals can use deceptive techniques such as opening eBay accounts online and providing strong self-ratings under different aliases in furtherance of providing a false sense of trust to potential victims. While there are limitations associated with self-reporting, the feedback system allows eBay to track the nature of complaints and identify specific areas that can be used to gather statistical data and narrow specific areas for target testing.

Given the statistical picture outlined by IC3, which found that non-payment and non-delivery of goods account for the majority of complaints, escrow services appear to provide an effective form of guardianship. eBay buyer protection such as PayPal attempts to promote a level of trust with eBay members by covering members to the amount US$500 when using the service for a qualified listing. PayPal is an intermediary service that provides an air gap between buyers and sellers. In addition to the self-regulatory approaches adopted by eBay, other approaches to reduce fraud include risk analysis conducted by eBay, fraud filters and security tools such as encryption which further increase methods of guardianship.

The methods of guardianship outlined above appear to increase confidence of legitimate members. However, it is also important for eBay members to be aware of the different techniques that criminals employ in committing Internet fraud. Ebay’s trust and safety manual promotes awareness and aims to educate online users on how to safely buy or sell online. Such an initiative is a positive approach and contributes to reducing the

131 For a more detailed analysis of how eBay’s feedback system works see Resnick and Zeckhauser
availability of targets. In addition, the IFCC (2005b:1) outlines a number of prevention tips for buyers and sellers to consider as well as publicising steps to take if victimised:

- Understand as much as possible about how the auction works, what your obligations are as a buyer, and what the seller’s obligations are before you bid.

- Find out what actions the Web site/company takes if a problem occurs and consider insuring the transaction and shipment.

- Learn as much as possible about the seller, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where the seller/business is located.

- Examine the feedback on the seller.

- Determine what method of payment the seller is asking from the buyer and where he/she is asking to send payment.

These approaches show legitimate members that eBay and enforcement agencies take auction fraud seriously and hence may deter some types of criminals through the various forms of guardianship and through education and awareness. Furthermore, the self-regulatory approach by eBay appears to constitute a strong framework to keep apace with technological changes and techniques used by criminals. The NAA propose that online auctioneers adhere to professional codes of conduct and regulatory approaches that are imposed upon auctioneers in the terrestrial world.

Having established that minimal differences exist between the nature of auctions in the terrestrial and virtual worlds, the NAA ‘... recommends state license and regulat[ing] [of] online auctions and auctioneers under modified forms of existing laws’ to be applied to auctioneers trading on the Internet (Theurer 2003:3). The absence of standards of conduct and a demonstrated knowledge of regulatory processes in online auctions prompted the NAA to recommend alternative regulatory approaches. It is the belief of the NAA that ‘... those individuals who conduct auctions on the Internet should be licensed in the state in which they reside’ (Theurer 2003:4). The objective of this

approach is to promote fair competition between online and terrestrial auctioneers and a standardised level of practice among auctioneers (see Theurer 2003).

The NAA (2003:4) suggests that ‘current licensing laws should be interpreted to include online auctions’ (in Theurer 2003:4). This means that the 29 states in the United States that license auctioneers in the terrestrial world should apply similar standards to online auctioneers in those states. The NAA (2003:4) recognise that modifications to the online environment will be necessary. For example, they suggest that ‘... knowledge of bid calling practices and course[s] of study at an accredited auction program or apprenticeship–are [sic] simply not practical for online auctioneers’ (NAA 2003 in Theurer 2003:4). The NAA (2003:5) believe that imposing regulation on online auctioneers ‘... guarantee[s] industry professionalism, protect[s] customers and ensure[s] fair competition between online and traditional auctioneers’ (in Theurer 2003:4).

However, should a national auction house such as eBay be required to obtain 29 licenses for each of the 29 US licensing states?

Building networks of trust between online corporations such as eBay and law enforcement agencies around the globe are likely to provide the key to forming effective approaches to controlling Internet fraud.

7.5.2 Internet Securities Fraud

Grabosky and Smith (2001) argue that a range of countermeasures is required to control securities fraud: state-based regulation through government agencies such as the Australian Securities and Investment Commission (ASIC); self-regulation through industry associations and companies; law enforcement, and international mutual cooperation; and code-based regulation. However, what separates these countermeasures is the need for code-based regulation such as software and hardware to respond to the technological and sophisticated nature of cyber crime.

State-based enforcement has traditionally played a central role and may be viewed as an effective regulatory response for securities fraud. As Grabosky et al. (2001:85) argue:

In order to protect against various forms of fraud, most nations with significant securities markets have developed strict regulations for offering securities. These entail a requirement that securities offered for sale be registered with the relevant regulatory agency, such as ...
Securities and Exchange Commission (SEC) in the United States, or the Australian Securities and Investment Commission (ASIC) in Australia, and that the offer be accompanied by a prospectus, setting out in considerable detail the circumstances of the offer.

Internet fraud sweeps conducted by state enforcement agencies in over 30 nations around the globe appear to be an effective method of state-based enforcement to combat online fraud. The ACCC (2004:1) notes:

The International Internet Sweep is an example of worldwide consumer protection agencies working together to combat cyberscams. ICPEN* [sic] is a network of consumer protection authorities of 31 countries. Its main objective is to take action to prevent and redress deceptive marketing practices with an international component. The network fosters cooperative efforts by member authorities to tackle consumer problems connected with cross-border transactions in both goods and services. Exchange of information between authorities also plays a key role in effective investigations and court action where necessary.

The advantage of this type of action is the global cooperation between agencies through the exchange of information and methods employed to educate investors. Forming networks of trust between enforcement agencies and the private sector may increase the response rate and knowledge of the techniques used by fraudsters.

Commonly held views of the challenges to law enforcement in investigating and controlling Internet fraud are well established. These include, for example, a lack of resources and manpower to investigate Internet fraud (see Farnsworth and Knap 2002); lack of training (Meyer and Short 1998); inadequate laws (Meyer and Short 1998; Farnsworth and Knap 2002); and jurisdictional issues (Farnsworth and Knap 2002; Smith et al. 2004). Burns et al. (2004:479) also suggest that ‘the changes required of law enforcement agencies in response to Internet fraud will undoubtedly pose vexing problems to organisations historically known for their rigidity’. The challenges of technological advancement in the organisational structures will undoubtedly contribute to the policing of Internet fraud.

Burns et al. (2004) carried out a study assessing law enforcement’s preparedness to address Internet fraud. A survey completed by 217 law enforcement agencies revealed a number of interesting findings. Burns et al. (2004:482) note that approximately ‘... 70 per cent of respondents agreed or strongly agreed that additional legislation was needed to deter Internet fraud [and approximately] ... three-quarters of the respondents reported the need for additional laws for effectively punishing Internet fraud’. Interestingly, these
figures suggest that an increase in law enforcement and additional laws may contribute
to the facilitation of national and international enforcement and a greater capacity to
define enforcement boundaries (Burns et al. 2004:482). The recognition of the role of
regulatory agencies along with law enforcement combined may produce more effective
outcomes in reducing and controlling Internet fraud. One of the key elements towards
controlling Internet fraud requires greater dissemination of information within law
enforcement and regulatory agencies.

Education and awareness is also an important yet underestimated response to cyber
crime. Studies by Dutton and Shepherd (2003) and Yi et al. (2002) have shown that
experience contributes to increasing levels of trust. Linked to experience are educating
and informing potential and current investors. The IC3 provides information on its
Website and publishes tips on how to avoid becoming a victim of fraud. Smith and
Grabosky (2001:66) suggest that ‘tremendous opportunities also exist for regulatory
agencies to communicate with clients and stakeholders’ thereby not limiting the role of
education and awareness to individual users.

In Australia, for example, the ASIC has a Webpage, FIDO, dedicated to informing
subscribers of the latest scam and educating users of the dangers associated with trading
online. Similarly, in the United States, ‘... the Commodity Futures Trading Commission,
the federal agency for the regulation of futures trading, posts photographs of suspects on
its Web page and provides a facility to e-mail information about suspects directly to the
agency’ (Smith and Grabosky 2001:66-7). The advantages of this service include the
Internet’s global reach, which allows users to view images and alert the broader
community, to increase awareness of the dangers associated with particular forms of
trading and alert users of the various strategies used by motivated offenders.

Investing in education provides an additional and effective regulatory approach. The
challenge with this form of regulation is ensuring that companies and regulatory
agencies continue to educate and alert online investors to be aware of strategies to
establish and exploit trust through online forums and chat rooms. ISPs may also provide
an additional response by alerting their members through online forums and chat rooms
on the strategies fraudsters use in furtherance of criminal opportunities.
Smith and Grabosky highlight the effectiveness of self-regulatory strategies against online securities fraud through monitoring and third party audits of Websites. They maintain that ‘the digital age has provided securities industry associations and stock exchanges with unprecedented market surveillance capability’. Smith and Grabosky (2001:68) cite examples to demonstrate this:

In the USA, the NASD has a Netwatch facility with sophisticated software for scanning and retrieval. The New York Stock Exchange (NYSE) “Stock Watch” is an electronic monitoring system to detect unusual trading patterns such as anomalies in price and volume, which may be indicative of manipulation and insider trading.

7.6 SUMMARY

It is trust that has a major role in building trust (Job and Reinhart 2003:84).

There is no single regulatory approach which will effectively control cyber crime but rather a multi-pronged approach is needed. Self-regulatory approaches may be one of the most effective components of regulation of online auctions to update and review methods of guardianship and decrease the availability of suitable targets. Although laws may be instituted, they are less swift in their approach to technological change and state-based enforcement. Moreover, the state may lack the human resources to detect and investigate this type of crime. In contrast, state-enforcement and market approaches appear to have more promise as an effective regulatory approach to online securities fraud. This is because mechanisms to detect online securities fraud have yielded successful convictions and shown confidence in the marketplace. Educating users through public awareness campaigns and conducting annual Internet sweeps is also an important preventative strategy that is currently in practice.

The analysis also showed that the global nature of the Internet requires a global response, which means that cooperation between corporations, law enforcement agencies and government is central to achieving success in the investigation of cross-national crimes. Despite the growth in regulation of the Internet, there remain new challenges ahead, such as the emergence of new technologies and industries, which need to be considered in efforts to combat cyber crime. These challenges reiterate the need to build networks of trust in the private and public sectors and an imagination in countering crime as creative as that of the perpetrators of cyber crime.
CHAPTER 8: DISCUSSION AND CONCLUSION

This chapter will discuss the findings of earlier chapters. It will also outline the issues that are central to controlling cyber crime and discuss the challenges for the future study of crime and criminal behaviour on the Internet.

8.1 CRIMINAL BEHAVIOUR ON THE INTERNET – SUMMARY OF FINDINGS AND IMPLICATIONS OF RESEARCH

This research set out to test whether existing theories of crime and criminal behaviour can be used to explain different forms of cyber crime and, if so, to what extent. The thesis also set out to identify those factors that may assist theoretical understandings of different forms of cyber crime and ways of controlling it. A further broad objective was to develop the issue of trust as a significant concept to understand criminal behaviour on the Internet from a criminological perspective and explore approaches of trust as a core regulatory dimension to control criminal behaviour on the Internet.

Chapter Two showed that various debates on defining white-collar crime through offender or offence-based classifications have to some extent befuddled the study of white-collar crime. This sustains a conclusion that criminology should not continue to focus on the offender if it is to move forward as a discipline. Similarly, the focus on the offence restricts the labelling of crime as either conventional crime or white-collar crime. In the meantime, studying cyber crime, which the subsequent chapters reveal to be a coherent category of criminality, as a phenomenon not entirely bounded by the concept of white-collar crime, is worthy as a way forward.

Chapter Three found that the five theories of criminal behaviour have some explanatory power for a diverse range of white-collar crimes. The findings suggest that Sutherland and Gottfredson and Hirschi’s general learning theory lack the ability to explain white-collar crime through the same principles of behaviour. Furthermore, the analysis showed that criminology’s pre-occupation with conventional crime and juvenile offending is still evident. White-collar crime challenges the assumption prevalent in much criminological theorising that criminal behaviour starts in adolescence and manifests psychological defects such as poor self-control. This thesis argues that an adequate theory of criminal behaviour needs to include adult offenders, regardless of
their status and position and include a broad range of crimes, rather than a focus on conventional crime, if is to remain important in understanding emerging forms of crime and criminality.

Chapter Four established that the nature of cyber crime encompasses a broad range of traditional and new forms of crime, which have emerged distinctly from the advancements in technological applications of the Internet. It also established that crimes carried out on the Internet are distinguished by three criminogenic attributes that assist in the proliferation of cyber crime: the use and preservation of anonymity, multiplicity, and exploration.

Chapter Four also showed that crimes carried out on the Internet encompass a mixture of conventional forms of crime and crimes that are white-collar and organised in nature. This presents new challenges in understanding criminal behaviour on the Internet because offenders can no longer be categorised as conventional or white-collar. The implications are that criminology’s pre-occupation with categorising crime as either conventional or white-collar crime has imposed limitations on the study of crime and criminal behaviour on the Internet. This research has also shown that crimes committed on the Internet challenge such assumptions, and confusion that engenders weak analysis may arise if distinctions between the two categories continue to be made.

Chapters Five, Six, and Seven were the central chapters of this research. The result of the analysis of Chapters Five and Six found that two theories survived as particularly useful for explaining crime on the Internet - Cohen and Felson’s routine activity theory and Shapiro’s theory of trust violation. These theories were able to explain diverse types of cyber crime. The remaining four theories: differential association theory, strain theory, techniques of neutralisation, and a general theory of crime showed much more limited applicability.

Differential association theory showed some promise from the outset given the ease with which associations are formed over the Internet through chat rooms, bulletin boards, e-mail, and news groups. The analysis found that the social organisation of the hacking underground allows criminal activity to be fostered through group association more easily than through individual learning. Whilst the analysis provides a strong correlation between hacking, group association, and learned behaviour, most forms of hacking are carried out by lone individuals. Similarly, these conclusions were formed
for piracy and Internet sex crimes against children. Although the examination found that
the Internet’s global capabilities have furthered the distribution of software, music, and
video through global associations, it is difficult to conclude whether these associations
influenced their behaviour.

The analysis concluded that some pornography rings are influenced by group
association. While the social and organisational structure of these groups indicate that
the more one associates with deviants, the greater the chance the deviant will develop
attitudes and skills that are favourable to a violation of law, a number of cases revealed
that group association and learned behaviour were not relevant to individuals who acted
alone.

Differential association theory was found to be least applicable to fraud although the
analysis demonstrated that small entities were involved in online fraudulent schemes.
That groups of people were involved in these schemes does not suggest that techniques
and skills were developed and used to carry out the fraud. Furthermore, a number of
examples also point to individuals participating alone in auction fraud, phishing, and
online share-market manipulation schemes.

The strength of this theory to explain hacking, piracy, and Internet sex crimes against
children was strengthened by the ease with which networks are established and
maintained by like-minded individuals (through chat rooms, e-mail, news groups, and
private bulletin boards) and the preservation of anonymity, which appear to increase the
likelihood of learned behaviour (through chat rooms, discussion groups, ftp servers, and
e-mail). As Internet take-up increases, the opportunity to establish networks for criminal
purposes in the future also appears likely. An important point to draw from this analysis
is that trust played a major role in both the success and failure of these groups. Trust
developed in these groups reinforced their purpose.

As a general theory of crime, differential association showed limitations as individuals
commit a wide variety of types of crimes in the absence of identifiable learning
mechanisms or association. While it was difficult to empirically assess criminal groups,
the examples analysed do lend support to the conclusion that networks facilitate the
growth of criminal activity. Hence, while differential association theory cannot be put to
use as productively as routine activity and violation of trust paradigms, it is not utterly
devoid of promise that might be explored in future research.
Merton’s (1938) strain theory showed limitations from the outset because only two of the four adaptations – innovation and rebellion – proved to have applicability to particular types of crime. The analysis of innovation showed examples of financial gain in all crime types; particularly strong relevance was evident with hacking, Internet securities fraud, and phishing. The limited applicability of innovation is that low income is not the only indicator of strain. The limited applicability of innovation can also be explained by additional motivations, for example, hackers and pirates are also motivated by curiosity, revenge, and thrill seeking rather than by the pursuit of wealth.

The rebellion mode was able to explain crimes committed by disgruntled employees who intentionally cause damage to computer systems, and by Internet pirates. The analysis showed through these crimes that the Internet provides ways for individuals to devise alternative methods of behaving and concealing activities in furtherance of criminal opportunities. The absence of a global legal framework and regulatory response appears to assist in the attractiveness for offenders in providing the means for the rebellion adaptation. The rebellion mode was unable to explain the role group processes and networks play in deviant behaviour. There is not compelling evidence that most cyber crime is motivated by blocked legitimate opportunities, though the anonymity of the Internet certainly creates new illegitimate opportunities.

Sykes and Matza’s (1957) five techniques of neutralisation proved partially applicable to piracy and child pornography although their theory was not very applicable to fraud. The strongest applicability to the five techniques was hacking. This theory has limited explanatory power for different forms of crime. The different motivations of pirates and fraudsters may partially explain the lack of support this theory offers. As more cases of cyber crime are investigated, evidence of the applicability of this theory may yield a different outcome.

The analysis of Gottfredson and Hirschi’s (1990) general theory of crime to different types of cyber crime found that a great many crimes are committed for reasons other than a propensity to low self-control. The analysis suggested that the Internet facilitates the means to carry out crimes, such as hacking and Internet sex crimes against children because of the ease of accessibility, the potential global reach, assumed anonymity, and its access to like-minded individuals. While a predisposition to low self-control can explain some forms of crime, the analysis contests Gottfredson and Hirschi’s (1990)
claim that crime reduces as individuals advance in age. This was the case among hacking, piracy, sex crimes against children and youth, and Internet fraud. Factors such as opportunity and access to information of like-minded individuals and assumed anonymity have showed that some perpetrators of Internet crime are first time offenders and in some cases, began engaging in criminal activity on the Internet in their early 40s.

The analysis of Cohen and Felson’s (1979) data provided strong evidence to explain a diverse range of crimes through three pre-requisites – a supply of motivated offenders, the availability of suitable targets, and absence of capable guardianship. The examination of a range of cyber crimes showed that the motivations to carry out cyber crime are analogous to the motivations to commit crime in the physical world. It also showed that the availability and attractiveness of suitable targets appear to increase due to factors such as the global nature of the Internet, the absence of time and physical space, and a range of different targets – information, individuals, Websites, corporations, and governments on a single platform.

The analysis also showed that an absence of capable guardianship contributes to the growth and proliferation of different forms of crime. This was evident through the lack of harmonised laws to prosecute cyber criminals, the time required to investigate different crimes, the limited extent of cooperation (in some cases) between law enforcement agencies and government departments, the lack of manpower and resources to properly assess and investigate cyber crime, the Internet’s multi-jurisdictional nature, and inadequate risk management by prospective victims. The implication for this is that strategies will require different approaches given the uniqueness of some forms of cyber crime and the different methods and targets used to carry out the crime.

Chapter Six found a recurrent patterning of breaches of cyber trust. Deception through exploiting an architecture of anonymity is the largest overarching pattern. Deception is then patterned as lying, phishing, bid-rigging, market rigging more widely, self-dealing, role conflict, espionage, stalking, hacking, perhaps corruption, seducing and tricking children, and acquiring false identities. Not all breaches of trust are best conceived as fundamentally about deception. There are forms of theft that are not particularly deceptive such as pirating music, and forms of exploitation that are not very deceptive such as exchange of child pornography between consenting adults. Yet abuse of trust
norms to deceive is revealed in this thesis as the dominant driver of the patterns revealed.

One of the predominant findings of Chapters Five and Six is that violation of trust plays an important role in explaining the role of criminal behaviour on the Internet. It is important to point out that some forms of trust create opportunities for would-be cyber offenders and as a result, more targets are available, and trusting individuals may not mobilise available safeguards, such as firewalls, which imply less guardianship.

The analysis showed that trust violation alone may not explain the motivations or targets although it demonstrated that violation of trust is a significant factor assisting in the successful commission of crime. The research also argued that trust violation complements Cohen and Felson’s three pre-requisites. The implications of this are that further empirical research is required to explore whether the integration of trust violation to Cohen and Felson’s theory enhances explanation.

Chapter Seven identified many regulatory tools that are available, so that a multi-pronged approach is a possibility. In the absence of knowing which strategies can work effectively on their own, the redundancy of a multi-pronged approach – covering the weaknesses of one with the strengths of another – has appeal. Furthermore, monitoring these approaches can only increase levels of trust and confidence in the marketplace for users and businesses. This trust is essential for delivering on the economic and social benefits of the Internet. Once again, building and maintaining networks of trust between local and global enforcement agencies may bolster countermeasures against Internet fraud.

The following section outlines a number of critical issues and challenges for future research, which result from the analysis in the previous seven chapters.

8.2 ISSUES AND FUTURE CHALLENGES IN REGULATING CYBERSPACE

One of the issues to emerge from this research is the need for a multi-pronged approach to regulation. This research showed that current laws are inadequate because of the absence and unlikelihood of a globally harmonised legal framework. One of the future challenges lies in recognising the jurisdictional boundaries of cyber crime and the need to maintain a global approach to investigating and prosecuting cyber criminals. Given
the Internet’s global nature and the lack of harmonised laws, an approach that emphasises self-regulation, market approaches, law enforcement, and mutual global cooperation together will be necessary to control the global phenomenon of cyber crime.

Self-regulation is an important regulatory response to reducing the number and levels of violation of trust. In the terrestrial world, for example, if an individual is aware that various streets are considered more unsafe than other streets, the likelihood of individuals visiting those streets for entertainment or recreational purposes diminish. The recent placement of street cameras in known hot spots of crime also increases the awareness of individuals with the objective of reducing crime in certain areas. If we adopt this approach and apply it to the Internet, i.e. if individuals were aware of the possible implications associated with communicating in public online forums and chat rooms for example, individuals may choose not to develop or may be more wary of developing friendships and relationships online. However, if this approach is applied we have fewer and fewer individuals trusting communication in the Internet. The issue is to develop ways to allow individuals to communicate in a safer environment.

Identifying which regulatory responses are more effective for different forms of crime is also important. The effective regulatory approaches may shift over time. These shifts may be due to the increasingly sophisticated methods used to carry out cyber crime, the increased role of criminal networks (informal and formal), technological changes, and the enactment of new laws. Some crimes may initially respond to self-regulation and market approaches, but monitoring may later indicate that additional forms of regulation may provide more effective outcomes. This is important for regulators and practitioners who need to be innovative in their approach to control different forms of cyber crime in a changing electronic environment.

Another challenge lies in considering a broad approach to regulating behaviour of Internet users. A future regulatory approach may require the implementation of a cyber crime control plan implemented by the state to enforce behaviour and impose conditions on Internet providers and corporations to monitor online behaviour if current regulatory strategies do not work. This approach places responsibility on the service providers although the monitoring of crime and criminal behaviour may again shift this approach to different agencies.
This research suggests that end user compromise presents one of the new challenges to controlling crime on the Internet because of the accessibility of suitable targets. Educating Internet users to behave in a manner that protects and empowers them on the Internet will continue to play a key role in prevention and must be adopted by industries and service providers.

It is important to re-emphasise the need to maintain cooperation between local and global interests and establish networks of trust. This research has argued that the development of trust networks can begin at the personal (micro) level and extend through to communities, organisations, corporations, enforcement agencies, government, and nations (macro level). Furthermore, as new technological applications develop to expand the Internet or attempt to supersede and create new applications, new ways will be created for the illegal facilitation and transaction of crime. Faster and more efficient methods will also become available and methods of concealment of criminal behaviour may be more diverse and sophisticated. It is important for practitioners and regulators to consider that further challenges to regulating cyber crime will continue to arise and to be debated, partly because new technologies enable greater expansion of local and global markets and increases in opportunity.

Another concern lies with the placement of resources, emphasis, and narrow focus on particular crimes while not distributing effective methods of control to new forms of crime as they emerge. This may create moral panics about the true nature and extent of cyber crime. Furthermore, statistics on crime continue to focus on conventional crime and juvenile offenders, which may reinforce stereotypical notions of what cyber crime is and what constitutes the type of offender.

This research recommends further empirical studies on different forms and trends in cyber crime as an important area for future analysis. Future research could consider empirically assessing criminal networks to examine whether learned behaviour and association are two central variables that link these networks to a range of cyber crimes. Two of the challenges are recognising the future capabilities of networks and applying responsive approaches to controlling crime through networks given that association and learned behaviour may play a significant role.

Regulating the Internet is still in its early days. However, as more and more research seeks to understand the phenomenon of criminal behaviour on the Internet and as cyber
crime proliferates, regulation needs to be further debated and refined. This research has found that the way criminologists have studied crime, and law makers applied laws to crime, may not be as effective in the virtual world. This is because the Internet is a place where both conventional and white-collar crimes are carried out. Given that this is a growing area, this research has shown that trust and the growth of networks provide the key to understanding criminal behaviour and developing methods for its control.

The research has demonstrated that regulation of the Internet is essential to ensure a safe and trustworthy medium to carry out commerce and communication. Further, the key in the global fight against cyber crime remains in building cooperative networks of trust between individuals, organisations, law enforcement, governments, and international bodies such as the Council of Europe (CoE) and the United Nations (UN). It is therefore important that these bodies continue to pursue such issues and guide legislative changes as new crimes and behaviours develop.

This research has contributed to the study of criminology through an examination of five theories of criminal behaviour, which were applied to different types of cyber crime. The umbrella hypothesis of this thesis was that existing theories of crime do explain criminal behaviour committed on the Internet. However, the research found that only two theories adequately explain a diverse range of cyber crimes – Cohen and Felson’s routine activity theory and Shapiro’s theory of trust violation. The results of the analysis also show that the issue of trust is significant to understanding the strategies employed in furtherance of criminal opportunities. The research establishes that criminogenic attributes, such as the use and preservation of anonymity, multiplicity, and exploration contribute to the proliferation of cyber crime. Given the diverse ways in which trust is violated, the research also suggests that trust is a significant issue and that networks need to be developed to control criminal behaviour on the Internet.
Bibliography


ABCI – See Australian Bureau of Criminal Intelligence

ACCC – See Australian Competition and Consumer Commission

Adams, D 2003, ‘Foiling the online conmen’, *The Sydney Morning Herald*, Fairfax Publications, Australia, 17 June 2003,


AHTCC – See Australian High-Tech Crime Centre


BIBLIOGRAPHY


Anti-Phishing Working Group 2004, *Committed to wiping out internet scams and fraud*, Anti-Phishing Working Group


http://www.antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf

Antiques Online 2004, Antiquesonline.com.au,

Antonova, M 2004, *Russian consumers choose pirates over copyright*, MosNews.com, 19 October 2004,

APWG – See Anti-Phishing Working Group


ASIC – See Australian Securities and Investments Commission


Barber, R 2001, ‘Hackers profiled – who are they and what are their motivations?’, *Computer Fraud and Security*, vol. 2, pp.14-17.

Barlow, HD 1991, ‘Explaining crimes and analogous acts, or the unrestrained will grab at pleasure whenever they can’, *Journal of Criminal Law Criminology*, vol. 82, pp. 229-242.
BIBLIOGRAPHY

Barnes, C 2000, Internet contributes to rise of identity theft, CNET News.com, 30 August 2000, 

Beales, H 2004, ‘Efforts to fight fraud on the internet’, Prepared statement of the 
Federal Trade Commission before the Senate Special Committee on Aging, 

Beccaria, C [1764] 1963, Of crimes and punishments, translated by H Paolucci, 
Macmillan, New York.

The Washington Post Company, 1 September 2000, 

Bennett, RR 1991, ‘Routine activities: a cross-national assessment of a criminological 

Benson, ML 1985, ‘Denying the guilty mind: accounting for involvement in white- 

Benson, ML & Moore, E 1992, ‘Are white-collar and common offenders the same?’ 

Bentham, J 1776, A Fragment on government; being an examination of what is 
delivered, on the subject of government in general in the introduction to Sir William 
Blackstone's commentaries; with a preface in which is given a critique on the work at 
large.

Bentham, J [1789] 1907, An introduction to the principles of morals and legislation, 


Bernburg, JG & Thorlindsson, T 2001, ‘Routine activities in social context: a closer 
look at the role of opportunity in deviant behaviour’, Justice Quarterly, vol. 18, no. 3, 

Bethel, R 2000, in Federal Trade Commission 2000, (eds) Going, going, gone... law 
enforcement to combat internet auction fraud, US Federal Trade Commission, 

Bevers, B 2000, Texas hacker pleads guilty to 7 charges of unlawfully obtaining 
access to computers belonging to the United States Postal Service, the State of Texas, 
the Canadian Department of Defence and the Private Sector, press release, 6 
December 2000, United States Postal Service, United States Department of Justice 


Bibliography


Bridwell, L 2003, 8th annual computer virus prevalence survey, ICSA Labs, a Division of TrueSecure Corporation. Herndon, VA.


Broadhurst, RG 2003, ‘Summary report’ draft, 2nd Asian cyber crime summit, Hong Kong University Council Chamber, 5-6 November 2003.


Broadhurst, RG & Grabosky, P 2005, Cyber-crime the Challenge in Asia, Hong Kong University Press, Hong Kong.


BSA – See Business Software Alliance


Burgess, WE 1950, ‘Comment to Hartung’, American Journal of Sociology vol. 56.
BIBLIOGRAPHY


Carson, V 2004, ‘Selim to face criminal charges over Pan collapse’, *The Australian*,
BIBLIOGRAPHY


CCIPS – See Computer Crime and Intellectual Property Section


Clarke, F, Dean, G & Oliver, K 2003, Corporate collapse, accounting, regulatory and ethical failure, 2nd edn, Cambridge University Press, United Kingdom.


Comey, JB 2002, United States charges engineer with theft of trade secret at White Plain Software Company, United States Attorney Southern District of New York, United States Department of Justice.


Cressey, DR 1953, Other people’s money: a study in the social psychology of embezzlement, Free Press, Glencoe, Illinois.


DPP – See Director of Public Prosecutions


eBay 2004, Welcome to the feedback forum, eBay.co.uk Education Centre, pages.ebay.co.uk/services/forum/feedback.html.


EHAP – See Ethical Hackers Against Porn


Ellis, L & Walsh, A 2000, Criminology - a global perspective, Allyn and Bacon, MA, USA.


BIBLIOGRAPHY


Friedrichs, D 1996, Trusted criminals: white collar crime in contemporary society, Wadsworth, USA.

Friedrichs, D 2001, Trusted criminals: white collar crime in contemporary society, 2nd edn, Wadsworth, USA.

FTC – See Federal Trade Commission

FTC – See Federal Trade Commission


Gartner Group 2001, On-line fraud Prevention, white paper for the E-Commerce Fraud Prevention Network, March 2001,


Grabosky, P 2000b, ‘The mushrooming of cyber crime’, presentation prepared for the


Griffin, SP 2002, ‘Actors or activities? on the social construction of “white-collar
BIBLIOGRAPHY


Hansell, S 2004, ‘Organised crime may be behind phishing fraudulent e-mail scams show more sophistication’, San Francisco Chronicle, 29 March 2004.

Hardy, IR 1996, The evolution of ARPANET e-mail, http://server.berkeley.edu/virtual-berkeley/e-mail_history.


BIBLIOGRAPHY


BIBLIOGRAPHY


Hochberg, FS 1998, Former chief computer network program designer arraigned for alleged $10 million computer “bomb”, news release, United States Attorney for the District of New Jersey, United States Department of Justice.


exploitation of women and children, *Coalition Against Trafficking in Women*,
http://action.web.ca/home/catw/readingroom.shtml?x=16747

Hume, D [1737] 1975, ‘A treatise of human nature’, with comments by LA Selby-

Hunter, M 2001, ‘How to beat the net’, *Community Care*, 22-28, 12 February, in J
no.15, pp. 1-20 *National Child Protection Clearinghouse*,

Hurst, TR 2001, ‘Securities fraud and the internet: adapting existing regulatory
226-233.

crime development and practitioner report 40*, London Home Office.

IC3 – See Internet Crime Complaint Center

IFCC – See Internet Fraud Complaint Center

www.ifpi.org

IIA – See Internet Industry Association

International Telecommunications Union 2004, in ‘Internet World Stats 2004’ (eds)
*Internet Usage Statistics – The Big Picture*, Miniwatts International Inc,
http://www.internetworldstats.com/stats.htm
http://www.itu.int/home/index.html.

Internet Crime Complaint Center 2005, *IC3 2004 Internet fraud crime report, January
1, 2004 – December 31, 2004*, National White Collar Crime Center, United States of
America.

Internet Fraud Complaint Center 2001, *Internet auction fraud, May 2001*,

Internet Fraud Complaint Center 2004 *IC3 2004 Internet fraud – crime report,
Federal Bureau of Investigation, United States of America,

Internet Fraud Complaint Center 2005, *United States Department of Justice Federal
Bureau of Investigation Press Release*, Internet Fraud Complaint Center, United States
of America,
www.ifccfbi.gov/strategy/wn052301.asp.
BIBLIOGRAPHY


ITC – See International Telecommunications Union


Jensen, PR 2001, *From the wireless to the web, the evolution of telecommunications 1901-2001*, University of New South Wales Press Ltd, Australia.

Jesiek, BK 2003, ‘Democratising software: open source, the hacker ethic, and beyond’, *First Monday Peer-reviewed Journal on the Internet*, vol.8, no.10, 6 October
2003,


Jones International Ltd 2001,


Kiesler, S 1992 Address at the workshop on rights and responsibilities of participants in networked communities, Washington DC, 6 November 1992.


Klain, EJ, Davies, HJ & Hicks, MA 2001, Child pornography: the criminal-justice system response, American Bar Association Centre on Children and the Law for the National Centre for Missing & Exploited Children, United States of America.


Knott, D 2002, in Australian Securities and Investments Commission 02/452 Simon
BIBLIOGRAPHY


Krambia-Kapardis, M 2001, _Enhancing the auditor’s fraud detection ability: an interdisciplinary approach_, Peter Lang, Frankfurt.


BIBLIOGRAPHY


Lilly, JR Cullen, FT & Ball, RA 2002, Criminological theory: context and consequences, 3rd edn, Sage Publications Inc, USA.


Lombroso-Ferrero, G, Savitz, LD 1972, (eds) 'Criminal man according to the classification of Cesare Lombroso', Montclair, New Jersey, Patterson Smith, N.J.


Longshore, D 1998, 'Self-control and criminal opportunity: a prospective test of the


Luhmann, N 1979, *Trust and power*, John Wiley and Sons Ltd, Chichester.


BIBLIOGRAPHY


McNulty, PJ 2003c, news release, United States District Court for the Eastern District of Virginia, United States Department of Justice, 10 January 2003.
BIBLIOGRAPHY


NAA - See National Auctioneers Association

NAMBLA – See North American Man/Boy Love Association


BIBLIOGRAPHY

Press, United Kingdom.


Newman, GR & Clarke, RV 2003, Superhighway robbery, preventing e-commerce crime, Willan Publishing, Devon, United Kingdom.


NPA – See National Police Agency


Nua Surveys 2005, How Many Online?, Jupiter Media Corporation, United States,
www.nua.com/surveys/how_many_online/world.html.

NWCCC – See National White-Collar Crime Centre


OECD – See Organisation for Economic Co-Operation and Development

Ogilvie, E 2000a, *Stalking: Criminal Justice Responses Conference* convened by the Australian Institute of Criminology, Canberra, Australia, 7-8 December 2000.


Parker, DB 1976, Crime by computer, Charles Scribner’s Sons, New York.


PBS – See Public Broadcasting Service


PCMLP – See Programme in Comparative Media Law & Policy


Pershing, JL 2003, ‘To snitch or not to snitch? applying the concept of neutralisation techniques to the enforcement of occupational misconduct’, Sociological Perspectives, vol. 46, no. 2, pp. 149-78.


PJCACC – See Parliamentary Joint Committee on the Australian Crime Commission Inquiry into Cyber Crime
Plasmoid 1999, The hacker's choice forums, 


Power, R 2000, Tangled web, tales of digital crime from the shadows of cyberspace, Que Corporation, United States.


BIBLIOGRAPHY


PSA – See Penn, Schoen & Berland Associates Inc

PSRA – See Princeton Survey Research Associates


BIBLIOGRAPHY

Programs, United States Department of Justice.


Rustad, ML 2001, Private enforcement of cybercrime on the electronic frontier’,


Scott, C 2003, ‘Regulation in the age of governance, the rise of the post regulatory state’, Paper presented at the National Europe Centre, Australian National University, Canberra.


SEC – See Securities and Exchange Commission


Sellin, T 1938, Culture and conflict in crime, Social Science Research Council, New York.


BIBLIOGRAPHY

of Crime, Springer-Verlag, New York Inc.


Short, C & Zackheim, M 2002, Computer Technology, the Law, and Society, University of Toronto.


Simon, D & Eitzen S 1993, Elite deviance, Allyn and Bacon, Boston.


Snyder, JM 2000, ‘Online auction fraud: are the auction houses doing all they should or could to stop online fraud?’, *Federal Communications Law Journal*, vol. 52, no. 2, pp. 453-472.

Sofaer, AD & Goodman, SE 2001, *The transnational dimension of cyber crime and
terrorism, Hoover Institution Press, United States.


Stephenson, P 2003, ‘Virus writers: price on their heads’, Computer Fraud & Security,
BIBLIOGRAPHY

vol. 12, pp. 1-3.


Sutherland, EH 1939, Principles of criminology, J P Lippincott, Philadelphia.


Sutherland, EH 1947, Criminology, 4th edn, J P Lippincott, Philadelphia.

Sutherland, EH 1974, Criminology, 9th edn, J.B. Lippincott, United States.

Sutherland, EH 1983, White-collar crime the uncut version, Yale University Press, USA.


TCG – See Trusted Computing Group


UN – See United Nations


United States Department of Justice 1998, Individual pleaded guilty to causing numerous anonymous e-mail messages to be sent to a senior supervisory level employee at the Department of Defence, United States Attorney District of Virginia. United States Department of Justice, October 16 1998, www.usdoj.gov/criminal/cybercrime/ngo_pr.htm.

United States Department of Justice 2001a, Internet fraud,
BIBLIOGRAPHY


USDOJ – See United States Department of Justice


Page 328
BIBLIOGRAPHY


Westfield, M 2003, *HIH: The inside story of Australia’s biggest corporate collapse*,

Page 329
BIBLIOGRAPHY

John Wiley Sons Australia Ltd.


Wright, BRE, Caspi, A, Moffitt, TE & Silva, PA 1999, 'Low self-control, social bonds, and crime: social causation, social selection, or both?', Criminology, vol. 37,
pp. 479-514.


**Cited Cases**


*Director of Public Prosecutions (on behalf of Pena) v. Sutcliffe* Supreme Court of Victoria, Common Law Division, 6562 of 2000 BC2001000570, 1 March 2001 in RG.
Smith, P Grabosky, & G Urbas, 2004, Cyber criminals on trial, Cambridge University Press, United Kingdom.

Director of Public Prosecutions v Bignell 1998, 1 Cr.App. R. 1.


Goodwin, AT 2003, United States v. Steiger, United States 11th Circuit Court of Appeals, nos. 01-15788, 01-16100 and 01-16269.


McNulty, PJ 2003b, United States v. Mark Shumaker, Criminal No. 03-326-A. United States District Court for the Eastern District of Virginia, Alexandria Division, United States Department of Justice.

Melson, KE 2001, United States of America v. Robert Philip Hanssen, Criminal No. 01-188-A United States District Court for the Eastern District of Virginia, Alexandria Division, United States Department of Justice.

Montgomery, Alabama Police Department 2003, in AT Goodwin 2003, (ed.) United States v. Steiger, United States 11th Circuit Court of Appeals, Nos. 01-15788, 01-16100 and 01-16269.


Regina v. Bow Street Stipendiary Magistrate, Ex parte Government of the United
BIBLIOGRAPHY


SEC v. Thor Equity Group, LLC and George E. Mahfouz Jr. (Civ. No. CIV 00-1699-PHX VAM (D.Ariz)).


United States v. Bradley Joseph Steiger 318 F.3d 1039.

