Theory and Crime: Does it Compute?

Alice Hutchings

Bachelor of Arts in Criminology and Criminal Justice (Hons)

School of Criminology and Criminal Justice

Arts, Education and Law

Griffith University

Submitted in fulfilment of the requirements of the degree of Doctor of Philosophy

August 2012
Abstract

This research examines computer fraud and hacking offenders. The aim of this study is to provide a comprehensive understanding of computer crimes that compromise data and financial security, particularly hacking and computer frauds. This understanding will allow us to organise what we know about computer crime, so that it can be understood and explained.

Computer crime was identified as an area that required further research, particularly in relation to offenders, which are a hard to access population. Particularly, it was noted that it is not understood why people became involved in computer crime offending. There has been a lack of theoretical examination in relation to these types of offenders. The theories that are applied in this research include differential association, social control theory, techniques of neutralisation, rational choice theory, labelling theory and structural strain theory, as well as feminist critiques of criminology. This was identified as an important area for research as there are many problems with the current crime prevention approaches and in investigating these offences.

Three qualitative studies were undertaken to address and provide an in-depth view of this problem. The first study involved an analysis of court documents for matters that had gone before the judiciary, while the second consisted of interviewing law enforcement officers who investigated these types of offenders. The third study involved interviewing active and former offenders, who were identified using snowball sampling techniques.
As was expected, it was found that males predominantly engage in computer crime. When females are involved, they are more likely to conduct fraud rather than hacking. A number of differences were found between offenders who only engaged in hacking and those that participated in computer fraud. Overall, hackers came from more privileged backgrounds, were more financially well off, were generally younger, had closer relationships to their parents, were better educated and were less likely to have prior engagement with the criminal justice system. Fraud was found to be predominantly motivated by financial gain, however the motivating factors for hacking were more disparate, including fun and excitement, revenge, to test skills and for a challenge.

The online environment was found to offer a number of enabling factors leading to offending. For example, offenders were physically removed from their victims, alleviating feelings of guilt. Online communities allow participants to stay anonymous while communicating, learning and sharing information. Offenders were able to cross jurisdictions using the internet, which is problematic for police investigations and therefore lessens the likelihood of detection. The online environment also offers a variety of ways for offenders to anonymise their attacks.

This thesis, informed by the research findings, proposes an integrated theory of computer crime offending. According to this theory there are two distinct pathways leading to offending, namely presented opportunity and associating with others. These pathways reflect the type of offending that occurs, with sole offenders, typically fraudsters, taking advantage of the presented opportunities when they have undergone some type of strain, usually economic.
Offender maintenance and desistence follow similar trajectories for both of the offence types. The integrated theory proposes that behaviour is maintained due to a low likelihood of detection, as well as the benefits available to offenders. Desistence occurred when offenders no longer receive benefits from offending or when the costs outweighed the benefits. These trajectories reflect rational choice theory.

The implications for this research include recommendations for the detection and prevention of these types of offences. Recommendations include providing legitimate opportunities for those who are likely to be motivated by curiosity and skill testing, targeting potential offenders early, when they first become involved in online communities and gaming, implementing mandatory breach reporting in Australia, providing greater resources for the investigation and prosecution of computer crime offences, implementing a national computer crime reporting system, and informing businesses about how they can reduce opportunities for crime.
Statement of Originality

This work has not previously been submitted for a degree or diploma in any university. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

______________________________

Alice Hutchings
Acknowledgements

Dear thesis,

This must be the hardest letter I’ve ever had to write. After four years together I’m breaking up with you. We’ve been through both high and low times together. Along the way we have shared a lot of love and a lot of hatred, many late nights fuelled with coffee, as well as much tears and laughter. However, it is over between us, I need to move on. I will always think of you fondly.

Sincerely, it is me, not you. I hope you understand.

It is a pleasure to thank those who made this thesis possible. I am indebted to my supervisory team, Dr Hennessey Hayes, Associate Professor Janet Ransley, Professor Simon Bronitt and Professor Peter Grabosky. Despite their hectic schedules they were always available when required with wise words and provided me with feedback and direction.

My deepest gratitude goes to all those who participated in this research and who gave up their time to talk to me, and in a way shared their lives with me. Your openness, honesty and trust were much appreciated and it is you who enabled this research to happen. I would also like to acknowledge the staff at the policing agencies who assisted me with my research applications.
I also thank the staff that provided me with support during my candidature, particularly Celia Dickson from the School of Criminology and Criminal Justice, and Melanie Davies, Kylie Baker and Joyce Wang from the ARC Centre of Excellence in Policing and Security (CEPS). Particular recognition goes to CEPS Police Fellow Inspector Jason Saunders, who provided me with invaluable assistance. Thank you to Paulina Piira from RegNet who assisted me while I was visiting the Australian National University to undertake data collection. I would also like to acknowledge the staff at the Australian Institute of Criminology for their support in finalising this thesis.

The PhD process is a journey that cannot be undertaken without support and friendships. To those that provided me with distraction and injected laughter and humour into my life I give my deepest thanks and gratitude. Too numerous to name, they know who they are. Most will probably only read up to here, if at all, to see if they have been mentioned; so sorry to disappoint.
Table of Contents

Chapter 1 ~ Introduction 1

Overview of research questions and design 4

Aim 5

Scope 6

Overview of the research 7

Chapter 2 ~ Computer Crime 8

Typologies of computer crime 8

White collar crime 9

Computer crimes that compromise financial security 10

Computer crimes that compromise data security 16

Organised crime 21

Cyberterrorism and cyberwarfare 23

Criminology and computer crime 24

Computer crime and the law in Australia 26
<table>
<thead>
<tr>
<th>Chapter 3 ~ Theory and Crime</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theory selection</td>
<td>53</td>
</tr>
<tr>
<td>Sutherland’s theory of differential association</td>
<td>56</td>
</tr>
<tr>
<td>Hirschi’s social control theory</td>
<td>61</td>
</tr>
<tr>
<td>Sykes and Matza’s theory of techniques of neutralisation</td>
<td>64</td>
</tr>
<tr>
<td>Clarke and Cornish’s rational choice theory</td>
<td>69</td>
</tr>
<tr>
<td>Becker’s labelling theory</td>
<td>72</td>
</tr>
<tr>
<td>Merton’s structural strain theory</td>
<td>76</td>
</tr>
<tr>
<td>Feminist critiques of criminology</td>
<td>79</td>
</tr>
<tr>
<td>Theory and practice: Implications for crime prevention</td>
<td>83</td>
</tr>
<tr>
<td>Conclusion</td>
<td>87</td>
</tr>
</tbody>
</table>
## Table of Contents

### Chapter 4 ~ Research Questions and Design

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research questions</td>
<td>89</td>
</tr>
<tr>
<td>Research design</td>
<td>90</td>
</tr>
<tr>
<td>Study one: Analysis of court documents</td>
<td>91</td>
</tr>
<tr>
<td>Study two: Interviews with law enforcement officers</td>
<td>93</td>
</tr>
<tr>
<td>Study three: Interviews with active and former offenders</td>
<td>95</td>
</tr>
<tr>
<td>Ethical considerations</td>
<td>97</td>
</tr>
<tr>
<td>Analyses</td>
<td>99</td>
</tr>
<tr>
<td>Reliability, validity and reflexivity</td>
<td>100</td>
</tr>
<tr>
<td>Limitations of the research design</td>
<td>102</td>
</tr>
<tr>
<td>Development of a new theoretical model of computer crime</td>
<td>103</td>
</tr>
</tbody>
</table>

### Chapter 5 ~ Demographics

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>106</td>
</tr>
<tr>
<td>Age</td>
<td>112</td>
</tr>
<tr>
<td>Social economic status</td>
<td>115</td>
</tr>
<tr>
<td>Country of origin</td>
<td>116</td>
</tr>
<tr>
<td>Conclusion</td>
<td>118</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>Motivations and Rationalisations</td>
</tr>
<tr>
<td></td>
<td>Motivations</td>
</tr>
<tr>
<td></td>
<td>Neutralisations</td>
</tr>
<tr>
<td></td>
<td>Target selection</td>
</tr>
<tr>
<td></td>
<td>Moral beliefs</td>
</tr>
<tr>
<td></td>
<td>Self-perception</td>
</tr>
<tr>
<td></td>
<td>Conclusion</td>
</tr>
<tr>
<td>7</td>
<td>Friendships and Families</td>
</tr>
<tr>
<td></td>
<td>Family backgrounds</td>
</tr>
<tr>
<td></td>
<td>Intimate relationships</td>
</tr>
<tr>
<td></td>
<td>Social life</td>
</tr>
<tr>
<td></td>
<td>Social organisation and co-offending</td>
</tr>
<tr>
<td></td>
<td>Conclusion</td>
</tr>
<tr>
<td>8</td>
<td>Work and Play</td>
</tr>
<tr>
<td></td>
<td>Education</td>
</tr>
<tr>
<td></td>
<td>Employment</td>
</tr>
<tr>
<td>Chapter Title</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Skills</td>
<td>168</td>
</tr>
<tr>
<td>Recreational activities</td>
<td>173</td>
</tr>
<tr>
<td>Conclusion</td>
<td>175</td>
</tr>
<tr>
<td>Chapter 9 ~ Life Events</td>
<td>177</td>
</tr>
<tr>
<td>Prior criminal history</td>
<td>177</td>
</tr>
<tr>
<td>Physical and mental health</td>
<td>182</td>
</tr>
<tr>
<td>Drugs, gambling and other addictions</td>
<td>185</td>
</tr>
<tr>
<td>Financial issues</td>
<td>188</td>
</tr>
<tr>
<td>Conclusion</td>
<td>190</td>
</tr>
<tr>
<td>Chapter 10 ~ Apprehension and Punishment</td>
<td>192</td>
</tr>
<tr>
<td>Views about detection</td>
<td>192</td>
</tr>
<tr>
<td>Views about punishment</td>
<td>197</td>
</tr>
<tr>
<td>Attitude towards law enforcement</td>
<td>200</td>
</tr>
<tr>
<td>Conclusion</td>
<td>202</td>
</tr>
</tbody>
</table>
# Table of Contents

Chapter 11 ~ Synthesis 203

- How well do existing theories of criminal behaviour account for computer crime? 204
- Is a new theoretical model needed to better explain computer crime? 213
- What should an integrated model look like? 213
- Recommendations for the detection and prevention of computer crime 218
- Future research 221

Appendix A ~ Australian State, Territory and Commonwealth Unauthorised Access-Related Offences 223

Appendix B ~ Australian State, Territory and Commonwealth Data-Related Offences 226

Appendix C ~ Australian State, Territory and Commonwealth Fraud-Related Offences 231

Appendix D ~ Australian State, Territory and Commonwealth Identity-Related Offences 235

Appendix E ~ Study Two Interview Schedule 238

Appendix F ~ Study Three Interview Schedule 245
Appendix G ~ Codebook  255

References  263
Tables

Table 1:

Sentences Imposed in Fraud/Theft, Hacking, and Unlawful Access/Modification ................................................................. 33

Cost of Fraud and Computer Security Incidents in Australia (AUD$) .............. 41

Summary of the Theories and their Key Constructs ........................................................ 87

Number of Cases in Study One by Type and Jurisdiction ................................. 92

Gender of Study One Participants by Offence Type ........................................ 107

Motivations and Rationalisations Reported in the Literature .......................... 121

Educational Levels, Where Known ................................................................. 160

Figures

Figure 1. Initiation, maintenance and desistence ........................................ 216
Chapter 1 ~ Introduction

This research examines offenders who commit computer crimes that compromise financial and data security, such as hacking and computer fraud. Hacking, for the purpose of this research, is defined as unauthorised access to a computer system, regardless of the motive, or misuse of legitimate access to a computer system. Computer frauds refer to the use of information and communication technology to manipulate others into providing money or identity information. There is a relationship between the two offence types considered in this study as hacking may facilitate fraud.

There is considerable literature relating to the appropriateness of various popular synonyms such as computer crime, cyber crime, cybercrime, e-crime, internet-related crime, electronic crime, online crime, virtual crime, digital crime, high tech crime, computer related crime, etc. For an overview of this debate see Smith, Grabosky and Urbas (2004). Smith et al. (2004), who insist on the use of “cyber crime” (with a space between cyber and crime) still interchange this term with “computer crime” within their book (see, for example, pp. 28 & 32). The use of “computer crime” within this thesis reflects personal preference, acknowledging that the offenders and victims are occupied in physical space. This removes the mystical aspect of a separate dimension called “cyberspace” and grounds the real life actions and subsequent consequences.
Computer crimes affect the public greatly, including the direct cost of victimisation as well as associated costs related to businesses recovering their financial loss (for example, banks passing on higher fees). As many as 95 per cent of computer crimes are not reported to authorities (Yar, 2006) and there appears to be little consistency in the way the financial cost is calculated. Estimates of losses by the Australian Competition and Consumer Commission have been as high as AUD$1 billion in Australia in the year 2008 due to advance fee fraud alone (Richmond, 2008). Rollings (2008) provides comparable cost-of-crime data for a range of offences within Australia. Whilst not including computer crimes as a specific category, it was identified that fraud-related offences accounted for the highest financial loss, costing AUD$8.5 billion in 2005, higher than burglary (AUD$2.2 billion), drug offences (AUD$1.8 billion) and arson (AUD$1.6 billion).

Of the small percentage of computer crimes that are reported, less than 20 per cent are likely to result in criminal charges (AusCERT, 2006). Whilst under-reporting and under-prosecution may be typical of most crime types, computer crimes are notoriously difficult to bring to prosecution, with problems including inadequate legislation, lack of evidence, and jurisdictional difficulties (AusCERT, 2006; Smith, 2001). These difficulties may create a limited law enforcement approach that has little deterrent effect and leads to a lack of confidence in law enforcement to adequately deal with this problem (Kshetri, 2006). As we do not currently understand offenders we cannot appropriately prevent, respond to, and control this type of crime.
Much of the previous empirical research into online hacking and fraud offences has been done without a theoretical framework (McQuade, 2006), focusing instead on descriptions of the tools and techniques used by offenders and the impact on society and victims. Some exceptions are the works of McQuade (2006), Walkley (2005) and Turgeman-Goldschmidt (2009). McQuade (2006) and Walkley (2005) both discussed how a number of criminological theories may explain computer crimes but did not conduct empirical tests of these theories. In fact, McQuade (2006, p. 141) stated that “… there has been extremely little empirical testing of established theories to explain in explicit terms why cybercrimes occur”. Turgeman-Goldschmidt (2009) interviewed Israeli hackers, identifying while doing so their use of techniques of neutralisation. Interestingly, Turgeman-Goldschmidt (2009) and Walkley (2005) came to quite different conclusions about the applicability of some of Sykes and Matza’s (1957) proposed neutralisations. For example, Turgeman-Goldschmidt (2009) found no evidence that offenders engage in denial of responsibility, which was the technique of neutralisation that Walkley (2005) argued had the greatest support. Pontell (2002, p. 319) has called for more “explanation and theory testing and ethnographic and descriptive study” into these types of crime in order to strengthen criminology as a discipline, particularly in its understanding of emerging deviant and criminal behaviours.

In addition, some of the prior research that have looked into the hacking subculture date from the late 1980’s and mid-1990’s, when the Internet was not as omnipresent in our lives as it is today (especially in disadvantaged homes) (Chantler, 1995; Meyer, 1989; Parker, 1998). The context today is
fundamentally different in terms of technology availability, as well as the opportunities for offending. Now, when personal computers are readily available in workplaces and homes, when information is increasingly digital and easily accessible almost instantaneously, and computing devices are increasingly mobile, there is a need for greater empirical attention to these matters.

The lack of understanding about these types of offenders and the crimes that they commit has resulted in a response that is predominantly reactive in nature. While in Australia there is a proactive annual awareness campaign aimed at increasing potential fraud victims’ vigilance, little, if anything, has been attempted to deter potential offenders from unauthorised access and computer fraud (Broadhurst, 2006). This places the onus on victims to protect themselves, which is problematic as we have seen fraudsters use a variety of ever-changing tactics to entice their victims. Additionally, while increasing the awareness of internet users may encourage some to avoid scams, the low operating cost of computer fraud allows the offender to target mass numbers of potential victims. Therefore, offenders may displace to other, more vulnerable, targets (Smith, Wolanin, & Worthington, 2003).

**Overview of research questions and design**

The questions addressed in this thesis are:

1. How well do existing theories of criminal behaviour account for computer crime?;
2. Is a new theoretical model needed to better explain computer crime?; and

3. What should an integrated model look like?

To address these research questions, three qualitative studies were undertaken. The first study analysed court documents relating to computer fraud and hacking offences, the second consisted of interviews with law enforcement officers who have investigated these types of offenders, and the third involved interviews with active and former offenders. The research questions, and the methods used in the three studies, are addressed in further detail in Chapter 4.

Aim

The principal aim of this research is to develop a theoretical understanding of computer crimes that compromise data and financial security, including offender initiation, maintenance and desistance. This has been achieved by critically assessing a range of criminological theories with a view to establishing a new theoretical model of computer crime. The theories that have been assessed in this research include differential association, social control theory, techniques of neutralisation, rational choice theory, labelling theory and structural strain theory, as well as feminist critiques of criminology.

A greater understanding about offenders would allow a more appropriate response to these types of crimes with proactive offender-oriented methods. This research attempts to overcome this gap in the literature by developing a comprehensive understanding of these offenders and crime types, which will,
ultimately, identify ways in which unauthorised access and computer frauds can be prevented. This research will help develop a more effective and appropriate government and law enforcement approach that facilitates the most suitable use of powers and resources.

By determining whether existing theories of crime adequately explain computer crime, this study will also be useful in addressing current debates within the field of criminology, such as whether computer crimes are a new type of crime, or, as proposed by Grabosky (2001), whether they represent “old wine in new bottles” (p. 243). Finally, this study aims to add to the literature that supports, or fails to supports, these theories. According to Mazerolle (2009), theories of crime should be subjected to rigorous scientific research to determine if they provide an adequate explanation of criminal behaviour across time and location. This study aims to identify the strengths and weaknesses with applying the theories to criminal behaviours that occur predominantly in cyber, rather than terrestrial, space.

Scope

Many theories have been carefully considered to determine whether they should be included in this evaluation. Criteria for inclusion in this research included whether the theory could be tested within the resources available to the research project. Therefore, some potentially interesting theories have been excluded to ensure that the research project can be kept to a manageable size. One such theory, which has often been discussed in relation to computer crime, is Cohen and Felson’s (1979) routine activity approach, which examines
how people's everyday activities place them at risk of victimisation. Sociological theories have been favoured over biological and psychological theories as, in the discipline of criminology, they have fared better when faced with rigorous empirical testing (Akers & Sellers, 2004).

**Overview of the research**

The following chapter discusses computer crimes, setting out what is already known about offenders. Chapter 3 provides an overview of the theories that will be examined in this research, including how they might apply to computer crime. Chapter 4 sets out the key research questions to be addressed and provides the details of the research design for answering these questions. Chapters 5 through 10 set out the research findings and apply these to the theoretical explanations. These chapters focus on offenders’ demographics, motivations and rationalisations, relationships with friends and families, work, education and recreational activities and views about detection and punishment. Conclusively, Chapter 11 sets out an integrated theoretical model of computer crime offending and provides recommendations for the detection and prevention of computer crime.
Chapter 2 ~ Computer Crime

It was suggested in Chapter 1 that computer crime was an important area for further research. The aim of this chapter is to provide support to justify the value of this research. This chapter describes what is known about computer crimes that compromise data and financial security. It firstly provides an overview of computer frauds and hacking offence typologies. This chapter then discusses why further research in this area is required before outlining the current legislative framework for dealing with these types of offences in Australia. Crime prevention techniques that are currently used to thwart computer crimes and the strengths and limitations of these approaches are discussed. This chapter also provides information about the estimated costs of these crimes, raising questions about how these costs are estimated and whether they are reflective of the true financial burden faced by victims.

Typologies of computer crime

Crime has been categorised in many different ways. One such typology is the differentiation between crimes against the person or property crimes. This categorisation can be carried across into computer crime classifications (Parker, 1998). The focus of this research are computer crimes that compromise intangible property, namely data and finances. These types of crimes include computer frauds and hacking. In contrast, manifestations of personal crimes on the internet include cyber grooming and cyber stalking.
Computer crimes have also been defined along two dimensions, namely “computer-assisted” crimes, whereby traditional offences have been moved from terrestrial to cyber space, and “computer-focussed” crimes, which are crimes that are wholly enabled by the internet and could not occur without it (Yar, 2006, p. 10). Yar (2005b) states that computer crimes are a “...new and distinctive form of crime” (p. 407), primarily due to the difference in where they are committed. “Real virtuality” (Yar, 2005b, p. 416) provides greater efficiency, more opportunities, increased anonymity for offenders, and extended geographical reach, so that targets or victims can coexist within different boundaries. However, Grabosky (2001), using the term “old wine in new bottles” (p. 243), argues that computer crimes are not fundamentally different from other terrestrial crimes, except that they use a different medium. Not only is the act of computer crime, such as fraud or unauthorised access, similar to terrestrial crime, but the motivations of “greed, lust, power, revenge, adventure, and the desire to taste “forbidden fruit” (Grabosky, 2001, pp. 243-244) are common across all crimes, including computer crime.

White collar crime

Early research into computer crimes classified them as a form of white collar crime, most likely because computers were mainly only available in the workplace (Chan, 2003). White collar crime has been defined as “a crime committed by a person of respectability and high social status in the course of his occupation” (Sutherland, 1949, p. 7). Nowadays, the issue as to whether computer crimes are white collar crimes can be contentious. Sutherland, who coined the term, specifically excluded from his definition of white collar crime
“confidence games of wealthy members of the underworld” (Sutherland, 1949, p. 7) as offenders did not hold a high social status. Since then, the definition of white collar crime has expanded considerably, with Friedrichs (2007) defining some types of “technocrime” (p. 7) as a marginal form of white collar crime, and Rosoff, Pontell and Tilman (2004) referring to hacking offences committed by juveniles as “white collar delinquency” (p. 488).

On the other hand, Chan (2003) asserts that not all computer crimes can be classified as white collar crimes, particularly hacking offences. In the 1980s computers became more widely available to the general public. This raises the question as to whether computer crime is a component of white collar crime; or conversely, whether the increasing use of computers in the workplace means that we should rethink this taxonomy and classify white collar crime as an element of computer crime. The increasing prevalence of digital technology means more white collar crime is likely to involve computers (Smith & Jorna, 2011). Although there is a considerable overlap with white collar crime, there has been a recent shift away from this typology, with Jaishankar (2011, p. xxvii) even proposing that computer crimes should be included under a new discipline called “cyber criminology”.

Computer crimes that compromise financial security

Fraud can be broadly defined as “an intentional dishonest act or omission done with the purpose of deceiving” (Nygh & Butt, 1998, p. 186). Developments in technology have created more opportunities for frauds that compromise financial security to take place. For example, Smith (2010) describes how the
development of the telephone in 1877 paved the way for phreaking\(^1\) in 1961 and telemarketing scams, first identified in 1965. ATMs were introduced in 1965, and the first ATM fraud was identified in 1985, while the introduction of the World Wide Web in 1991 led to the first instances of spam and online identity crime in 1995 (Smith, 2010).

Computer fraud conducted in the workplace may include, for example, altering computer data to divert funds for personal use or manipulating financial records to hide unauthorised transactions. Computer fraud conducted online uses a variety of media, including email, social networking sites, such as chat or dating websites, and online trading sites, such as eBay (Brenner, 2007; Finch, 2007), to manipulate others into providing money or identity details.

Identity theft refers to stealing another's identity, while identity fraud refers to the use of another's real or a fictitious identity for an unlawful purpose (Australasian Centre for Policing Research, 2004). The internet allows the offender to not only glean enough information about a victim's identity, but also provides a forum for the subsequent use of that identity, such as using another's credit card, incurring debt in their name, or obtaining a passport (Finch, 2007). The theft of an identity may also occur during the commission of another online scam, such as phishing. Identity fraud illustrates how multiple victims may be involved in scams. For example, victims may include the individual whose

\(^1\) Phone phreaking refers to hacking into telecommunication systems (Grabosky, Smith, & Dempsey, 2001).
identity has been stolen and the financial institution, government agency or service provider that has been duped.

Card-not-present payment frauds involve the purchase of goods over the internet or telephone using credit card details obtained by identity fraud, accessing another's account details, or using counterfeit or cloned cards (Wall, 2007). Often the fraudulent use of credit cards is separated from the theft of the credit card information, so multiple offenders may be involved in the commission of the offence. For example, compromised credit card details are frequently offered for sale on online hacking sites (Australian Institute of Criminology, 2006; Glenny, 2011; Holt & Lampke, 2010).

Investment fraud, involving the trading of stocks and shares, was enabled with the use of computers when the NASDAQ began trading as the first electronic stock market in 1971 (Stoll, 2006). Investment fraud may take a variety of forms, including the sale of shares for non-existent companies, misrepresentation of the worth of shares, market manipulation, and insider trading (Grabosky et al., 2001). Market manipulation includes “pump-and-dump” (Grabosky et al., 2001, p. 84) schemes, whereby stock prices are artificially inflated by rumour mongering on the part of the offender, who reaps a profit while the victims sell at deflated prices. The opposite is known as “slur and slurp” (Grabosky et al., 2001, p. 84), whereby prices are lowered so that the offender can buy at a bargain price.

Advance fee frauds, also known as Nigerian frauds or 419 scams, have existed in a number of forms since “the Spanish Prisoner” scam, which dates back to the sixteenth century (Yar, 2006). Advance fee fraud often involves the
offender asking the victim to participate in some sort of questionable activity in return for a financial benefit, therefore reducing the probability that the victim will involve the authorities once they realise they have been defrauded (Smith, Holmes, & Kaufmann, 1999). Victims may also be unwilling to report losses due to embarrassment or fear of reprisal (Smith et al., 1999). Advance fee fraud may take a number of forms, including telling the victim that if they provide financial assistance to rescue a person held captive they will receive a share of great wealth that is in this person’s possession. In another variation the victim is told that a large amount of money is held in an overseas bank but cannot be accessed. In return for providing financial assistance to extract the money from the country the victim is promised a share. Multiple fraudsters may be involved in the scam, for example, claiming to be bank managers, lawyers, and even law enforcement officers (Ross & Smith, 2011). Although advance fee frauds occur across the world, there have been a large number of such frauds originating from Nigeria or involving Nigerian nationals living abroad, which has resulted in the term Nigerian fraud or 419 fraud (419 referred to the previous section of the Nigerian Criminal Code which prohibited such activity) (Smith et al., 1999). Perpetrators may also be involved in other illegal activities, such as identity, immigration and credit card fraud (Smith et al., 1999). The commission of advance fee frauds moved from mail and facsimile to email with the growth of the internet (Yar, 2006).

Romance scams are another form of advance fee fraud and are usually conducted using online dating and social networking sites. Internet dating sites first appeared in 1993, and social networking sites in 1997 (Boyd & Ellison,
2007). Offenders strike up relationships with potential victims before requesting money, allegedly to cover the cost of flights or medical expenses (Wall, 2007). The period of “grooming” may take several months and the victim is lulled into a false sense of security. Reports have emerged that often victims do not want to recognise that they have been victimised and that the relationship is not real, thus allowing the offender to request more and more money (Edwards, 2008). In some cases offenders have reportedly convinced victims to participate in illegal activities in order to obtain money, such as money laundering, credit card fraud or trafficking drugs (Edwards, 2008).

Online auction sites, such as eBay, founded in 1995 (eBay, 2012), provide opportunities for internet auction fraud. Frauds that are committed on these sites include the sale of stolen or counterfeit goods; not delivering items; misrepresentation of products; shill bidding, where the price is artificially inflated due to false bids; and fee stacking, whereby additional fees are added on after the auction (Yar, 2006). Internet auction frauds can also be conducted by the bidder, for example, the successful bidder may overpay with a counterfeit cheque, so that the bidder receives the goods at no cost, as well as a refund on the overpaid amount (Wall, 2007).

Phishing, first identified in 2002 (Smith, 2010), targets the account holders of banks, financial institutions, online commerce sites such as eBay and government agencies such as the Australian Tax Office. Phishing involves a fraudulent email sent to the account holder advising that there is a problem with their account, or that their account details need to be verified, purportedly from the bank or other commerce site. Victims are provided with a link directing them
to a “spoofed”, or fake, website where they are asked to provide their account
details, passwords and possibly other personal information, such as date of birth.
Offenders can then use this information to obtain funds from the victims’
accounts, or commit other forms of identity fraud using the victims’ personal
information (Yar, 2006).

Spear phishing is conducted with the aim of gaining access to the
business’s computer system. Spear phishing differs from phishing in that rather
than targeting a large number of prospective victims, a specific business owner
or a business’s employees are selected. The attack is tailored to enhance its
perceived legitimacy, such as appearing to come from a service provider that the
business deals with. Further, as spear phishing emails are directed towards a
small number of individuals rather than many recipients, they may be less likely
to be detected and blocked by email filters (Sheng, 2009).

Duffield and Grabosky (2001) have compared the psychological correlates
of the motivated offenders (one of the components of the routine activity
approach) of fraud, depending on the context in which it occurs and the nature of
the relationship between the offender and the victim. Under their typologies,
many computer frauds would be classified as “fraud committed against a number
of individuals through print or electronic media... pitched at a relatively large
number of prospective victims” (Duffield & Grabosky, 2001, p. 1). Duffield and
Grabosky (2001) describe the motivational elements common to all types of fraud
to be financial strain, power over people, and the gratification obtained from
mastery of a situation. Additionally, offenders may justify or rationalise their
actions (Duffield & Grabosky, 2001). For example, rationalisation by an offender
may incorporate the fact that the victim may be entitled to a refund from their financial institution (who can afford it), trivialising the crime (as they are only obtaining a little from a lot of people), and inferring that it has been decriminalised (as it is not pursued by law enforcers). Duffield and Grabosky (2001) also claim that each of their fraud typologies have unique correlating psychological factors. In the case of computer frauds, which use an indirect means to access potential victims, social cues are removed, leading “to a reduction in the influence of social norms and constraints on the average person’s behaviour” (Duffield & Grabosky, 2001, p. 5).

**Computer crimes that compromise data security**

Some of the activities pursued by computer enthusiasts have been labelled as criminal. One example is “hacking”, an umbrella term which, these days, encompasses a variety of pursuits that compromise computer security. Both hacking and cracking refer to gaining unauthorised access to a computer system. The distinction between the terms is that “cracking” is sometimes used to refer to having another criminal motive once access has been gained (Brenner, 2007; Wall, 2007), for example, obtaining confidential information, including credit card details, or “defacing” websites. Here, the term cracking is not to be confused with software cracking, which refers to the removal of copyright protection from commercially available software to enable it to be copied and installed without authorisation (“pirated”) (Goode & Cruise, 2006). For the purpose of this research hacking is also used to describe activities whereby the offender does have legitimate access to a computer system, such
as in a workplace, but uses it in a way that is unauthorised, sometimes referred to as insider abuse of access.

Instances of unauthorised access that are targeted towards particular organisations or governments, are highly technical, and are particularly clandestine in nature so as to continue undetected for a period of time, usually to conduct espionage, are referred to as advanced persistent threats (Thomson, 2011). Hackers may use a variety of technical means to gain unauthorised access to a computer system. These include exploiting software weaknesses and vulnerabilities, malware infection, such as keylogging programs, session hijacking, man-in-the-middle attacks, and obtaining passwords through the use of phishing and spear phishing. Keylogging programs record users’ keystrokes, including passwords and account names (McQuade, 2006). Keylogging programs may be disguised as legitimate software, such as a game, known as a trojan. Trojans are named after the gift offered to the city of Troy that allowed the Greeks to enter surreptitiously (Grabosky, 2007a).

Hacking tools can be used to detect vulnerabilities and automate exploits. Examples include vulnerability scanners, remote administration programs, port scanners, sniffers and password crackers (Furnell, 2002). Some tools are freely available to be downloaded online, while others can be purchased from web forums (Chu, Holt, & Ahn, 2010; Motoyama, McCoy, Levchenko, Savage, & Voelker, 2011). “Script kiddie” is a term used to refer to someone that use others’ programs in order to hack rather than developing their own (McQuade, 2006).
Session hijacking refers to exploiting a valid computer session. An example involves the use of wireless internet connections, whereby users are at risk of having their accounts accessible to other network users without their knowledge. This occurs when the cookies, used to authenticate the user, sent by an unencrypted website are intercepted and used to impersonate the account holder (Dacosta, Chakradeo, Ahamad, & Traynor, 2011). Session hijacking can also be conducted using a man-in-the-middle attack. In this context a proxy intercepts traffic between a website and the browser. This occurs when the browser believes that the proxy is the legitimate website and the website authenticates the proxy as the browser (Knights et al. 2006). The proxy can then read and alter the data being transmitted, including account passwords.

Insider abuse of access occurs when an employee or contractor abuses the trust placed in them (Shaw, Ruby, & Post, 1998). Employees have knowledge of a business’s computer systems and, while they may have legitimate access to those systems, there is the potential for unauthorised use. Businesses that are slow in restricting access after terminating someone’s employment may find that their systems have been sabotaged.

In addition to technical methods, hackers may also engage social engineering techniques to obtain passwords and unauthorised access to computer systems. While there does not seem to be a set definition of social engineering most definitions agree with that of Mitnick and Simon (2002, p. iv) in that:

*Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to*
take advantage of people to obtain information with or without the use of technology (p. iv).

However, definitions of social engineering may differ. For example, Wall’s (2007) definition is restricted to information sought from staff within organisations for the purpose of gaining access to secure systems. On the other hand, Smith’s (2007) definition is restricted to instances where the victim believes that the information is required for a legitimate purpose, which may exclude some situations where offenders manipulate victims to disclose information without informing the victims that the information is required for a specific reason, or by someone in authority.

Hacking also facilitates fraud. For example, hacked webservers may result in compromised credit card details. Web forums provide a marketplace for malware (malicious software) and stolen data, as well as services such as the distribution of spam, web hosting and proxy services which may be used for fraudulent purposes (Chu et al., 2010; Franklin, Paxson, Perrig, & Savage, 2007; Holt & Lampke, 2010; Motoyama et al., 2011). Similarly, hacked emails or social media profiles may be used to disseminate spam spruiking fraudulent pharmaceuticals or other products and for the purposes of advance fee fraud.

Hackers are often differentiated by bestowing them with metaphoric hats depending on their motivations. Traditionally these include malicious “black hat” and ethical “white hat” hackers (Furnell, 2010; Thomas, 2005). However this terminology has also been extended to include “grey hat” hackers (who expose security flaws to both those who can fix the flaws and those who exploit them)
and “blue hat” hackers (who hack for organisations such as Microsoft to identify potential flaws) (Erickson & Howard, 2007).

Many publications relating to hacking mention the following “hacker ethics” as recorded by Levy (1984):

- **Access to computers – and everything which might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative!** (p. 27).
- **All information should be free** (p. 27).
- **Mistrust Authority – Promote Decentralization** (p. 28).
- **Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position** (p. 30).
- **You can create art and beauty on a computer** (p. 30).
- **Computers can change your life for the better** (p. 33).

It may be argued that these authors, however, misrepresent Levy (1984), as he was not referring to hackers who were involved in illegal activities (Furnell, 2002). Instead, Levy (1984) was using the previous meaning of the term hackers, those who “…guide[ed] computers to greater heights than anyone expected” (p. 36). The hacker ethic described by Levy was purportedly developed by a group of programmers in the 1950s, before modems were developed and when programs ran using punch cards.² Therefore, these hacker ethics should be considered in historical context. For example, the principle “all information should be free” referred to “a free exchange of information” (Levy, 1984).

---

² Punch cards were pieces of manila cardboard with holes punched in them which represented instructions to the computer (Levy, 1984).
1984, p. 27), such as sharing computer programs, rather than accessing another computer system illegally. Similarly, the authorities that were to be mistrusted were not necessarily law enforcement agencies, but rather “bureaucracies, whether corporate, government, or university” (Levy, 1984), as they limited the free exchange of information.

Organised crime

According to the United Nations Convention Against Transnational Organised Crime, the definition of an “organised criminal group” is a group of three or more persons that has been formed for a period of time with the aim of committing a serious criminal offence for a financial or material benefit (United Nations Office on Drugs and Crime, 2004). Research evidence indicates that hackers do work together to some extent (Chantler, 1995), or to collaborate on how to commit offences (Meyer, 1989), both on- and offline (Holt, 2007). Jordan and Taylor (1998) suggest that the hacker community is characterised by a fluid, informal and loosely structured membership, with a high turnover.

Organised crime syndicates also reportedly recruit hackers for their technical skills (Australian Institute of Criminology, 2006; Choo, 2008; Parker, 1998), which may be applied to extortion and espionage, as well as conducting computer frauds. Organised crime involving hackers is reportedly most common in Russia, Romania and the Ukraine (Australian Institute of Criminology, 2005b), however online activities allows syndicates to operate internationally (Choo, 2008). Choo (2008) differentiates between organised crime groups that engage in computer crime to facilitate their traditional activities; those that operate solely
in the online environment; and “organised groups of ideologically and politically motivated individuals” (Choo, 2008, p. 271) who use computer crime to facilitate criminal conduct. Organised crime groups that operate online only, or “organised cybercrime groups” (Choo, 2008, p. 276) are usually less structured, smaller, more likely to operate across borders, and are less hierarchical than traditional syndicates (Choo, 2008). The Australian Crime Commission (2011) includes the use of new technologies and specialists, as well as involvement in financial crimes such as fraud, in their definition of high-threat organised crime groups. The use of new technologies is also listed as a future threat from organised crime organisations (Australian Crime Commission, 2011).

Activities that traditional organised crime groups are reportedly involved in include narcotics and human trafficking, nuclear smuggling, extortion, prostitution, illegal bookmaking, unlicensed money lending, identity crimes, frauds and scams, money laundering, extortion, selling counterfeit drugs, software piracy and credit card fraud (Choo, 2008). Many of these offences can easily be carried over to the cyber domain, presumably quite successfully for the criminal enterprise. For example, extortion of gambling and pornography sites has reportedly been conducted by threatening distributed denial of service\textsuperscript{3} attacks (Choo, 2008), while scams such as phishing attacks can reach a wide audience for little cost (Grabosky, 2007b). However, it is unclear to what extent such activities are attributable to organised crime syndicates, sole operators, or

\textsuperscript{3} Denial of Service, or DoS, attacks, involve overloading a website or computer system so that legitimate access is blocked. When using botnets this is known as a Distributed Denial of Service, or DDoS, attack (Grabosky, 2007b).
other groups. Felson (1998) states that criminologists, along with the mainstream media, tend to overstate the extent that mundane crimes are organised.

Cyberterrorism and cyberwarfare

Although cyberterrorism and cyberwarfare are not in themselves activities that are included in this research, reportedly there are some overlaps with computer fraud and hacking. Although there have reportedly been no terrorist attacks using hacking abilities to target critical infrastructure\(^4\) to cause widespread damage (Australian Institute of Criminology, 2005b; Theohary & Rollins, 2011), government agencies regularly conduct operations to test their ability to deal with such a catastrophe. For example, “Cyber Storm” exercises have been conducted internationally since the year 2006 (Department of Homeland Security, 2011). Although critical infrastructure does not seem to have been attacked electronically by terrorists, online crime, such as frauds, may be committed to fund terrorist organisations (Choo, 2008; Smith, McCusker, & Walters, 2010). Choo (2008) also points out that terrorists may use information freely available on the internet to plan their attacks, such as how to build bombs, as well as the use of legitimate information such as satellite imagery to map out terrain. Websites maintained by terrorist organisations may distribute propaganda, solicit funding and recruit members by reaching an international audience (Choo, 2008; Seib, 2008). The internet can also be used for

\(^4\) Critical infrastructure includes, among others, electricity, water, communications, air traffic control and financial systems (Grabosky, 2007b).
communication within terrorist organisations, which may extend to “psychological warfare” (Grabosky, 2007b, p. 205), which refers to deceptive communication to give the impression that an attack is imminent, therefore distracting law enforcement and intelligence services from other activities (Grabosky, 2007b).

Cyberwarfare, where countries attack each other electronically at times of conflict, has reportedly happened during a disagreement between Russia and Estonia in 2007 (Lesk, 2007), the Russia/Georgia war in 2008 (Cluley, 2008) and the Israeli/Gaza war in 2009 (Cluley, 2009). There has been speculation that the Stuxnet worm\(^5\) that targeted Iranian nuclear facilities was the outcome of United States and Israeli cooperation (Stratfor Global Intelligence, 2011). Additionally, espionage has been known to have been committed electronically as far back as 1986, as detailed by Stoll (1989), whose book *The Cuckoo’s Egg* recounts his efforts to track down a German hacker who, using the university network that Stoll was protecting, was accessing United States government agencies in order to provide information to the Soviet KGB.

**Criminology and computer crime**

As computer crimes are a comparatively new phenomenon they have not received as much academic attention as other types of crime, such as “the mundane crimes of the poor” (Hayes & Prenzler, 2003, p. 15). The House of Representatives Standing Committee on Communications (2010), in their report into cyber crime, acknowledged that research in this area is lacking, which has in

\(^5\) A worm is a self-replicating program that spreads automatically (Grabosky, 2007a).
turn led to an uninformed policy response. At the 2008 American Society of Criminology conference only one per cent of papers related to computer crime or technology intensive crime (Dupont, 2009). Parker (1998) states, in relation to quantifying the amount of hacking activities that occur, that “qualified researchers have never found sufficient funding to do valid surveys and test their success” (p. 165). As Grabosky and Broadhurst (2005) point out, researchers may find it difficult to obtain reliable data relating to computer crime, particularly when the reputations of companies, governments and individuals are at stake. Also, computer crimes have many manifestations. As a result, some computer crimes are more likely to receive the attention of researchers, policy makers and funding bodies than others. These may include crimes that have resulted in “moral panic” (Cohen, 1973), (defined as “disproportionate reactions to perceived threats” (Critcher, 2006, p. 2)), such as child pornography or cyber grooming (Theohary & Rollins, 2011).

Another possible explanation for this gap is that the origins of what we call computer crime may not have always been considered criminal. Historically the term “hacking” referred to operators of legitimate amateur radio and computer code writers, who were admired for their technical skills rather than reviled (Levy, 1984; Moschovitis, Poole, Schuyler, & Senft, 1999; Thomas, 2005). In addition, software piracy was previously a non-issue, with software developers sharing information, codes and programs in return for peer recognition (Levy, 1984). According to Moschovitis et al. (1999), it was software companies, such as Microsoft, that saw program sharing as damaging to their profit margins, that made software piracy a problem.
A final reason for the lack of criminological attention is that, despite the apparent widespread nature of computer crime, very few cases are dealt with by the criminal justice system. First, victims may not report their offences, and when they do report only some will be pursued by law enforcement. Second, of those that are pursued only a small number will end up being prosecuted, and a smaller amount still will result in a conviction. Therefore, computer crime may escape the attention of academic researchers.

Despite criminology falling behind in its explanation of computer crime, it has not ignored the subject. This chapter discusses previous research into these crimes. However, when criminological theories have been applied to explain these behaviours, it has often not been supported by empirical research, or research relating to offenders. There has also been a tendency to describe “how” offenders are committing these offences, rather than “why”. Instead, what we think we know about computer crime offenders has largely been influenced and shaped by “haxploitation movies” (Wall, 2010, p. 90). These perceptions have perpetuated due to their appearance in mainstream media (Webber & Vass, 2010), which appeals to the public’s desire for entertainment that thrills (Wall, 2010).

**Computer crime and the law in Australia**

When computer misuse comes to light it may be identified as a crime under legislative frameworks. Alternatively it may be something that is dealt with internally when employees abuse their employers' systems (Bronitt & Gani, 2005), be subject to regulatory oversight, such as the Australian Securities and
Investments Commission or the Australian Competition Consumer Commission, or attract civil remedies when intellectual property or commercial laws have been violated (Bronitt & Gani, 2005).

This section will highlight various legislative frameworks associated with responding to and preventing computer crime. Legislation criminalising hacking may be found in all Australian states and territories. In most jurisdictions, one of the elements of these offences is that the computer must be restricted, meaning that it is protected against unauthorised use. Appendices A and B provide the statutory offences in Australian jurisdictions that may be applicable to hacking. Appendix A outlines the offences relating to unauthorised access related matters, while Appendix B summarises the data related offences. In addition to these offences, hackers who target government or public services may be charged with sabotage under state, territory or commonwealth legislation.

Australia has taken an ad hoc approach to incorporating cybercrime matters into its legal system. This is partly due to different approaches taken by the states and territories, which generally have jurisdiction over criminal law, and the law lagging behind the evolution of technology. The law has required, and will likely continue to require, continual updating in this area to address new challenges. For example, in the 1980s laws were changed to incorporate computer hacking, or unauthorised access, as traditional property offences were found not to apply to intangible data held on computers (Bronitt & Gani, 2005).

In relation to computer crime, the Commonwealth has jurisdiction over matters relating to telecommunications systems, intellectual property, and its own computers (Urbas & Choo, 2008). Urbas and Choo (2008) predict that the
Commonwealth will begin pursuing the investigation and prosecution of more computer related crimes, taking over the responsibility of the states and territories. As telecommunication systems invariably include access to the internet, some computer crime matters may fall under Commonwealth jurisdiction, enabling this wider scope of federal powers (Bronitt & McSherry, 2010).

A national law reform process has resulted in a gradual move towards uniformity for computer crime related matters across Australian jurisdictions since the 1990s (Bronitt & Gani, 2005). A model criminal code drafted by the Model Criminal Code Officers Committee has been adopted wholly or in part by some Australian jurisdictions (Clough, 2010) and is the basis for the provisions in the Criminal Code Act 1995 (Cth) (the Commonwealth Criminal Code) that relate to computer crime. However, these provisions currently address only those offences that are not covered by existing state laws (Bronitt & Gani, 2005).

In 2011 the Australian Government announced that it intends to accede to the Council of Europe Convention on Cybercrime (the Convention). The Convention requires the harmonization of criminal laws in relation to hacking, fraud, child exploitation material and copyright infringement, and aims to enhance international cooperation (Parliament of Australia Joint Standing Committee on Treaties, 2011). Acceding to the Convention will require amendments to the Commonwealth Criminal Code so that the provisions are no longer limited to Commonwealth computers; a computer where data is held on behalf of the Commonwealth; or where the case involves access, modification or impairment via a telecommunications service. However, a savings clause within existing
legislation means that offences relating to computer crime do not exclude or limit the operation of other Commonwealth, state or territory laws (Parliament of Australia Joint Standing Committee on Treaties, 2011).

Fraudsters that operate online face the same charges applicable if the fraud was conducted in physical space, with Tasmania being the only Australian state to have a separate offence for computer related fraud. Appendix C compares the Australian state and territory legislation that may be applicable to computer fraud. Separate offences may be applicable to frauds conducted by company officials or agents. Appendix D summarises identity-related offences that may be applicable to computer fraud, such as possession of or dealing with identification information and falsification of documents.

In addition to variations between jurisdictions, some types of offences may meet the elements of different charges. To take phishing as an example, depending on the jurisdiction, there may be three possible junctures at which a typical act of phishing could be classified as a criminal offence. The first point is when the offending website is created and phishing emails are distributed, the second is when the information is stolen from the victims, and the third is when that information is used, either directly by the phishing offender, or when it is sold to another for fraudulent use. An additional point is the liability of financial managers and money mules, who receive the money from the phisher and then transfer them abroad by means of hawala6 or more conventional funds-transfer systems such as Western Union. Within Australia, Commonwealth law and some

---

6 Hawala refers to a type of alternative remittance system used to transfer funds (Rees, 2010).
state or territory laws are applicable at all three points, while the remaining
Australian states have gaps at various junctures. Relevant provisions from the
*Trade Practices Act 1974* (Commonwealth) may also be applicable to misleading
practices conducted online. In addition, the *Spam Act 2003* (Commonwealth)
provides civil penalties for the unsolicited sending of commercial email with an
Australian link and the use of harvested address lists, which may be used in the
commission of computer frauds.

As demonstrated in Appendices A to D, there is inconsistency and a lack
of uniformity across Australian jurisdictions in relation to offence provisions and
maximum penalties, with the Commonwealth, New South Wales, Victoria and the
Australian Capital Territory generally having the most comprehensive legislation.
These jurisdictions are also those that have most closely adopted the model
criminal code for computer crime related matters. However, charges may be laid
in the state where the offender or victim(s) are located, or the jurisdictions
through which communications have passed (Smith et al., 2004). While this
means that investigating officers in one state may cooperate with law
enforcement located in another jurisdiction in order to have the most appropriate
charges laid to meet the offence(s) committed, a national protocol has been
developed by the National Cyber Crime Working Group, established by the
Standing Council of Attorneys-General, that provides a framework for
determining which jurisdiction will deal with complaints (O’Connor, 2011). The
issues relating to inconsistent laws is not limited to Australia, with some activities
considered illegal here not being unlawful in other countries, which may affect
extradition arrangements and transnational cooperation (Urbas & Grabosky,
2006). However, Australian citizens who commit computer crimes overseas may be charged under commonwealth legislation even if no part of the offence took place in Australia (Bronitt & McSherry, 2010).

Selvadurai, Islam and Gillies (2010) argue, in relation to identity theft, that having broad federal provisions and a multitude of state and territory provisions is inadequate. This lack of an integrated approach could create confusion with how to proceed with cases, and the applicable penalties vary greatly across jurisdictions. Selvadurai et al. (2010) recommend the creation of a single, comprehensive federal offence of identity theft. The proposed offence should “apply to all parties involved in the “chain” of data capture, transfer and use” (Selvadurai et al., 2010, p. 41). Similarly, Bronitt and Gani (2005) recommend that laws should be harmonised across regions, in addition to developing effective extradition arrangements.

As mentioned above, there is variation in applicable penalties for computer crime related offences. Smith et al. (2004) compiled 240 case studies from criminal law sentencing outcomes to determine how offenders charged with computer crime offences have been dealt with by the judicial process in North America, the United Kingdom and Australasia from 1972 to 2003. Of these 240 cases, 164 involved a finding of guilt or a guilty plea, and of these 164, the authors were able to locate sentencing outcomes for 139 cases. Of these 139 cases, 101 included online hacking or fraud offenses, while the remainder related to various other computer crimes, such as obtaining telecommunications services
dishonestly; malicious code, viruses,\(^7\) dissemination of unsolicited messages, and DDoS attacks; software piracy and intellectual property offenses, illegal child pornography or other obscene images; and online stalking or sending of threatening messages. Smith et al. (2004) note that the cases they have collected are not a representative sample, including those that are more likely to be high profile, and that it is difficult to determine how many cases have been prosecuted and offenders convicted due to the way these types of offenses are classified.

Smith et al. (2004) categorised the types of sentences imposed for the various types of offenses. Those relating to online theft or fraud (cases where fraud or theft was the principal reason for the misuse of computers), hacking (external access to networks for curiosity or malicious reasons) and access or modification (unlawful access to computers and modification of data) are shown below in Table 1. It is important to note, however, that multiple entries are recorded for some cases, and some cases involve multiple offence types (Smith et al., 2004). For example, the death penalty was imposed only once in the cases reviewed (in China); however, this case would have included both fraud and hacking offenses. In other cases, the offender may have received more than one type of sanction (Smith et al., 2004).

\(^7\) Viruses are a type of self-replicating malicious code that are spread by opening infected files (Grabosky, 2007a).
Table 1

Sentences Imposed in Fraud/Theft, Hacking, and Unlawful Access/Modification

<table>
<thead>
<tr>
<th>Sentence imposed</th>
<th>Fraud/Theft</th>
<th>Hacking</th>
<th>Access/Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apology</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Publicity of sanction</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspended sentence</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Probation/supervised release/conditional discharge</td>
<td>10</td>
<td>19</td>
<td>8</td>
</tr>
<tr>
<td>Restricted use of computers and/or internet</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>Forfeiture of computers</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Home detention</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Community service</td>
<td>3</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Compensation/restitution to victims</td>
<td>12</td>
<td>17</td>
<td>10</td>
</tr>
<tr>
<td>Periodic detention</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Fine or payment of costs</td>
<td>10</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>Imprisonment full-time, 12 months or less</td>
<td>6</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>Imprisonment full-time, 13 to 23 months</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Imprisonment full-time, 24 to 59 months</td>
<td>17</td>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td>Imprisonment full-time, 60 to 119 months</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Imprisonment full-time, 120 months or more</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Death</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

Source: Smith et al. (2004)

Smith et al. (2004) discuss a number of factors that may explain the variability in penalties to the differences across jurisdictions. These include that certain types of criminal behaviours may attract multiple criminal charges, offences involving multiple victims may be perceived as being more severe and therefore attract harsher penalties, and some matters may be perceived as being more serious than they are due to the complex investigations and evidentiary requirements. There were also differences in penalties across jurisdictions, with custodial sentences more likely to be imposed in the United States. In addition, as computer crimes are comparatively new, the variability could reflect the
continued establishment of precedents for appropriate sentences (Smith et al., 2004).

Overall, the trend relating to computer crime and the law appears to be a growing influence of international treaties and the continued harmonisation and coordination of law enforcement efforts.

**Computer crime and crime prevention**

Criminological theories and assumptions about the nature of crime and offenders can inform crime prevention methods. In relation to hacking and computer fraud a variety of crime prevention techniques are actively used by state agencies. These strategies may be categorised as creating awareness among potential victims, monitoring and regulation of internet users and control or restriction of internet content. In relation to computer fraud, proactive steps have aimed to encourage potential victims to ensure that their computers and personal information are safe. One example is an annual campaign run by the Australasian Consumer Fraud Taskforce (ACFT) since 2007. The ACFT consists of 22 government agencies and departments concerned with consumer protection in relation to frauds and scams (Australian Competition & Consumer Commission, 2011a). Smith and Akman (2008) evaluated the 2007 campaign and concluded that it was highly effective in raising consumer awareness. The campaign included the distribution of posters, flyers, identity fraud prevention kits, media releases, radio and television appearances, and advertisements and articles in newspapers and magazines (Smith & Akman, 2008).
Some countries have actively monitored and regulated the communication and online behaviours of their citizens. For example, China regulates cybercafés in that they must hold a valid licence and patrons must be aged over the age of 18 or be accompanied by a parent or guardian (Wong & Wong, 2005). In China, India and Italy users must produce valid personal identification in order to use the services offered by cybercafés (Barge, 2007). Such requirements raise additional implications in relation to threats to privacy and the potential for misplacement, loss and theft of stored identity information.

Internet filtering is actively used in China (Wong & Wong, 2005), the Kingdom of Saudi Arabia and approximately 57 other nation-states (Shannon & Thomas, 2005). China actively censors internet content, such as gambling, pornography and anti-government information (Wong & Wong, 2005), while the filters used by the Kingdom of Saudi Arabia have been found to block information relating to “religion, health, education, reference, humour and entertainment” (Shannon & Thomas, 2005, p. 339). However, due to the volume of information, the changing nature of technology and the use of email and P2P\(^8\) networks to distribute data, it is impossible to filter all undesired content (Wong & Wong, 2005). Also, research indicates that there is a large gap between the likelihood of being inadvertently exposed to online pornography and the perceived likelihood (Zimmer & Hunter, 2000).

In 2008 Australia announced plans to filter online material, in which refused classification material, including “child sexual abuse imagery, bestiality,

---

\(^8\) A P2P, or peer-to-peer, network refers to a direct network communication between two computers, without the use of an intermediary host or server (Phair, 2007).
sexual violence, detailed instruction in crime, violence or drug use and/or material that advocates the doing of a terrorist act” would be blocked at the Internet Service Provider (ISP) level (Department of Broadband, 2011). However, the plans have been politically unpopular, with protests launched by Anonymous, a hactivist group, by way of DDoS attacks against the website of the Australian Federal Parliament (Hardy, 2011). The government is currently reviewing what material would be covered under the refused classification category. Meanwhile, three ISPs have agreed to voluntarily block child exploitation material (Department of Broadband, 2011).

Target hardening approaches are used by individuals and private enterprises, as well as governments. These include technologies such as antivirus software, firewalls,\(^9\) encryption\(^{10}\) and virtual private networks (VPNs).\(^{11}\) These types of approaches are aimed at making it harder for offenders. However, these technical target hardening methods have resulted in a competition between offenders and those who protect computer systems and displacement to other, more vulnerable, targets (Attorney-General’s Department, 2000; Ekblom, 1999). These more vulnerable targets may include those who cannot afford the same level of protection, or those who are already less fortunate (Yar, 2010a). As stated by Parker (1998, p. 171), “an attack by a

---

\(^9\) Firewalls restrict incoming traffic to protected computer systems (Casey, Larson, & Long, 2002).

\(^{10}\) Encryption, or cryptology, refers to changing data to ciphertext so that it cannot be used until unlocked with a ‘key’, or decrypted (Parker, 1998).

\(^{11}\) Virtual Private Networks (VPNs) provide a secure, encrypted connection through the public internet to a private network (Casey et al., 2002).
sufficiently resolute hacker will always succeed, given enough time” (emphasis in original). Similarly, the Anti-Phishing Working Group (2008) state that:

Criminal hackers have apparently redoubled their efforts to develop new techniques and scripts to bypass security measures taken by consumers and enterprises – in addition to increasing the numbers of crimeware-spreading websites (Anti-Phishing Working Group, 2008, p. 8).

Technologies developed to deflect offenders may actually be of practical use to facilitate criminal behaviour. For example, encrypted data has been used for the transmission of information relating to organised crime (Australian Institute of Criminology, 2006; Choo, 2008; Denning & Baugh, 1998; Grabosky, 2007b; Rogerson & Pease, 2004). Another limitation of target hardening is that it becomes more difficult for legitimate users to navigate the internet as “current solutions involve a multitude of documents, plastic cards, PIN numbers [sic] and passwords to carry and remember (or to lose and forget)” (Rogerson & Pease, 2004, p. 1). In addition, the use of passwords involves a human element that may be overcome by the use of social engineering techniques to obtain identification information (Adams & Sasse, 1999), if not by technical means such as password cracking and keylogging software (McQuade, 2006).

There seems to be little, if anything, to discourage potential offenders from attempting fraud or accessing a system without authorisation. This is supported by Chantler (1995) who found that 98.6 per cent of hackers that responded to his question as to whether the threat of detection and prosecution inhibited their

---

12 Password cracking software uses brute force to access a computer system by attempting to match a dictionary of potential passwords against a username (McQuade, 2006).
activities answered in the negative. Offenders may not be deterred from the possibility of apprehension or punishment due to the many known obstacles faced by law enforcement, such as jurisdictional and evidentiary issues and the difficulties and expense of investigation and prosecution (Lynch, 2005). Offenders have a range of tools and techniques available to them that enable them to evade detection, such as the use of cyber cafes, proxy servers\textsuperscript{13} (Broadhurst & Grabosky, 2005), wardriving,\textsuperscript{14} Tor\textsuperscript{15} networks, wireless broadband, the use of publicly available wireless networks, and anonymous remailers\textsuperscript{16} (Uchimura, 2005). In addition, most computer crimes are never reported to the police (Yar, 2006).

Proactive offender-oriented crime prevention methods could potentially take a number of different approaches. Ekblom (1997) differentiates between offender-oriented crime prevention methods that target potential offenders early in their life course; those that target the current circumstances that offenders or potential offenders may be in that are conducive to crime; and the restriction of resources available that enable offenders to commit crime. Such prevention methods require knowledge about the causal mechanisms for crime.

\textsuperscript{13} Using an open proxy server to make indirect network connections allows a user to hide their Internet Protocol (IP) address (Phair, 2007). An IP address is used to address computers for communication (Curran, 2010).

\textsuperscript{14} Wardriving refers to driving in a local area with a portable device such as a laptop for the purposes of gaining unauthorised access to wireless networks (Freeman, 2006).

\textsuperscript{15} The onion router, or Tor, is a network of encrypted connections on the internet. “Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it’s going” (The Tor Project, 2011).

\textsuperscript{16} Anonymous remailers remove the sender’s details from an email before forwarding it to the intended recipient (du Pont, 2001).
Smith et al. (2004) provide some examples where offenders, once they become aware of the enormity of the damage that they have caused and the subsequent impact on victims, have been remorseful for their actions. However, this awareness, and its potential deterrent effects, does not occur until after the damage has already been done. As cited by Smith et al. (2004, p. 114), “the challenge that faces us is how to ensure that potential offenders realise the significance of their actions prior to engaging in cyber crime” (emphasis in original). However, Grabosky (2005) predicts that computer ethics training, while useful, would have only a marginal impact on offending.

As noted by Garland (1996), it is not solely the state’s responsibility to prevent or control crime. In relation to computer crime the state is especially limited due to the challenges presented by jurisdiction and anonymity. Crime prevention should be situated in knowledge of the understanding of the offender’s perspective in order to be effective. The way criminological theory can assist with this understanding is presented in Chapter 11. Wright and Bennett (1990) claim that the implementation of crime prevention initiatives without this kind of understanding can be a waste of money and potentially results in the reduction of the quality of life. In relation to computer crime prevention, this reduction in the quality of life is becoming more evident with the number of different passwords which must be remembered and the time and bandwidth used to download and install security patches.
Prevalence and economic cost

The importance of this area as a research topic may be emphasised by examining the prevalence and financial costs of these types of crime. However, estimates of financial cost can vary wildly across time, place and the operationalisation of “fraud” or “hacking”. For example, it is difficult to ascertain from police data the extent that these crimes are reported to the authorities. Due to the recent nature of computer crime offences, incidences such as computer fraud may be recorded under a general ‘fraud’ category (Broadhurst & Grabosky, 2005). The House of Representatives Standing Committee on Communications (2010) reported that Australian state, territory and federal governments collected “fragmented” data relating to computer crime. For example, scams recipients and victims may report matters to policing agencies, state and territory consumer protection agencies, the Australian Competition and Consumer Commission (ACCC), the Australian Communications and Media Authority, the Australian Securities and Investments Commission or the Australian Tax Office. Other organisations that may receive complaints about scams include banks and financial institutions, online trading and auction sites, as well as social media sites (Australian Competition & Consumer Commission, 2011b). Insider abuse of access is often dealt with internally, and therefore never becomes public knowledge (Shaw et al., 1998). This not only makes identifying the extent of these offences difficult, but also the trends to see how the prevalence has changed over time. Some estimates of the cost of fraud in Australia are provided below in Table 2.
| Source                                                                 | Estimated cost | Period                      | Geographic area       | Victims                                | Types of offenses                                                                 | Cost includes                                                                                   | How calculated                                      |
|------------------------------------------------------------------------|----------------|-----------------------------|-----------------------|----------------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Australian Transaction Reports and Analysis Centre (Cuganesan & Lacey, 2003) | $1.1B          | 2001/02 financial year      | Australia             | Public and private sector organisations | Identity fraud                                                                   | Prevention, deterrence, detection, investigation, recovery, restoration, financial loss, intangible loss and opportunity costs | Estimated from a sample of 120 organisations        |
| Australian Competition and Consumer Commission (Richmond, 2008)        | $1B            | 2008                        | Australia             | Individuals                           | Advance fee fraud                                                               | Direct financial loss                                                                             | Calculated from a proportion of funds sent from Australia to Nigeria |
| Australian Bureau of Statistics (2012)                                 | $1.4B          | 2010/11 financial year      | Australia             | Individuals                           | Personal frauds such as identity theft and credit card fraud, and scams including lotteries, pyramid scheme, phishing and related scams, chain letters, advance fee fraud, and other scams, such as door-to-door sales and fraudulent repair work | Direct financial loss                                                                             | Estimated from a sample of 26,405 individuals       |
| Australian Institute of Criminology (Richards, 2009)                   | $595-649M      | 2006/07 financial year      | Australia             | Businesses, ranging in both size and industry sector, excluding government organisations | Unauthorised use, damage, monitoring attack or theft of business information technology | Direct financial loss, costs to repair the damage, loss of revenue and any directly related costs | Estimated from a sample of 4,000 businesses         |
| Drugs and Crime Prevention Committee (2004)                            | $641M          | 2003                        | Victoria              | Not specified                         | Fraud and white collar crime                                                    | Direct financial and intangible losses                                                            | Estimated from police data and the results of victimisation surveys |
| KPMG (2010)                                                            | $345.4M        | February 2008 to January 2010 | Australia and New Zealand | Public and private sector organisations | Fraud                                                                          | Direct financial loss                                                                             | Estimated from a sample of 214 organisations        |
As can be seen in Table 2, the estimated cost varied from AUD$345.4 million for two years for all of Australia and New Zealand for fraud (KPMG, 2010), to AUD$641 million in one year for fraud only in one Australian state (Drugs and Crime Prevention Committee, 2004), escalating up to $1.1 billion for just one type of fraud in one year in Australia (Australian Transaction Reports and Analysis Centre, 2003). Reasons for this variation may be partly due to where the figures are obtained (for example, police data compared to victimisation surveys) and what the costs include, such as the direct financial loss or “intangible losses”. While the cost of hacking is not as well documented than computer fraud, it would be expected that any estimates would suffer from the same variations and problems as estimates of fraud costs. These problems will be discussed later.

Reports indicate that the rate of computer crime has been rising for some time. For example, Speer (2000) reported that in 1988 the American CERT Coordination team handled six incidents of computer crime compared to 3,734 ten years later in 1998, and then in just one year the rate almost doubled again, with 6,844 incidents in 1999. The Australian Computer Crime and Security Survey found that in 2006, six per cent of respondent organisations detected identification theft against staff, customers or clients and eight companies reported a combined annual loss of AUD$215,103 (AusCERT, 2006). This is a substantial increase from the 2005 survey, in which four companies reported an annual loss of AUD$62,000 resulting from identity theft (AusCERT, 2005). While this may be due to the increased sample size of the 2006 survey, it is important to keep in mind that this survey contains a number of limitations. The survey had
a low (17 per cent) response rate (AusCERT, 2006); only eight company respondents reported identity theft (resulting in an average AUD$26,888 loss per company); and different companies may calculate their losses in different ways (Australian Institute of Criminology, 2005a). In addition, no specific information was provided on organisations likely to be targeted for attacks, such as banks and other financial institutions, which only constituted six per cent of the overall sample (AusCERT, 2006).

Results from the Australian Business Assessment of Computer User Survey (ABACUS) for the 2006/07 financial year indicate that 14 per cent of the 4,000 respondents had experienced a computer security incident (Richards, 2009). Of those that had experienced a computer security incident, nine per cent experienced insider abuse of access; nine per cent reported theft or loss of hardware; 64 per cent experienced viruses or malicious code; 44 per cent were infected with spyware;17 24 per cent experienced phishing attacks; four per cent experienced DoS attacks; three per cent had their network or data sabotaged; nine per cent had their network accessed without authorisation; five per cent experienced theft or breach of proprietary or confidential information; and three per cent experienced an incident involving their business’s web application (Richards, 2009). However, in some instances it is unclear what these categories represent. For example, it is not differentiated whether phishing attacks relates to the receipt of a phishing email, or whether the company itself

17 Spyware refers to a program that can monitor computer activity (Grabosky, 2007a).
has been fraudulently represented by offenders attempting to obtain the details of their customers (Richards, 2009).

Interestingly, when broken down by industry type, only 19 per cent of businesses providing financial or insurance services reported a computer security incident, which led to the conclusion that financial organisations are not more likely to be targets than those in other industry sectors (Richards, 2009). What is unknown, however, is whether respondents would have interpreted the definition of a computer security incident, namely “unauthorised use, damage, monitoring attack or theft of your business information technology” (Richards, 2009, p. 2) as including instances where third parties, such as customers, have had their security breached in relation to the services offered by the business. This is particularly relevant to phishing, where it may be argued that it is the customer who provided their personal information on, for example, a website that appeared to look like, but was not, that of a legitimate company. As identified above, the ABACUS did not identify how many respondents were fraudulently represented in this way by offenders in phishing attacks. In addition, financial service providers may be unwilling to disclose victimisation due to concerns about consumer confidence.

As mentioned previously, numerous problems make estimating the true cost of computer crime, or comparing the cost across time or jurisdiction, difficult. Estimates usually escalate over time, presumably reflecting increases in offending – either the same number of offenders are offending more and causing greater damage or the number of offenders are increasing. Alternatively, more victim complaints may be received and/or recorded. However, the impact may
also be inflated due to companies claiming that more time or money was required to fix the damage than was actually the case (Thomas, 2005), particularly if they are seeking compensation through the legal system or making an insurance claim. The estimates may also include the costs to secure a system to avoid re-victimisation if security was previously lax, therefore reflect not the cost of damage done, but the cost of target hardening. Corporations and policing agencies may also overestimate the cost of victimisation in order to lobby for stricter penalties and increased powers (Grabosky, 2005).

Furthermore, the public’s perception of potential damage may be inflated by the computer security industry, who stands to profit from the fear of victimisation (Grabosky, 2005), with the amount spent each year on computer security by Australian businesses estimated to be between AUD$1.37billion and AUD$1.95billion (Richards, 2009). This essentially means that a financial gain can be achieved from offending by those who aim to protect against it. This creates a new industry making money from victimisation, therefore their marketing aims to generate fear among potential victims. In fact, this perception of risk has been used for further fraud victimisation through the use of “scareware” (Yar, 2010b, p. 115), whereby a victim’s computer is infected with a virus that informs them that they need to purchase bogus antivirus software to remove it.

Other costs may be hard to calculate. These include accurately determining losses incurred due to consumers losing confidence, industrial espionage, the impact on the economy as the funds are not being spent elsewhere, lost time, and the emotional impact on victims. Ross and Smith
(2011) surveyed Australians who had been identified by the Australian Transaction Reports and Analysis Centre as having sent money to Nigeria in the 12 months to 31 March 2008. Of the 59 per cent of respondents who were identified as being victims of advance fee fraud, the average amount sent overseas was $12,000. However, costs are not only financial, with 43 per cent of victims reporting emotional trauma, 40 per cent reporting a loss of confidence in other people and 12 per cent experienced marital or relationship problems. Financial hardship was also reported by 54 per cent of victims (Ross & Smith, 2011). Some may argue that the cost is under-representative as companies do not admit to victimisation or may not know that they have been victimised (Pontell, 2002). However, whatever the true cost is, it cannot be denied that it is likely to be substantial. Perhaps the most accurate statement that could be found relating to the financial cost of computer crime is provided by Rosoff et al. (2004), who state “…some experts have adopted an “agnostic” position that the true cost is unknowable” (p. 479).

Despite a recommendation by the Australian Law Reform Commission in 2008 (Australian Law Reform Commission, 2008), there is currently no requirement in Australia for businesses to advise individuals if their personal identifying information has been breached accidently or by unauthorised access to a computer system. Yar (2006) estimates that as little as five per cent of computer crimes are reported to authorities. Targeted corporations may under-report incidents for a number of reasons. The ABACUS survey revealed that in the 2006/07 financial year 77 per cent of respondents that had experienced a computer security incident dealt with their most serious incident internally; eight
per cent reported the incident to the police, three per cent reported to a non-
police enforcement or regulatory agency, and 11 per cent reported to another
organisation such as Visa or MasterCard, a lawyer or AusCERT (Richards,
2009). In 2006 the Australian Computer Crime and Security Survey found that of
the respondent companies that had experienced any type of electronic attack, 69
per cent chose not to report it to anyone outside their organisation (AusCERT,
2006). Reasons for not reporting included, among others: perceived negative
publicity (46 per cent); not being aware of law enforcement interest (52 per cent);
not thinking perpetrators would be caught (57 per cent); and not thinking law
enforcement was capable (55 per cent) (AusCERT, 2006).

Reviewing the outcome of investigations reported in the Australian
Computer Crime and Security Survey it is not surprising that organisations hold
negative views about law enforcement action, with only 19 per cent of law
enforcement investigations resulting in criminal charges (AusCERT, 2006). Other
outcomes included allegations not being investigated (21 per cent),
inadequate legislation (two per cent), lack of evidence (49 per cent), and
jurisdictional difficulties (seven per cent) (AusCERT, 2006). These difficulties
faced by law enforcement agencies emphasise the need for prevention in
addition to prosecution. As Graycar and Smith (2002) note, taking no action may
convey the message that online offences are tolerated by law enforcement
agencies.

In addition, individuals may not report victimisation for a number of
reasons. Muscat, James and Graycar (2002) conducted a study on consumer
fraud and found that only 35 per cent of victims reported the incident to the police
or another agency. Reasons that victims may not report include not being aware that they have become a victim due to not checking banking activity or credit rating (MacGibbon, 2005), not being aware of law enforcement interest (Federal Deposit Insurance Corporation, 2004), and feeling responsible for becoming a victim (Muscat et al., 2002). The Internet Crime Complaint Center (IC3), an American central reporting and referral body, has received and monitored complaints relating to computer fraud, intellectual property infringements, hacking, espionage, child pornography, money laundering and identity theft since May 2000 (Internet Crime Complaint Center, 2009). The IC3 attributes victims’ awareness of law enforcement interest to the escalating rate of internet auction fraud reported. Since eBay provided a link to the IC3 website, it is reported that the percentage of reports relating to internet auction fraud has increased to 23.5 per cent of all fraud categories in 2008 (Internet Crime Complaint Center, 2009).

The number of potential victims (the number of people and businesses that use the internet) has been increasing steadily. As at 31 December 2010 there were 10.4 million internet subscriptions in Australia (Australian Bureau of Statistics, 2011) compared to 3.8 million in 2000 (Australian Bureau of Statistics, 2001), an increase of 173.7 per cent over ten years. Not only has the number of people with access to the internet increased, but more people are spending more time online. In 2008, 55 per cent of Australians accessed the internet eight times per week (classified as “heavy use”) compared to 44 per cent in 2006 (Australian Communications and Media Authority, 2008). Time online is used for a variety of purposes; however the two highest categories include checking email (98 per cent of Australian internet users) and using internet banking (72 per cent)
(Australian Communications and Media Authority, 2008). This is problematic as much computer fraud is conducted by email, and some frauds, such as phishing, specifically relate to the use of internet banking. Although the breakdown of internet activities provided by the Australian Communications and Media Authority (2008) did not include online shopping as a single category, internet auction sites (which are conducive to internet auction fraud) were accessed by 37 per cent of Australian internet users. Online social networking sites, such as Facebook, Myspace and Linkedin, which are also popular with fraudsters, were accessed by 26 per cent of Australian internet users (Australian Communications and Media Authority, 2008).

**Conclusion**

This chapter has demonstrated that, although not much is known about the prevalence and overall cost of computer crimes, there is little doubt that it is considerable. In addition, the cost of computer crimes does not stop at the direct financial loss, but includes the emotional costs, costs to the economy, business reputations and those related to recovery. Despite this impact, relatively little is known about who commits these crimes. This chapter has argued that this is due to the lack of attention to computer crimes within the criminology discipline, as the technologies that enable these offences to occur have emerged rapidly over a short period in time.

Although an industry has emerged providing solutions aimed at stopping computer intrusions and removing malicious software, or malware, from computers, it resembles little more than a game of cat and mouse. Offender
techniques are constantly evolving, and this chapter has attempted to demonstrate that crime prevention strategies should not be limited to technical approaches. Already steps are being taken to better educate potential victims, however the number of people who can be victimised is considerable, and offenders have a large pool of susceptible targets.

The importance of knowing more about these offenders, and ways to deter them, increases as more and more information is stored on computer networks. For example, many businesses are transferring to ‘paperless offices’, where filing is completed electronically. In addition, advances in technology and the convenience this provides to potential users means that more vulnerabilities are likely to arise. The challenge is to explain offending behaviour in order to provide a better and more effective crime prevention strategy. The next chapter outlines the theories used in this research to address this challenge.
Chapter 3 ~ Theory and Crime

Criminological theories allow us to organise what we know about crime, so that it can be understood and explained. For example, theories address issues such as how offenders learn the techniques of committing crime, their associations with other offenders, family and society, their attitudes towards crime and their victims, their motivations for committing crime and their perceptions of apprehension and punishment. During the 20th century explanations of crime followed various trends that represented differences in the assumptions about crime. Garland (2001, p. 15) identified three main eras, namely the post-war “welfare” period, the “control” period from the 1970s and “contemporary criminology”. During the post-war period abnormal psychological explanations were popular, along with sociological theories of anomie, relative deprivation, sub cultural and labelling theories. These theories led to crime prevention efforts that focussed on individual treatment, as well as overcoming deprivation within society through the provision of support such as welfare, education and employment (Garland, 2001). The control period saw the introduction of theories that focussed on inadequate controls rather than deprivation. The implications for this era related to increasing social controls in the family, the community and the state as well as greater enforcement of the law (Garland, 2001). Contemporary criminology, on the other hand, viewed crime as being normal and routine and the focus turned to situations that fostered crime
and how these could be changed through the use of situational crime prevention methods (Garland, 2001).

Although often attempting to explain the same phenomenon, theories of crime vary greatly, particularly in their assumptions relating to criminal behaviour. Einstadter and Henry (2006) conducted an analysis of the evident and implicit underlying assumptions of various criminological theories and determined that they could be differentiated according to their assumptions of human nature, human behaviour, society and social order, the role of law, definitions of crime, causal logic and criminal justice implications. For example, assumptions relating to human nature and human behaviour relate to issues such as to the extent that we do not commit crime because we agree on what is appropriate behaviour, or because of the laws that constrain our otherwise law-breaking tendencies; the extent to which our behaviour is freely chosen or determined by external forces; and whether those forces are internal, such as biology or personality, or external, such as the social environment. An example of an assumption about society and social order is whether society concentrates economic and political power within relatively few sections of society, leading to conflict, or whether power is dispersed among people with common values, leading to consensus. Assumptions relating to the role of the law or definitions of crime relate to what behaviours are studied, i.e. whether crime is legally defined by law, or whether it includes other social harms, including crimes of the powerful such as corporations and the state.
This chapter begins by explaining how the theories that underpin this research were selected. The chapter then critically evaluates the theories and how they may be applied to explain hacking and computer fraud. The theories are differential association theory, social control theory, techniques of neutralisation, rational choice theory, labelling theory and structural strain theory, as well as feminist critiques of criminology. The order in which these theories are presented reflect shifts in the perspectives of theorists, beginning with an emphasis on learning and social control, the interaction that offenders have with the criminal justice system, through to a analytical examination of the role of gender in relation to crime. This critical evaluation has been conducted by examining the key elements of the theories; how the theories have been tested in the past; how the theoretical concepts have been measured; potential weaknesses of the theories in their application to these particular types of crime; and valid criticisms of the theories that have been raised by the scientific community. The chapter concludes by discussing the practical implications of the theories, particularly how they can inform crime prevention methods and programs.

Theory selection

Garland differentiates between what he terms the “criminology of the self” (Garland, 1996, p. 461), whereby offenders are viewed as rational, calculating beings, and “criminology of the other” (Garland, 1996, p. 461), a more traditional, community-held, view whereby offenders are viewed as pathological. The theories selected for this research reflect “criminology of the self”, whereby
offending is acknowledged as a normal, everyday occurrence. As is discussed later in this chapter, the frameworks relating to “criminology of the self” and “criminology of the other” have implications for crime prevention initiatives and the role of the state in controlling crime. “Criminology of the self” explanations are favoured because, at the most basic level, crimes, and what behaviours are deemed to be criminal, are a social construct. This is particularly pertinent to computer crimes, which could not exist without the technology developments experienced by society in the last century, and particularly in the past few decades.

However, not every theory that could be included under the “criminology of the self” framework could reasonably be included in this research project. Therefore, some potentially interesting and informative theories have been excluded after careful consideration. These include Cohen and Felson’s (1979) routine activity approach, which proposes that predatory crime occurs when a suitable target is in the presence of a motivated offender and is without a capable guardian. Although one of the pillars of this theory relates to the supply of motivated offenders, the routine activity approach deliberately avoids any notions about criminal motivations (Clarke & Felson, 1993).

Agnew’s (1992) general strain theory was another explanation that was considered for inclusion in this study. Expanding on structural strain theory, general strain theory incorporates individual and emotional factors in response to experiences of strain (Agnew, 1992). However, structural strain theory was chosen for inclusion instead due to its focus on societal, rather than individual, factors. Similar reasoning explains why social control theory was favoured over
Gottfredson and Hirschi’s (1990) general theory, which includes a focus on the individual’s self-control.

The theories examined in this chapter were selected in order to focus on a number of different facets within society that are theorised to lead to offending. Differential association examines how crimes are learnt in association with others, social control theory focuses on the controlling influences of society, while techniques of neutralisation may be considered both a learning theory and a control theory as it incorporates what neutralisations may be learnt, and how these neutralisations may allow crimes to occur by loosening social control. Rational choice theory examines the likelihood of detection, the level of technical skills required or the level of anticipated benefit. The costs to offenders are not limited to the punishments meted out by the criminal justice system, but could also include feelings of guilt or shame, which may be mediated by the internet as offenders are not in physical contact with victims.

Labelling theory examines how those that are labelled as deviant behave in order to meet those expectations, while structural strain theory examines how people adapt when they are unable to meet the unrealistic goals set by society. Finally, the feminist critiques of criminology examine the gender ratio that is apparent for much criminal behaviour, and prompts theorists to incorporate into their explanations for offending.
Sutherland's theory of differential association

The key point from Sutherland’s theory of differential association is that criminal behaviour is normal behaviour learnt in interaction with others (Vold, Bernard, & Snipes, 2002). Differential association theory was designed to explain lawbreaking behaviour by the rich and the poor alike. Sutherland argued that theories that relate to poverty and the conditions related to poverty are “inadequate and invalid” (Sutherland, 1949, p. 5). This is because “…the theories do not consistently fit the data of criminal behaviour [and] the cases on which these theories are based are a biased sample of all criminal acts” (Sutherland, 1949, p. 5). Accordingly, Sutherland’s definition of crime included acts of deviance against society, not limited by the criminal code (Sutherland, 1949, p. 6).

Sutherland’s theory of differential association consists of nine specific points. Summarised, these points indicate that criminal behaviour is learnt in interaction with other persons in intimate personal groups. What is learnt includes both the techniques of committing crime, and “motives, drives, rationalisations and attitudes” (Sutherland, Cressey, & Luckenbill, 1992, p. 89) either favourable or unfavourable to committing crime. Crime is committed when those definitions favourable to committing crime exceeds those unfavourable to crime (Sutherland et al., 1992).

There are two basic elements of differential association. The first is the cognitive element, or the content of what is learnt, such as “specific techniques for committing crimes; appropriate motives, drives, rationalisations, and attitudes;
and more general definitions favourable to law violation” (Vold et al., 2002, p. 160). Sutherland did not specify the learning mechanisms, simply stating that “the process of learning criminal behaviour … involves all of the mechanisms that are involved in any other learning” (Sutherland et al., 1992, p. 90). The second element of differential association is the associations with other people in intimate personal groups where the learning takes place (Vold et al., 2002).

In explaining why different people exposed to the same social conditions may or may not conduct criminal behaviour, Sutherland claimed that it is the meanings that they give to these conditions that they experience that determines whether they violate the law. These meanings vary with the “frequency, duration, priority and intensity” (Sutherland et al., 1992, p. 89) of the associations with criminal groups. Sutherland supported this argument with qualitative research techniques (Vold et al., 2002).

Glueck and Cressey have stated that the theory of differential association cannot be tested (Vold et al., 2002). One criticism of the theory is that the meanings favourable to crime cannot be observed or measured (Matsueda, 1988). Another criticism lies with establishing whether criminal behaviour is caused by associating with criminal groups, or whether those who break the law are more likely to seek out others “whose values and behaviours are similar to their own” (Vold et al., 2002, p. 163). Also, as Burgess and Akers (1966) point out, Sutherland’s theory does not allow for the learning of behaviour that occurs in non-social situations, such as on television, reading from a book, etc. This is particularly important to this research, as it begs the question as to whether computer crimes can be learnt on the internet without social interaction.
On the other hand, Matsueda claims that the theory can be, and has been, tested (cited in Vold et al., 2002). He claims that while not all definitions favourable or unfavourable to crime may not be directly observable, or weighted to form a ratio, those that are support differential association (Matsueda, 1982). An example of such an indicator is a scale with responses ranging from favourable to unfavourable definitions of the legal code (Matsueda, 1982). Later Matsueda (1988) argued that: juveniles who report having more delinquent friends also report committing more delinquent acts; definitions favourable to law violation are associated with increased tendencies to engage in criminal and delinquent behaviour; legal defences to crime, such as self-defence and insanity, are definitions favourable to crime that are included in the law rather than excluded from it; and statistical techniques have found support for the complex casual structure in Sutherland’s theory, especially involving the ratio of definitions favourable and unfavourable to violating the law.

Examples of studies that have tested Sutherland’s theory of differential association have focussed on rural offenders (Clinard, 1944), group and solo offenders (Hochstetler, Copes, & DeLisi, 2002), juvenile delinquency (Hoffmann, 2002; Jensen, 1972; Matsueda, 1982; Matsueda & Heimer, 1987; McCarthy, 1996; Warr, 1993a, 1993b; Warr & Stafford, 1991), white collar crime (Piquero, Tibbetts, & Blankenship, 2005b), and whether differential association explains both criminal and non-criminal behaviours (Jackson, Tittle, & Burke, 1986). It is apparent that there seems to be some confusion as to how the concept “attitudes favourable to crime” is conceptualised. For example, Jensen (1972), Matsueda (1982; 1987), Matsueda and Heimer (1987) and McCarthy (1996) measured the
attitudes of the participants, while Piquero et al. (2005b) measured what participants perceived their peers’ attitudes to be, and Warr and Stafford (1991) and Hoffman (2002) measured both. Jackson et al. (1986) and Hochstetler et al. (2002) included the offending behaviour of respondents’ peers as indicators of their attitudes, while Warr (1993a, 1993b) did not measure attitudes favourable to crime at all in his studies to determine the relationships of parental influence and age with crime. Similarly, Clinard (1944) did not measure attitudes favourable to crime, but rather associations with criminal peers. Additionally, the absence of research including a time-ordered causal sequence is notable. In fact, the study by Piquero et al. (2005b) was the only one that attempted to do so, and the only study that did not use delinquency as its dependent variable, instead using a vignette concerning a hypothetical scenario in which participants indicated whether they would participate in white collar crime, as well as the perceived attitudes of their associates.

The study by Clinard (1944) was the only one included in this comparison that did not support some facet of differential association. Clinard (1944) concluded that crime committed by rural offenders was not explained by differential association, as these offenders typically did not associate with others engaged in similar behaviours.

Hollinger (1993), while not organising his study of software piracy and unauthorised computer account access around a theoretical perspective, included variables measuring participants’ friends’ involvement in these types of crime, as well as self-reported involvement. Hollinger (1993) found that as the number of friends who were involved in unauthorised access to computer
accounts increase, so did the likelihood that the participant would report partaking in this activity. However, Hollinger (1993) included only one measure of friends’ involvement, namely “How many of your best friends do the following at least occasionally?” (p. 10). Hollinger (1993) also did not measure attitudes favourable to this type of crime and did not establish the time ordering sequence.

Walkley (2005) examined how well differential association explained a number of computer crimes, including hacking and internet fraud. In her analysis Walkley (2005) mainly focussed, using open source data and previously reported findings, on whether offenders interact or operate in isolation, rather than what the interaction involved, such as learning definitions favourable towards committing crime. Despite noting that hackers communicate online using email, chat rooms and bulletin board systems (BBSs), at
defferences and by telephone (using phone phreaking), Walkley (2005) concluded that most hackers acted alone. Walkley (2005) also concluded that differential association could not be applied to all forms of fraud as some fraudsters operate solo.

18 Bulletin board systems, or BBSs, are personal computers that allow users to dial in using a computer and modem. BBSs are similar to online forums held on the internet, whereby users can leave messages for each other, as well as download and upload software (Chantler, 1995).

19 Parker (1998) describes a number of hacker conferences held in the United States of America and The Netherlands, which he claims are a place for hackers to brag, meet others, develop reputations, get drunk, use drugs, as well as increase their knowledge and skills. The main conferences are DefCon, held annually in Las Vegas; Hack Tic, held every four years in The Netherlands; the 2600 conference held annually in New York City; SummerCon, held annually in Atlanta; and HoHoCon, held around Christmastime in Texas (Parker, 1998). In Australia, Ruxcon is an annual computer security conference (Ruxcon Org, 2008). Holt (2005) states that attendance at these conferences is biased towards those who are willing to engage in social situations and can afford the cost of travel, accommodation and attendance fees, and that they are not representative of hacker activity.
Hirschi’s social control theory

Hirschi’s social control theory assumes that crime is a normal behaviour that occurs when controlling forces, such as social bonds, have been weakened (Vold et al., 2002). Hirschi theorised that people desisted from crime because of the bonds they had to social groups, such as family, school and peers. The four social bonds include: attachment to others, which results in sensitivity towards others’ feelings; commitment to society, which expends time, energy, money and emotions; involvement in conventional activities, which restricts crime opportunities; and moral beliefs, or the degree to which one agrees with the rules of society (Curran & Renzetti, 2001; Vold et al., 2002). While the four social bonds are theorised to be interrelated, in that those with bonds to society are likely to be bonded in more than one way, the social bonds have an additive effect, and it takes only the absence of one bond to result in criminal behaviour (Curran & Renzetti, 2001).

Many studies have supported the theorised effects of attachment to others and commitment to society in desisting from crime. However, less support has been found for involvement in conventional activities and desistance from crime. In fact, the opposite has been found, with those involved in conventional activities more likely to commit crime (Vold et al., 2002). In addition, there has been some contention as to whether measures of moral beliefs, such as “it is alright to get around the law if you can get away with it” (Vold et al., 2002, p. 187) are actually measuring weak conventional beliefs, or strong deviant beliefs. This distinction is important as social control theory states that “moral beliefs” bond people to society, thereby reducing criminal behaviour, while differential association theory
states that learning attitudes such as these through association with deviant peers leads to crime.

Kempf (1993) conducted a meta analysis of 71 studies testing social control theory that had been published between 1969 and 1991. Of these studies, 69 had used self-report survey data, while the remaining two had used official adult records and aggregate data. Only 17 studies included variables conceptualising all four of the proposed social bonds, with attachment to others being the most frequently included variable. Involvement in conventional activities was the variable that was included least often. One study justified this exclusion by claiming that the variable was too ambiguous, and others may have omitted the variable as Hirschi believed it to be of lesser importance. Overall, Kempf (1993, p. 153) stated that she found “the absence of arguments defending the omission of the other three elements of the social bond… perplexing”.

Kempf (1993, pp. 164-165) concluded that “different, and sometimes contrary, results were found… Higher levels of explanation were found for the general crime model, minor delinquency and school infractions”. Curran and Renzetti (2001) argue that the explanatory power of social control theory does not extend beyond juvenile delinquency, minor offending and misdemeanours. Given this limitation, the applicability of this theory to computer crime offences would be of some interest.

One criticism of the studies was that, like many of the studies testing other theories discussed previously, the studies reviewed by Kempf (1993) did not establish temporal order, therefore it is not known whether a break in social bonds pre- or postdates delinquency. Computer crime provides a prime example
of problems relating to establishing temporal order, as it is often characterised by physical isolation from others (Chantler, 1995). Therefore, are computer crimes committed because the offenders do not have bonds to society, or do they not have those bonds because they commit computer crime? Another criticism is that most of the studies involved young male participants and delinquency, with females, adults and racial minorities, along with other types of crimes, under researched (Kempf, 1993).

There is a body of research that compares Hirschi’s social control theory with learning theories, including Sutherland’s theory of differential association. For example, Matsueda (1982) reanalysed the data initially used by Hirschi (1969) to support and formulate his theory and found that differential association was supported over social control theory. Matsueda and Heimer (1987) also compared social control theory with differential association to test their strengths in explaining the relationship between race and delinquency and found differential association to be the stronger of the two.

The routine activity approach, which proposes that predatory crime occurs when a suitable target is in the presence of a motivated offender and is without a capable guardian (Cohen & Felson, 1979; Felson, 1998), will not be evaluated here in relation to computer crime offending. However, it is interesting to note that this theory offers an alternative explanation for the finding that computer crime offenders often come from broken families (Chantler, 1995). Instead of the assuming that this is an indicator that attachment to the family may not be present, the routine activity approach would explicate that a single parent family may have less supervision, or guardianship, therefore providing greater
opportunity for adolescent offenders, regardless of how well parent and child get along.

**Sykes and Matza’s theory of techniques of neutralisation**

Sykes and Matza’s (1957) theory of techniques of neutralisation is that offenders learn to use techniques to justify or neutralise acts that might otherwise produce feelings of shame or guilt, and distinguish between “appropriate and inappropriate targets for... deviance” (Sykes & Matza, 1957, p. 666). These techniques include to deny responsibility, to deny injury, to deny the victim, to condemn the condemners, and to appeal to higher loyalties (Sykes & Matza, 1957). Minor (1981, p. 298) claims that the neutralisation technique of denying the victim includes both “victims who are deemed to deserve their fate, such as homosexuals, members of minority groups, and crooked store owners [and] victims who are simply absent or unknown to the delinquent”.

Matza’s (1990) book, *Delinquency and Drift*, originally published in 1964, extends techniques of neutralisation he originally proposed with Sykes in 1957. Matza (1990) maintained that those that commit crime are not fundamentally different from those that do not; in fact they spend most of their time behaving in a law abiding way. Matza’s (1990) theory is that most delinquents drift in and out of crime, enabled by the loosening of social control. The conditions that make this drift to criminal behaviour possible include the use of the techniques of neutralisation.
Matza (1990) was particularly interested in explaining why people generally stop offending as they grow older, which he claimed was not adequately explained by other sociological theories. Therefore, his drift theory is particularly applicable to juvenile delinquency. As juveniles are uncommitted to their deviant behaviour they are free to drift between conventional and unlawful activities (Velarde, 1978). Matza (1990) clarified that the drifters, or juvenile delinquents, explained by his theory did not include all offenders, particularly those who are “neurotically compulsive” (p. 29) and those that develop commitment towards offending.

Minor (1980, 1981) contends that many tests of the theory of techniques of neutralisation are problematic on two counts. Firstly, measures of neutralisation techniques that have been used may also be measuring unconventional commitment. For example:

... respondents could agree with the statement “People should not blame Jack for shoplifting if this was the normal thing to do where Jack lived” if they thought that it was a good excuse or if they thought shoplifting was morally acceptable regardless of the excuse (Minor, 1980, p. 105; 1981, p. 296).

This distinction is important, because if crime or deviant behaviour is accepted due to unconventional attitudes, then neutralisation techniques are unnecessary (Agnew, 1994).

The second problem identified by Minor (1980, 1981) has already been raised when discussing the theory of differential association, and is a common problem when testing theories; namely, establishing the time-order effect. This is problematic as the theory maintains that neutralisation techniques precede, and thereby influence, criminal or deviant behaviour, while rationalisations occur
afterwards. Minor claims that his 1981 study was the first to overcome both of these limitations, by using longitudinal data and controlling for unconventional attitudes towards crime.

Nine studies published between 1980 and 2009 that tested Sykes and Matza’s (1957) theory of techniques of neutralisation were compared. Particular attention was paid to how, or if, the research determined causal ordering and controlled for general approval of crime and deviance. The difference in research methodologies was striking, with the first three studies, conducted between 1980 and 1994, all using a quantitative research design, specifically surveys with likert scale responses relating to a number of potential neutralisation techniques (Agnew, 1994; Minor, 1980, 1981). In comparison, the six studies published between 2003 and 2009 all used qualitative methods, including open-ended interviews, observations and analysing internet blogs (Cohn & Vaccaro, 2006; Copes, 2003; Cromwell & Thurman, 2003; Evans & Porche, 2005; Goode & Cruise, 2006; Turgeman-Goldschmidt, 2009) to identify and analyse techniques of neutralisation. These differences in methodologies may have had an impact on the research results.

Only two studies attempted to establish causal ordering, namely Minor (1981), who compared data collected in two waves, with a three month gap between, and Agnew (1994), who used data from two waves of a longitudinal study and compared techniques of neutralisation reported at time one with offending behaviour recorded at time two. Also, general approval of crime or deviance was included as a control variable on only four occasions (Agnew, 1994; Copes, 2003; Cromwell & Thurman, 2003; Minor, 1981). This was typically
measured by asking respondents to respond to items such as “How do you feel about…”, or “How wrong is it for someone your age to…”

Sykes and Matza (1957) argued that techniques of neutralisations were an extension of legal defences to crime, such as provocation or self-defence, which were seen as legitimate by those utilising them but not by the justice system. An interesting defence that has been raised by some defendants accused of computer-related crime, sometimes successfully, is that of addiction to computers, which they argued compelled them to act in the way that they did (Smith et al., 2004). Such an excuse would relate to the technique denial of responsibility posed by Sykes and Matza (1957).

McQuade (2006) states that neutralisation theory is a sound explanation for computer crime as the physical removal from the victim allows the offender to deny injury or deny the victim with ease:

Since they cannot see the Internet or the people who create content, victims, if they are contemplated at all, become faceless entities, computer systems, or perhaps corporations rather than real people whose livelihoods and wellbeing are compromised… (McQuade, 2006, p. 160).

Yar (2005a) also states that hackers’ self-purported motivations for offending, such as “intellectual curiosity, the desire for expanding the boundaries of knowledge, a commitment to the free flow and exchange of information, resistance to political authoritarianism and corporate domination, and the aim of improving computer security by exposing the laxity and ineptitude of those charged with safeguarding socially sensitive data” (Yar, 2005a, p. 391) may be forms of neutralisations aimed to overcoming guilt. Additional neutralisations proposed by Grabosky (2005) include blaming the victim as being deserving of
attack, claiming that no harm was done by looking at the data, that corporate
victims such as Microsoft could afford it, or claiming that everyone else did it.

The study by Turgeman-Goldschmidt (2009) involved in-depth interviews
with 54 Israelis who engaged in hacking, software piracy and phone phreaking to
determine whether they neutralised their offending behaviour. Turgeman-
Goldschmidt (2009) found evidence that these offenders: deny injury by claiming
that “downloading information is copying rather than stealing” (p. 325); deny the
victim by justifying their actions as revenge or targeting sites owned by the
‘enemy’, such as Nazis and Microsoft; condemn the condemners, such as those
who prevent access to the information that they are seeking; and appeal to
higher loyalties, especially the hacker ethic of freedom of information. However,
Turgeman-Goldschmidt (2009) found no evidence that these offenders engaged
in denial of responsibility.

In comparison, Walkley (2005) analysed techniques of neutralisation to
determine its explanatory power in relation hacking and internet fraud, concluding
that there was strong support for denial of responsibility and mixed support for
the other techniques of neutralisation. Using open source data Walkley (2005)
claimed that, when internet addiction, as a mental health problem, has been used
as a defence in court, the defendants were neutralising their actions by denying
responsibility. Walkley (2005) also stated that two defendants, who claimed that
their computer had been infected with a virus or trojan which had caused the
damage they were charged with, were also engaging in denial of responsibility,
 despite the fact that in both instances the defendants had been acquitted and
therefore were found not to have been responsible at all.
Clarke and Cornish’s rational choice theory

Rational choice theory assumes that offenders calculate the perceived costs and benefits of crime with the assumption that they seek some type of advantage from their actions, be it “money, sex or excitement” (Cornish & Clarke, 1987, p. 935). Clarke and Cornish’s rational choice theory looks at how offenders in particular situations make these calculations (Vold et al., 2002). The theory acknowledges that offenders’ perceptions of costs and benefits can be subjective, “…constrained as they are by time, the offender’s cognitive abilities, and the availability of relevant information…”, (Cornish & Clarke, 1987, p. 933), and therefore may not be rational at all (Akers & Sellers, 2004). Other “choice-structuring properties” (Cornish & Clarke, 1987, p. 935) are offence specific.

When offenders weigh up the type and amount of benefit likely against the perceived risk of detection and punishment, they take into consideration their skills and the skills needed to successfully commit the offence, and the availability of necessary equipment or situations (Cornish & Clarke, 1987). In addition, each of these considerations may not have equal weight. For example, a high likelihood of detection may be more influential in deterring crime than harsh punishments (Clarke, 1997).

A comparison was made of six studies published between 1989 and 2005 that tested rational choice theory. Four of these six studies used hypothetical scenarios involving illegal behaviours, namely drink driving, larceny and sexual assault (Nagin & Paternoster, 1993), sexual assault (Bachman, Paternoster, & Ward, 1992), corporate crime (Paternoster & Simpson, 1996) and tax non-
compliance (Klepper & Nagin, 1989). The study by Paternoster (1989) looked at juvenile delinquency, namely underage drinking, marijuana use, petty theft and vandalism and relied on self report data. Dugan, Lafree and Piquero (2005), on the other hand, compared data relating to the frequency and type of airline hijackings with the timing of counter-hijacking interventions that increased the cost and likelihood of detection.

These studies were examined to identify whether they included variables to measure the skills required to commit the behaviours being researched. This is because the theory states that the skills needed to commit the crime are taken into consideration when contemplating the costs and benefits of the act. None of the six studies included a measure of skill levels, however it may be assumed that the types of offences did not require a deep technical knowledge, as may be required for computer crime. Only the study by Paternoster (1989) included a measure of opportunity, asking whether respondents’ parents knew where they were when they were away from home, whether their parents knew who they were with when they were away from home, and of the people the respondent “hang out around”, how many committed the delinquent acts being researched.

Two of the six studies included a measure of benefits. Nagin and Paternoster (1993) manipulated the benefits in the hypothetical scenarios presented. For example, for the scenario involved drink driving the possible benefits changed when the distance between the bar and the home varied, as well as the inconvenience of returning to retrieve the car, which varied from getting a lift to having to catch a bus or walk. Participants were also asked “how much fun or a kick” (Nagin & Paternoster, 1993, p. 482) it would be if they were...
to commit the offence. The other study to include a measure of benefits was by Paternoster and Simpson (1996) in relation to corporate crime. Respondents were asked “how much of a thrill or how exciting it would be to commit the described act”; “how likely such an act would be to advance their career”; “financial gains such as saving money and increasing revenues”; and “non-financial benefits, such as providing the opportunity to legally challenge a suspect law” (Paternoster & Simpson, 1996, pp. 562-564).

All of the six studies included measures of both the respondents’ perceived likelihood of detection and the perceived harshness of punishment in the costs of committing crime. The measure of likelihood of detection included detection by police, the likelihood that the incident would be reported by the victim (in the case of sexual assault), and the probability of the matter being brought before the civil courts and other regulatory agencies. Measurements of punishment included criminal punishment, such as arrest and jail, punishment from other authorities, such as dismissal from university or school and diminished job prospects, punishment from family and friends, such as loss of respect, and punishment from the self, such as guilt, shame and other painful emotions.

In a study by McQuade examining students’ perceptions of being caught for a variety of technology enabled crimes, it was found that respondents believed that the likelihood of being detected was low, and that the punishment for those that were caught was not severe (McQuade, 2006). Hollinger (1993) measured university students’ perceived chances of being caught accessing a computer account without authorisation and found that self-reported involvement in this activity was not related to the perceived chance of being caught.
Becker’s labelling theory

There are two components of Becker’s labelling theory. The first, with its roots in critical criminology, examines what behaviours are defined as criminal, the groups that make these decisions, and against whom the rules are enforced (Paternoster & Iovanni, 1989). Becker (1963) claimed that much of the previous research into crime accepted the conventional view that it is deviant to break social rules, and that those who do so have a disposition towards crime. By doing this, the political process of how rules are created and enforced is ignored, and those who have committed the same deviant act are characterised together, without accounting for individual personalities and life situations (Becker, 1963). According to Becker (1963), because social groups make the rules, apply the rules and label those who break the rules as deviant, crime is created by society. Rather than sharing criminal dispositions, those who have been found to have broken the law share “the label and the experience of being labelled as outsiders” (Becker, 1963, p. 10), therefore explanations of crime should focus on the process by which people are labelled as criminals, and the result of that judgment.

The second component of Becker’s labelling theory, from the “symbolic interactionist tradition” (Paternoster & Iovanni, 1989, p. 363), examines the meanings of crime to the individual and to society. Becker stated that offenders, depending on the seriousness of the crime, may be considered by others to be “outsiders” (1963, p. 1), as they have broken a social rule. This labelling leads to a “self-fulfilling prophecy” (Einstadter & Henry, 2006, p. 224), in which individuals adopt criminal identities and subsequently reoffend. The labelling process may
involve numerous people and institutions, including, for example, parents, peers, teachers, courts, police officers, prison guards, welfare agencies and deviant peers.

In fact, someone associating with deviant peers may be labelled twice simultaneously: by their associates as well as by law enforcement agencies, who may target certain groups that have been known to commit crime in the past. Labelling theory competes with deterrence principles, as it sees the criminal justice system as creating more crime, rather than acting as a deterrent through its ability to punish (Tittle, 1995).

A major criticism of labelling theory is that it does not explain initial or undetected law breaking, rather it explains offending behaviour that occurs after the offender has been labelled as such (Akers & Sellers, 2004; Tittle, 1995). However, Einstadter and Henry (2006) claim that labelling theory explains both “primary” and “secondary deviance” (pp. 222-223). Primary deviance, or initial lawbreaking, occurs when the labelling process is directed at social groups, usually minorities and the powerless, while secondary deviance occurs as a result of the labelling of primary deviance (Einstadter & Henry, 2006). According to Paternoster and Iovanni (1989), the relationship between labelling and secondary deviance is not deterministic; rather labelling may increase the likelihood of recidivism.

Tittle (1995) states that the outcome of the labelling process may differ for different types of crimes. For example, the term ‘hacker’ could be considered to be a label in itself (Yar, 2005a); however, as also discussed previously, this term
has only recently begun to have negative connotations as previously it referred to
a skilled and innovative computer user or programmer.

Other criticisms of labelling theory raised by Tittle (1995) include a lack of
focus on other reasons for reoffending, such as opportunity, and that offenders
may actively seek to be labelled as criminal to “serve as tools of defence or
domination” (Tittle, 1995, p. 9). Paternoster and Iovanni (1989) counter the claim
that labelling theory does not account for these factors as the labelling process,
when conducted by a deviant audience, may increase secondary deviance by
“opening up deviant routines and opportunities” (p. 363). A critical audience and
lack of empirical support meant that the once popular theory was “pronounced
dead by 1985” (Paternoster & Iovanni, 1989, p. 359). However, Paternoster and
Iovanni (1989) claim that tests of the theory have been poorly designed and
conceptualised.

A comparison was made of 12 studies published between 1974 and 2008
that tested labelling theory in relation to gaining employment (Davies & Tanner,
2003), perceptions of abuse and neglect of children by their teen mothers
(Haynes-Lawrence, 2008), juvenile delinquency (Bernburg, Krohn, & Rivera,
2006; Farrington, 1977; Fisher & Erickson, 1973; Johnson, Simons, & Conger,
2004; Klein, 1974; Palamara, Cullen, & Gersten, 1986; Smith & Paternoster,
1990; Thomas & Bishop, 1984), adult offending (Bernburg & Krohn, 2003), and
drug use (Ray & Downs, 1986). All except two (Haynes-Lawrence, 2008; Klein,
1974) used longitudinal or time series designs, however researchers still found it
difficult to untangle the order of events (Thomas & Bishop, 1984).
All studies, apart from that by Haynes-Lawrence (2008) (a qualitative study that looked at the labelling process by social workers and did not include subsequent offending as a dependent variable), measured the effect of labelling by the criminal justice system. Examples of these measures included whether participants had been stopped by police, charged, convicted, sentenced or jailed (Davies & Tanner, 2003). Other formal labels included those by schools (Davies & Tanner, 2003; Thomas & Bishop, 1984), social workers (Haynes-Lawrence, 2008; Ray & Downs, 1986), mental health agencies (Palamara et al., 1986; Ray & Downs, 1986), and hospitals and drug and alcohol treatment programs (Ray & Downs, 1986). Only two studies measured participants’ self-concept, or how they viewed themselves after the labelling process. Thomas and Bishop (1984) included items such as “anybody who thinks I’m a bad person or a delinquent is just wrong” (p. 1233), while Ray and Downs (1986), who examined drug use, asked participants whether they identified themselves as a nonuser, experimenter, occasional user, regular user, drug abuser or addicted to drugs. Other informal labels included whether participants belonged to minority groups, such as race (Smith & Paternoster, 1990) or low socio-economic status (Johnson et al., 2004), how participants believed their parents perceived them (Ray & Downs, 1986) and deviant peer associations (Bernburg et al., 2006; Farrington, 1977; Johnson et al., 2004).
Merton’s structural strain theory

Merton’s structural strain theory, originally developed in 1938, is based on the premise that those who are unable to achieve culturally defined goals experience strain. Goals are culturally specific, for example, “the American Dream” (Merton, 1968, p. 190) of wealth, as are the approved means of achieving them, such as “hard work, honesty, education and deferred gratification” (Vold et al., 2002, p. 136). While society maintains that these goals are achievable by all, the social structure means that not everyone has equal access to the resources to achieve those goals, such as a good education and access to opportunities. Depending on their commitment to the goals and means, those who experience strain, usually members of the lower class, use one of the following five modes of adaptation: conformity, in which both the goals and means to achieve them remain important; innovation, in which goals remain important but the rules or the approved means of obtaining them do not; ritualism, which involves abandoning the goals due to their inability to be attained, and instead abiding by the institutional norms; retreatism, which involves rejecting the cultural goals as well as the means; and rebellion, which is rejecting the goals and means and substituting them with completely new ones (Merton, 1968).

Of the five modes of adaptation, conformity is the most common (Merton, 1968), while innovation, retreatism and rebellion are those that can lead to criminal behaviour. Innovation is considered to be the most important mode of adaptation for explaining crime (Vold et al., 2002). While still striving for their goal, such as wealth, offenders use innovative means to achieve this, such as
various forms of property or white collar crime that generate income (Merton, 1968). Retreatism is reportedly the least common type of adaptation (Merton, 1968). Retreatists drop out of, or escape from, society and potentially engage in criminal behaviour such as drug use. They are reportedly the “psychotics, autists, pariahs, outcasts, vagrants, vagabonds, tramps, chronic drunkards and drug addicts” (Merton, 1968, p. 207). Rebels, who substitute the culturally approved goals with alternative goals, may become criminally involved if associated with activities such as violent revolution or terrorism (Vold et al., 2002).

Einstadter and Henry (2006) note that many researchers analysing the theory have failed to agree on how to conceptualise concepts such as goals or means. For example, some researchers will measure goals as aspirations, while others see them as expectations; some will measure long term and general goals while others will focus on those that are short-term and specific (Einstadter & Henry, 2006). Similarly, means may be measured by changes, options or offers, or alternatively as resources, such as educational or skills (Einstadter & Henry, 2006). Studies that have failed to support structural strain theory have also been criticised for not including those who are most likely to be experiencing strain, such as the poor and those who are not at school (Baron, 2006). Another criticism of strain theory is that, while it is an appealing explanation of property crimes, it does not go far in explaining personal crimes such as assault (Einstadter & Henry, 2006).
A comparison was made of seven studies published between 1989 and 2006 that tested structural strain theory in relation to juvenile delinquency by high school students (Menard, 1995; Ozbay, 2003; Vowell & May, 2000), delinquency by youths at a high risk of offending (Baron, 2006; Farnworth & Leiber, 1989), adult offending (Burton, Cullen, Evans, & Dunaway, 1994), and telemarketing fraud (Shover, Coffey, & Sanders, 2004). Only the study by Menard (1995) categorised respondents into modes of adaptation, while the other studies instead looked at the direct relationship between strain and offending. Menard (1995) was also the only researcher who attempted to identify causal ordering, employing a time ordered cross sectional model. The only qualitative study was that by Shover et al. (2004), who interviewed 47 participants who had been convicted of telemarketing fraud. Shover et al. (2004) concluded that the offenders were innovators, that found fraud to be an alternative way to obtain their goals of financial success.

The studies reviewed typically conceptualised strain as adverse personal, familial and financial circumstances that impacted on the ability for participants to achieve their goals. These measurements are reflective of the means available to achieve culturally specific goals. However, it is noted that this conceptualisation departs from Merton’s original thesis that strain occurs due to a structural-cultural disjunction in that some social groups (particularly those that are already disadvantaged) are systemically denied access to socially sanctioned means for achieving approved social goals.

It is possible to envisage how the three modes of adaptation that could lead to crime can be applied to different types of computer crime. For example,
innovators, who aim to achieve goals by any means, could turn to computer 
frauds and other activities that may lead to financial gain. Similarly, rebels may 
be involved in hactivism and online sabotage, while retreatists, compelled to 
escape from the real world into the cyber realm, may become the “computer 
bums, compulsive programmers” (Levy, 1984, p. 125), entangling themselves 
within the ‘computer underground’ as they do so.

Walkley (2005) analysed structural strain theory to determine its 
explanatory power in relation to hacking and internet fraud, focussing only on the 
innovation and rebellion modes of adaptation. Walkley (2005) claimed that 
computer crime offenders who sought financial gain were innovators, despite no 
evidence to suggest that they had experienced strain. Walkley (2005) also made 
the plausible connection between rebellion and disgruntled employees who steal 
or damage their (former) employer’s information.

**Feminist critiques of criminology**

This research will consider two feminist critiques of criminology, 
particularly whether the theories that will be tested apply equally to females as 
well as males (the “generalisability problem”), and why males are more likely to 
commit crime than females (the “gender ratio problem”) (Daly & Chesney-Lind, 
1988, pp. 514-515). Most theories of criminal behaviour have been developed 
with male criminality in mind, and have been primarily tested on male participants 
(Smith & Paternoster, 1987). Concerns have been raised that by ignoring the 
gender aspect in explanations of crime, theorists may actually be overstepping a
key explanatory variable, that is, “the social construction of masculinity” (Einstadter & Henry, 2006, p. 264).

The concept of “gender” is understood to incorporate much more than biological sex differences between males and females (Daly & Chesney-Lind, 1988). Females not only have different chromosomes and sexual organs than males, but also, depending in the historical and social context, will experience life in a different way throughout their lifespan. For example, there is evidence that from an early age females experience different parenting styles than males and are expected to act less aggressively (Cowan, Cowan, & Kerig, 1993). In many countries females have only been granted suffrage in the past century (Ramirez, Soysal, & Shanahan, 1997), and in some jurisdictions women still do not have the right to vote. Even in Australia in the 21st century females experience a significant income gap compared to males, with females generally working fewer hours, holding fewer senior leadership positions, generating less income, and retiring with a smaller amount of superannuation (Cassells, Miranti, Nepal, & Tanton, 2009). There is also mounting evidence to indicate that males and females have very different experiences with the criminal justice system as victims as well as offenders.

Just as it has been noted that there is “geek mythology” (Margolis & Fisher, 2002, p. 67) relating to misconceptions about computer enthusiasts, Miller and Mullins (2006) discuss common stereotypes about the differences between males and females. It is important to be aware of these “gender-based assumptions” (Miller & Mullins, 2006, p. 220), which include psychological dichotomies such as rationality/emotionality, aggressiveness/passiveness and
instrumental/relational differences between the genders, rather than social differences in the construction of gender (Miller & Mullins, 2006).

While the gender ratio problem seems to be as pronounced in computer crime as it is in most other types of offending, it does not appear to be stable across types of computer crime offenses. For example, Chantler (1995) estimates that female hackers constitute one to three per cent of the hacker population, while almost one quarter of computer fraud is committed by female offenders (Internet Crime Complaint Center, 2009). It seems that the gender ratio problem, in relation to hacking, may be intensified with the lower numbers of females who engage in crime in general (Hayes & Prenzler, 2007), as well the lower number of females that participate in highly skilled computer activities (Margolis & Fisher, 2002). Understanding and explaining this gender ratio imbalance is beginning to be recognised as an important part of good crime theory (Miller & Mullins, 2006).

Simons, Miller and Aigner (1980) tested four of the theories that will be covered in this research, namely differential association, social control theory, labelling theory and structural strain theory, to determine if they explained female delinquency to the extent that they explain male delinquency. Interestingly, Simons et al. (1980) found all of the theories except structural strain theory predicted offending by females equally as well as they predicted male offending, and that the differences in offending rates were related to the differences between the genders in exposure to factors related to delinquency. Of the variables measured, females were less adversely situated than males in all aspects except occupational opportunity. Simons et al. (1980) noted, however,
that the theories do not explain why females are less likely to be exposed to aversive conditions than males.

Similarly, Smith and Paternoster (1987) tested the ability of social control theory, differential association, structural strain theory and rational choice theory to explain marijuana use by female as well as male high school students. Their findings supported those by Simons et al. (1980), in that females had lower levels of exposure to the factors that are related to deviant behaviour. A study by Alarid, Burton and Cullen (2000) to test the ability of social control theory and differential association to explain criminal behaviour by incarcerated serious offenders found that, while both theories were supported, parental attachment was a stronger predictor of female offending, and differential association was a stronger explanation of male offending. A further study by Piquero, Gover, MacDonald and Piquero (2005a) into juvenile delinquency indicates that males may be more likely affected by delinquent peers than females.

One way that feminist critiques may assist with our comprehension of computer crime offending is a greater understanding of the different opportunities that males and females have to develop peer relationships with other offenders. Females may have fewer opportunities or less exposure to delinquent peer relationships than males. Research to date indicates that many hackers do work together to some extent, both in off- and online environments (Chantler, 1995; Meyer, 1989), and that some may lack the social skills to make friendships outside of the hacking environment (Chantler, 1995).

Less is known about whether females embrace the opportunity to hide their gender when hiding behind the anonymity of the online environment,
although research suggests that internet users are likely to represent their true
gender on online gaming communities and social media sites (Huh & Williams,
2010; Schultze & Leahy, 2009). In addition, worldwide, females are less likely to
be connected online than males, although the gender/digital divide is most
pronounced in developing nations (Watson Kakar, Hausman, Thomas, Denny-
Brown, & Bhatia, 2012). As this gender/digital divide decreases it may allow
females greater access to work and income potential, as well as increase
exposure to illegal online behaviours.

**Theory and practice: Implications for crime prevention**

Criminological theory has important applications in relation to informing
crime prevention programmes (Mazerolle, 2009). On a broad level, if the cause
of crime is societal, than the use of individual rehabilitation will fail (Garland,
2001). Crime prevention techniques that use the “criminology of the self”
(Garland, 1996, p. 461) framework focus on the responsibilisation strategy, which
emerged as the state has acknowledged that it cannot claim primary
responsibility for crime control (Garland, 1996). Instead, rather than focusing on
punishing offenders, the focus of punitive policies, or fixing the causes of crime,
which has become unpopular since the perceived failure of the welfare strategy,
the responsibilisation strategy moves towards minimising the effects of crime and
implementing crime prevention policies that are supported by research findings
(Garland, 1996). As a result of the responsibilisation strategy the state has
become more powerful by “governance-at-a-distance” (Garland, 1996, p. 454),
which consists of empowering and encouraging private companies and citizens
to undertake crime control to take responsibility for themselves and their property. Governance-at-a-distance is complemented by the neo-liberal principles of a market-based economy, efficiency, and effectiveness (O'Malley, 1999). These views, and the subsequent policies, mirror the framework developed by rational choice theories and situational crime prevention (Garland, 1996, pp. 450-451).

The recurring message of the responsibilisation strategy is that the state cannot be solely responsible for controlling crime (Garland, 1996). It follows that a strong state would not fear the electoral backlash for acknowledging this, which supports Garland’s view that punitive policies are an indication of a weak government (Garland, 1996). A weak state refuses to admit this inability to control crime and instead attempts to reassert its power by promising heavy punishment of offenders (Garland, 1996), thereby resorting to punitive policies to win votes (Hough, Roberts, Stalans, & Indermaur, 2003). Punitive policies pathologise criminals, which is represented by Garland’s “criminology of the other” (Garland, 1996, p. 461). Using this view of criminality harsh sentencing policies are seen to be commonsensical, as lengthy incarceration takes these offenders “out of circulation” (Garland, 1996). O’Malley (1999) links punitive policies with the political stance of neo-conservatism whereby the state is perceived to be the preserver of law and order.

While the responsibilisation strategy can be applauded for valuing evidence-based strategies, de-demobilising criminals and allaying fears about crime, Garland (1996) rightly points to the existing divisions of social class, and how the franchising of crime strategies could negatively reinforce these. Under
the responsibilisation strategy crime control has the capacity to become a commodity rather than a public service, available only to those who can afford it. This could be at the expense of those who already suffer the most, as lower social classes would not only be unable to protect themselves against current levels of victimisation, but their disadvantage may be compounded as a result of the limitation of situational crime prevention to move offending to more accessible targets.

Meanwhile, punitive policies have enduring effects on members of the community that are caught within the criminal justice system. These are more likely to be those who already occupy a marginalised position within society, such as those belonging to racial minority groups or a lower socio-economic class (Hough et al., 2003). This may not necessarily reflect higher offending within these populations, but rather increased policing and/or heavier sentencing brought about by punitive policies.

All of the theories discussed in this chapter have been applied to crime prevention in one way or another, with varying levels of success. For example, social control theory lends itself to crime prevention efforts that strengthen the bonds between the individual and their family, school and neighbourhood (Gilling, 1997). Crime prevention informed by learning theories look at changing the attitudes about crime held by groups, rather than individuals (Cressey, 1955).

Merton’s structural strain theory, which identifies the disjuncture between the goals set forth by society and the means by which individuals had to achieve these, provides two options for crime prevention. The first option is to provide more opportunities to achieve culturally specific goals, such as education and
employment, while the second option is to change the culturally specific goals. For example, “the American Dream” of wealth and prestige is unachievable for many, therefore it has the potential to be replaced with another, more realistic, goal (Gilling, 1997).

As mentioned previously, the implications of labelling theory and rational choice theory are at odds. Crime prevention efforts that use labelling theory as their framework aim to make the formal criminal justice system more tolerant, enabling offenders to be diverted to a less detrimental or stigmatising system, therefore lessening the likelihood that they will reoffend (Gilling, 1997). On the other hand, rational choice theory lends itself to crime prevention policies that increase the costs of committing crime and decrease the benefits, such as increasing the probability of being caught and make committing crime harder (Gilling, 1997), as well as the use of harsh penalties as a deterrent (Garland, 2001).

Contemporary criminological theories, such as rational choice theory and the routine activity approach, do not see the answer to reducing crime in changing the morality of people or society, but rather in changing the situation in which crime occurs (Garland, 2001). A potential implication of such crime prevention techniques on the internet is not promising due to the wide expanse of cyber space and the ease in which potential victims and offenders can interact. Offenders do not have to physically relocate in order for crime to be displaced to more vulnerable targets (Broadhurst & Grabosky, 2005).
Conclusion

This chapter has set out some of the possible explanations of computer crime as informed by sociological theories. The theories discussed here are an important part of this research. These theories provide policy makers and practitioners with a framework to view and understand crime and respond appropriately. A summary of the theories, along with their key constructions, is provided in Table 3.

Table 3
Summary of the Theories and their Key Constructs

<table>
<thead>
<tr>
<th>Theory</th>
<th>Key constructs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sutherland’s theory of differential association</td>
<td>Definitions favourable to criminal behaviour</td>
</tr>
<tr>
<td></td>
<td>Associations with others who have definitions favourable to criminal behaviour</td>
</tr>
<tr>
<td>Hirschi’s social control theory</td>
<td>Attachment to others</td>
</tr>
<tr>
<td></td>
<td>Commitment to society</td>
</tr>
<tr>
<td></td>
<td>Involvement in conventional activities</td>
</tr>
<tr>
<td></td>
<td>Moral beliefs</td>
</tr>
<tr>
<td>Sykes and Matza’s theory of techniques of neutralisation</td>
<td>Denial of responsibility</td>
</tr>
<tr>
<td></td>
<td>Denial of injury</td>
</tr>
<tr>
<td></td>
<td>Denial of the victim</td>
</tr>
<tr>
<td></td>
<td>Condemn the condemners</td>
</tr>
<tr>
<td></td>
<td>Appeal to higher loyalties</td>
</tr>
<tr>
<td>Clarke and Cornish’s rational choice theory</td>
<td>Benefits of crime</td>
</tr>
<tr>
<td></td>
<td>Costs of crime</td>
</tr>
<tr>
<td></td>
<td>Likelihood of detection</td>
</tr>
<tr>
<td></td>
<td>Severity of punishment</td>
</tr>
<tr>
<td>Becker’s labelling theory</td>
<td>Labelling by the criminal justice system</td>
</tr>
<tr>
<td></td>
<td>Other formal labelling</td>
</tr>
<tr>
<td></td>
<td>Informal labels</td>
</tr>
<tr>
<td></td>
<td>Self-concept</td>
</tr>
<tr>
<td>Merton’s structural strain theory</td>
<td>Goals</td>
</tr>
<tr>
<td></td>
<td>Means</td>
</tr>
<tr>
<td></td>
<td>Strain</td>
</tr>
<tr>
<td>Feminist critiques of criminology</td>
<td>The generalisability problem</td>
</tr>
<tr>
<td></td>
<td>The gender ratio problem</td>
</tr>
</tbody>
</table>

87
As stated by Garland (2004, p. 165) “the purpose of theory is the development of knowledge and understanding of the world. And to serve that purpose, it must be put to work”. The discussion of the theories covered in this chapter has informed the research design and data collection set out in the following chapter. The theories have been tested in this research to determine whether they explain computer crimes that compromise data and financial security. To this end this chapter has discussed the strengths and limitations of these theories, as well as their contradictions and compatibilities. The proposed analysis of the data will then feed back in determining which theories, or part thereof, provide an understanding of computer crime offending. For example, in relation to the feminist critiques of criminology, this research will highlight whether the theories explain male and female offending, as well as possible explanations as to why the majority of offenders are male.
Chapter 4 ~ Research Questions and Design

This chapter sets out the research questions, as well as the research design that has been applied to answer these questions. The discussion of the research design will focus on the various studies that have been conducted, including the methods, research subjects, ethical considerations, data analysis and issues relating to reliability and validity.

Research questions

This research critically evaluates a variety of existing theories of criminal behaviour to determine whether they explain computer crime offending. The key aim is to develop a theoretical understanding of computer crimes that compromise data and financial security, including offender initiation, maintenance and desistance, with a view to establishing one integrated theoretical model. The questions for this research are:

1. How well do existing theories of criminal behaviour account for computer crime?
2. Is a new theoretical model needed to better explain computer crime?; and
3. What should an integrated model look like?
Question two, whether a new theoretical model is needed to better explain computer crime, is two-fold. It first examines whether the theories tested are adequate in their explanation of these types of crimes. It was expected that each theory would provide a unique insight into offending, allowing for these theories to be integrated to develop a more comprehensive explanation, so that there are not many divergent theories explaining the one behaviour.

Research design

The research questions have been answered using qualitative analysis to assess these theories of crime and develop an integrated theory of computer crime. The qualitative analysis consists of three separate studies: an analysis of court documents, interviews with law enforcement officers, and interviews with active and former offenders. The existing theories of crime to be applied to explain hacking and computer fraud were critically evaluated to identify the key themes of the theories and their operational definitions. These conceptualisations informed the interview schedules attached at Appendices E and F and the codebook attached at Appendix G.

The units of analysis for this research are the offenders who attempt or perpetrate computer crimes that compromise financial and data security. A qualitative research design was selected for its ability to provide a deeper understanding of offending behaviour than may be achieved through a quantitative design (Mazerolle, 2009). Qualitative research captures nuances and provides richness to data that may not otherwise be quantifiable. In addition, qualitative research can be undertaken when the ability to meet the quantitative
requirements in relation to obtaining a large, randomly selected sample size are less than ideal (Berg, 2007). An overview of the three studies will be provided in remainder of this chapter, as well as a discussion of the ethical considerations, proposed analysis, reliability and validity considerations and limitations of the research design.

**Study one: Analysis of court documents**

Study one consisted of analysing sentencing remarks and court judgments relating to 54 prosecutions involving computer fraud and hacking offenses in Australia, the United Kingdom, the United States of America and Canada. Multiple jurisdictions were selected in order to increase the sample size. Smith et al. (2004) identified 77 cases involving 92 offenders who had pled or had been found guilty in the above jurisdictions from 1972 to 2003 for hacking and/or computer fraud related matters. Those documents that were available on public databases were identified and re-examined. A systematic review of legal databases was conducted to identify additional relevant cases and any appeals of the identified cases that contained further information. The systematic review involved a monthly review of the following online databases to identify relevant cases:

- A.C.T. Supreme Court;
- District Court of Western Australia;
- South Australia Courts Administration Authority;
- Supreme Court of Queensland Library;
- Supreme Court of Tasmania;
• Supreme Court of the Northern Territory; and
• Supreme Court of Western Australia.

When sorted by type of offence, 44.4 per cent (n=24) had committed a fraud offence, 27.8 per cent (n=15) had committed a hacking offence, and the remaining 27.8 per cent (n=15) committed offences that could be classified as both hacking and fraud. Table 4 shows the number of cases that can be classified as hacking, fraud or both by jurisdiction.

Table 4

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Hacking</th>
<th>Fraud</th>
<th>Both hacking and fraud</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australian Capital Territory</td>
<td>1</td>
<td>-</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>New South Wales</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>New Zealand</td>
<td>1</td>
<td>-</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Northern Territory</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Queensland</td>
<td>1</td>
<td>2</td>
<td>-</td>
<td>3</td>
</tr>
<tr>
<td>South Australia</td>
<td>2</td>
<td>-</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Tasmania</td>
<td>1</td>
<td>9</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>United States of America</td>
<td>-</td>
<td>3</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Victoria</td>
<td>-</td>
<td>5</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>Western Australia</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>15</strong></td>
<td><strong>24</strong></td>
<td><strong>15</strong></td>
<td><strong>54</strong></td>
</tr>
</tbody>
</table>

There were 353,414 words included in the analysis for study one, an average of 6,544 per case. The members of the judiciary proceeding over the matter authored all documents. As well as outlining the facts of the matter, the nature of the harm caused, and details about the lead up to the offence(s), such as how the offence came to be and the involvement of others, the documents typically included factors of relevance when sentencing offenders, including mitigating and aggravating circumstances. Within Australia sentencing statutes
are applicable in each jurisdiction that set out what these factors may be. These typically include the offender’s criminal history, their level of remorse, their attitude and the level to which they cooperated with the criminal justice system, the effect that various punishments may have on the offender and the family, such as the ability to maintain employment (Edney & Bagaric, 2007).

**Study two: Interviews with law enforcement officers**

Study two consisted of interviews with law enforcement officers within computer crime or fraud specialist units from four policing agencies in Australia, namely the Queensland Police Service, Western Australia Police, Victoria Police and the Australian Federal Police. These interviews focussed on officers’ perceptions of, and experience with, offenders who have been identified by the criminal justice system. The interviews were one-on-one, open-ended, semi-structured and based on the operationalisation of the theoretical concepts that were identified during the critical examination of prior studies and meta-studies that had tested the theories pertinent to this research. Further questions were then asked in order to delve into areas of particular interest to gain a more complete understanding of the subject matter. Some questions tapped into more than one concept. The interview schedule, which was used to help guide the interview process, is attached at Appendix E. The questions were grouped together under common themes, such as family, educational experience, friendships, however the interview schedules do not necessarily represent the order in which the questions were asked.
Participants were asked about their experiences with offenders within the last five years. It was expected that recall would be fairly accurate given the limited number of cases available. It was considered appropriate to gather information using law enforcement officers as third parties due to the nature of the offender population, which is generally considered to be hard to access. Gathering data from third parties is consistent with prior research relating to offenders, for example, the Cambridge Study in Delinquent Development, which included interviews with parents and questionnaires completed by teachers (Farrington, 1989). The 15 law enforcement officers interviewed in study two included 14 males and one female. The interviews ranged from 32 minutes to one hour and 16 minutes in length, with an average time of 51 minutes.

The participating law enforcement agencies contacted the relevant law enforcement officers within the specialised computer crime or fraud units to seek their consent to disclose their personal details to the researcher, or provided them with the contact details so that they could contact the researcher directly. The researcher travelled to the relevant jurisdiction to conduct the interviews for the face-to-face interviews. The participants in study two had been employed with the law enforcement agency for an average of 13.6 years, and had spent an average of 3.5 years within the specialised computer crime or fraud unit. Eleven interviews were conducted face-to-face and four by phone. The participants were cooperative and did not appear to try and deceive the researcher.
Study three: Interviews with active and former offenders

Study three consisted of face-to-face interviews with active and former offenders. Participants were sampled using snowball sampling, a non-random, purposive method. Initial recruitment used informal networks. Those known to the researcher who worked and/or studied in the IT industry were encouraged to source participants. The benefit of such an approach is that recruiters are able to assure potential participants that the researcher is legitimate (Wright, Decker, Redfern, & Smith, 1992). Participants were also encouraged to approach additional potential participants. Recruitment consisted of advising potential participants about the research and what is entailed and providing the contact details of the researcher. In this way participants self-identified as being a member of the target population and, by having the participant contact the researcher, means that they were in control of the amount of personal information that they provided. Participants were offered a gift voucher for EB Games, a national chain of electronic gaming stores, to the value of $30 as a thank you for being interviewed. Ethical considerations taken into account when selecting this amount related to the amount of time participants would be devoting to the interview, as well as what might be considered coercive, in that a high value may have encouraged participation by those who otherwise may not have agreed to be interviewed (Australian Research Council, 2007).

Studying active offenders has many benefits over studying a prison sample as active offenders may be characteristically different in their frequency, nature and severity of offending, as well as their skill levels and abilities.
Studying offenders in their natural settings constitutes traditional criminological research. For example, Sutherland and Cressey state:

Those who have had intimate contacts with criminals “in the open” know that criminals are not “natural” in police stations, courts, and prisons, and that they must be studied in their everyday life outside of institutions if they are to be understood… In this way, [s]he can make observations on attitudes, traits, and processes which can hardly be made in any other way. Also, [her] observations are of unapprehended criminals, not the criminals selected by the processes of arrest and imprisonment (Sutherland & Cressey, 1974, pp. 67-68).

The sample size was determined by adhering to the principal of theoretical saturation. This guideline indicates that the sample size is adequate for qualitative research when it has reached the point that no new information or themes are being observed in the data (Guest, Bunce, & Johnson, 2006). Kvale (2007) advises that qualitative interview studies commonly have sample sizes of around 15 participants, plus or minus 10, and that many larger studies would actually benefit from a smaller sample with greater attention to the analysis. Christie (1997) differentiates between “near data”, which includes information pertaining to a small number of participants while providing thousands of insights, and “distant data”, such as large datasets from official records, which may contain thousands of cases but provides little in-depth understanding. Of the seven offenders who participated in study three, five identified as hackers and two as both hackers and fraudsters. Five were active offenders and two identified themselves as former offenders.

The interview schedule was a modified version of McAdams’ (2008) *Life Story Interview* with additional questions based on the operationalisation of the theoretical concepts. A copy of the interview schedule is included at Appendix F.
Wright and Bennett (1990) support the use of semi-structured interviews with offenders, stating that they “...avoid imposing artificial concepts and categories on subjects, thereby letting them speak freely using their own terminology” (p. 142). Participants were first asked whether they have been involved with hacking, computer fraud, or both, and whether they identified themselves as current or former offenders. The answers to these questions allowed the interviewer to tailor the rest of the interview to the participant, and assisted with later analysis. For example, former offenders were asked additional questions as to why they ceased offending, as well as what their situation was at the time that they were offending. Interviews were recorded and transcribed verbatim by the researcher, with any identifiable information replaced with pseudonyms. The interviews ranged from 45 minutes to two hours and 18 minutes in length, with a mean time of one hour and 39 minutes.

With the researcher vouched for, the participants were cooperative and obliging. They appeared to be truthful and forthcoming during the interviews. All the interviews were conducted in public places chosen by the participant, typically a coffee shop. While at the beginning some of the participants seemed tense or unsure of what was expected of them, by the end of the interviews they had all relaxed and opened up.

**Ethical considerations**

Ethical clearance was granted for this research. The research was conducted in accordance with the approved protocol. A number of potential ethical considerations arose out of the research design, including potential harm.
to participants and the researcher, researching illegal behaviour, maintaining confidentiality and anonymity, and keeping data secure. As the interviews in study three covered aspects such as home life, upbringing, friendships, social activities, etc., there was the potential for some level of psychological harm to participants (for example, remembering or talking about a bad experience). To minimise this risk participants were provided with the details of freely available psychological services that they could contact. Participants were also able to withdraw from the study at any time.

There was also the potential risk of harm to the researcher while interviewing participants face-to-face. To minimise this risk interviews were conducted in a public area. The researcher's principal supervisor was advised when and where interviews were to take place and when they had been concluded. The researcher also kept a mobile phone on her person during interviews. Face-to-face interviews were conducted rather than an online questionnaire, which could have become a target for hackers, and therefore a security risk. In addition, there was the potential that respondents would be concerned that their IP address would be recorded in an online environment.

The researcher determined an appropriate course of action if faced with information concerning offences that were in progress, offences that were intended to be committed, or if court ordered or subpoenaed to provide evidence about participants. While the research involved people that had engaged in illegal behaviour it did not relate to the specifics of individual events, nor was it intended to expose legal behaviour. However, there was the potential for the researcher to be told about current illegal activities or those that involve serious
harm. While the researcher was not under any contractual, professional or legal obligation to disclose illegal behaviour, there was a moral question to consider relating to elective disclosure. To mitigate this risk to participants, they were informed at the beginning of the interview that they should not divulge any current activities, and they would be reminded of this if they begin to do so.

There was a possibility that the researcher may be compelled by law enforcement or a court to disclose information. However, as the data were not collected in an identified form and remained anonymous the researcher could not disclose any identifiable information about any participants if such a circumstance arose. This means that it would have been difficult for a law enforcement or other agency to identify that data with an individual. This technique is consistent with other research relating to self-reported criminal behaviour (Israel, 2004).

**Analyses**

Coding of the data was mainly “concept-driven” (Gibbs, 2007, p. 44), in that the codes used primarily arose from the literature. Key theoretical concepts and how these have been measured previously were identified in the critical evaluation of prior studies that tested the existing theories of crime, and the data that were collected from interviews and court documents were coded in accordance with these concepts. The codebook is attached at Appendix G. “Data-driven coding” or “open coding” (Gibbs, 2007, p. 45) was also utilised when other key themes arose during analysis. NVivo, a qualitative data analysis program, was used to classify and sort the data according to the codes applied to see how the data represented the theoretical frameworks.
Reliability, validity and reflexivity

This section will address some of the possible limitations of this part of the research design relating to reliability, validity and reflexivity, and how the researcher attempted to overcome these, where feasible.

It is possible that the data obtained are not an accurate depiction, i.e. that the information provided is not truthful or valid. This may occur because the participant had trouble with recollection, misinterpreted the question or preferred not to give an honest answer. It may be asked how the researcher can believe the accounts of those who, due to the subject matter, may be untrustworthy. However, Wright and Bennett (1990) have examined the literature relating to the truthfulness of accounts given by offenders during qualitative interviews. They conclude that much information provided during interviews is consistent with official records, and that, after agreeing to be interviewed, offenders perceive lying to be pointless as they may as well not have consented at all. In addition, during the interviews with active and former offenders, time was spent checking for distortions and exploring the participants’ responses with them to seek clarification. Some questions were also asked in more than one way in order to compare the responses. For example, the questions "how did you choose the target(s) that you did" and “what type of target do you avoid” are both aimed at examining the applicability of rational choice theory in relation to risk, reward and difficulty levels.

The validity of the research design is also improved by triangulation (Gibbs, 2007). The different sources of data and theories being tested allowed
for two types of triangulation, namely “triangulation of measures”, as there are
different methods of data collection, and “triangulation of theory”, as multiple
theoretical perspectives have been employed (Neuman, 2006, pp. 150-151).

As only one researcher coded the data it is not necessary, to demonstrate
inter-rater reliability. However, to strengthen internal reliability an associate, who
is not connected to this research project, agreed to code a sample of the non-
identifiable data so that it could be cross-referenced with the researcher’s coding.

Another problem with reliability may be “definitional drift” (Gibbs, 2007, p.
98), where the meanings of codes may change over time. Gibbs (2007) suggests making notes about all the possible meanings of each code to enable a
more reliable and stable coding system. Gibbs (2007) also suggests comparing
one data source to others during coding to ensure consistency and accuracy,
investigating negative cases and exploring alternative explanations to improve
the reliability of the research findings.

Gibbs (2007) also raises the question of reflexivity in relation to qualitative
research. Reflexivity refers to the preconceptions and effects the researcher
brings to the study, for example, preconceived notions of what the research will
find, which may affect how questions are asked, or biases and experiences
towards the subject being researched. Reflexivity has gained much attention in
qualitative studies, however this challenge to objectiveness may also be applied
to quantitative research designs (Gibbs, 2007). Reflexivity may also change
during the research project, as the researcher’s interpretations and
understandings adjust to the phenomenon being studied. Gibbs (2007, pp. 92-
93) provides some suggestions for “reflexive good practice”, including critically
assessing the data and biases held by the researcher, being explicit about any theoretical models and the assumptions that these may hold in relation to broader values, discussing what decisions were made and why, and avoiding over-simplification of the data.

**Limitations of the research design**

The previous section reviewed some of the caveats relating to reliability and validity. However, it is noted that other limitations may arise due to biases within the research design. For example, as noted by Smith et al. (2004), the limitations of using court documents include the fact that many matters are heard in the lower courts where judgments may not be published, and that it is difficult to determine which matters involve computer crime due to the classification of offenses. Another limitation that is relevant to study one is that cases brought before the courts are unlikely to be representative of the larger population of hackers and computer fraudsters who are not apprehended or prosecuted. This limitation was mitigated by the inclusion of study three.

The sample of active and former offenders was not chosen at random; therefore it may be argued that the participants are not representative of the offender population. In addition, those who agree to be interviewed may differ from the typical offender. However, although this sample is not likely to include offenders who have worked for, or are part of, a terrorist organisation or organised crime syndicate, it may include more mainstream offenders who, collectively, may cause significant damage or fear of victimisation. This limitation
was also minimised by comparing offenders who have been identified by the criminal justice system and those who have not.

The final limitation that will be raised here is determining the time-order sequence. This was identified as being a major limitation of many prior studies examining the theorised causal explanations of crime. It is acknowledged that the best way to test the causal ordering is a longitudinal design; however this is not feasible for the current study. Instead, an attempt to overcome this limitation was made by asking respondents who identify as former offenders to think back to when they were engaged in hacking or computer fraud and recount those experiences during the interview. For example, former offenders were asked “what was your employment status at the time you were engaging in hacking/fraud”, while current offenders were asked whether they are presently employed.

**Development of a new theoretical model of computer crime**

The final part of the project was the development of an integrated theory that contributes to our understanding of computer crime. It was identified that a number of outcomes were possible, namely that one or more theories may have contributed much to the understanding of computer crime, none of the theories may have been good explanations, or components of theories may have provided insights into why offending occurs. However, as stated by Akers and Sellers (2004, p. 267), “a modicum of truth can usually be found in each theory”. This allows for the development of integrated theory, which refers to the integration of existing theory to create a more comprehensive explanation (Tittle,
Theory integration may involve merging compatible aspects of the theories, or even competing theoretical claims, such as explaining the differing effects of criminal justice system intervention on subsequent offending put forward by rational choice theory and labelling theory (Tittle, 1995).

It was possible that none of the theories would provide a good explanation for computer crime offending. In this case, a grounded theory, which refers to theory generation arising from the qualitative observations that have taken place (Maxfield & Babbie, 2005; Neuman, 2006), would have been developed. The use of qualitative data allows for “a deep understanding of phenomenon, events, people, or organizations” (Berg, 2007, p. 285), which is ideal for informing theory.
Chapter 5 ~ Demographics

Parker, an information security specialist who has interviewed a number of hackers, states “the only common factor among hackers is the use of personal computers and modems connecting them” (1998, p. 170). Despite this, research, including Parker’s own, indicates that hackers possess some commonalities, such as age and gender. It is important that our understanding of the demographics of offenders is based on empirical research as it is noted that there are many romantic stereotypes about hackers, most likely generated by the popular media. Margolis and Fisher (2002) caution against continuing any misconceptions about computer enthusiasts, which they call, somewhat humorously, “geek mythology” (p. 67).

This chapter compares the research findings for hackers and fraudsters in relation to gender and age. In doing so, this chapter will address the possibility that those involved in computer fraud do not share similar characteristics with hackers. For example, Hayes and Prenzler (2003) state that the number of general fraud offences committed by the elderly and females may be increasing, while it seems that hacking continues to be committed by young males. This chapter explores the possibility that females may have less opportunity to develop peer relationships and become accepted by the hacker community. This chapter also includes an analysis of offenders’ social economic status and their country of origin.
Gender

From all accounts it appears that hacking is predominantly conducted by males (Chantler, 1995; Jordan & Taylor, 1998; Parker, 1998; Taylor, 1999; Turgeman-Goldschmidt, 2005). For example, Taylor (1999) states that the gender ratio at hacking conferences is approximately one female to every hundred males, and that often females are only transiently involved in the hacker subculture while dating a hacker. Hollinger’s (1993) study of college students found that 5.2 per cent of males and 1.8 per cent of females admitted to having accessed another’s computer account or files without permission. Interestingly, Skinner and Fream’s (1997) research examining music piracy and unauthorised computer access by a student population indicated that 13.6 per cent of females sampled admitted to guessing passwords, 9.5 per cent admitted to accessing a computer account without permission to browse files and 2.3 per cent admitted to adding, deleting, changing or printing information in another’s computer file without the owner’s knowledge or permission. The percentage of males admitting to the same behaviours was 25.2, 22.7 and 10.5 respectively. However, Skinner and Fream (1997) purposely sampled students from university courses where students were required to have a high level of computer expertise, therefore the high involvement in these activities, particularly by females, may not be generalisable. Supporting the earlier statement that computer fraud offenders may have different characteristics than hackers, the American Internet Crime Complaint Center (Internet Crime Complaint Center, 2009) reported that of the computer fraud complaints received in 2008 where the gender of the offender was known, 22.6 per cent of complaints involved females.
Table 5 provides a gender breakdown of the study one participants by offence type. It is noted that these are small samples and therefore percentages are prone to fluctuations. Of the 12 female offenders, 8.3 per cent \((n=1)\) were involved in hacking, 25 per cent \((n=3)\) in hacking and computer fraud and 66.7 per cent \((n=8)\) committed fraud related offences. Conversely, 38.1 per cent \((n=16)\) of the 42 males were involved in fraud, 28.6 per cent \((n=12)\) conducted both fraud and hacking offences and the remaining 33.3 per cent \((n=14)\) were before the courts for hacking offences. All participants in study three were male.

Table 5

<table>
<thead>
<tr>
<th>Offence type</th>
<th>Male</th>
<th>Female</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>%</td>
<td>n</td>
</tr>
<tr>
<td>Hacking</td>
<td>14</td>
<td>25.9</td>
<td>1</td>
</tr>
<tr>
<td>Computer fraud</td>
<td>16</td>
<td>29.6</td>
<td>8</td>
</tr>
<tr>
<td>Hacking and computer fraud</td>
<td>12</td>
<td>22.2</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>42</td>
<td>77.8</td>
<td>12</td>
</tr>
</tbody>
</table>

Note: percentages may not sum to total due to rounding.

During the interviews with active and former offenders and law enforcement officers participants were asked how many females they had reason to believe were involved in hacking and computer fraud. Both offenders and law enforcement officers agreed that the number of female offenders was low:

*I wouldn’t imagine there would be many, I’ve only known one girl that has been involved in it* (Interview #3, male hacker, aged 22).

*You know, I really have wracked my brain to try and think of females that have been, you know, targets of investigations and I don’t think I can think of one. I’m sure there might be one, but it would be a rarity. It would be, you know, it wouldn’t even make up five per cent* (Law Enforcement Officer #8).
There was some indication that when females were involved their offences were not as serious, less technical, or that they played peripheral roles in the offending behaviour. Participants were asked why they believed males mainly committed these types of offences. Four main reasons were provided, namely: societal factors; that the ratio reflected the lack of interest females held in computer related areas; that females were less accepted by the hacker community; and that females committed fewer crimes than males in general.

Societal factors include aspects such as sexual stereotyping (for example, boys may receive more technical toys when compared to the dolls and cuddly toys received by girls). This was a popular theme that emerged in the data:

*Honestly, social upbringing and society’s perceived roles. And how they are basically ingrained. So often what you will see is a girl that is out and guys are busy, they’re hanging with their mates, they’re doing something. Girls are either reading a book or out with their friends, doing makeup, doing all those things during those years, you know* (Interview #1, male hacker and fraudster, aged 27).

*Oh, I think that um, the entire kind of computer industry is quite male, I am not sure why that is, um, it could be simply because, my first interest in computers was through gaming, as was a lot of people’s. And I think that the entire gaming culture is very anti-feminist. Which I think is a severe problem with it, but it has always been like that* (Interview #6, male former hacker, aged 18).

This gender inequality is also evident in the computer sciences: although females use the internet as often as males, they constitute less than 20 per cent of computer science graduates (Margolis & Fisher, 2002). Many participants stated that females were simply not interested in computers or technology, or that females were more socially inclined:

*Um, well I see in general that it’s mostly looked at as being male orientated, like there’s not many females working in that area. I*
mean, especially at my university, there’s not that many girls in the IT classes. If you go over to the business classes most of the girls are in the business classes (Interview #3, male hacker, aged 22).

I think computers are typically just geeky blokes. Um, I think that’s right across it IT side of it, it’s more male dominated I would have thought… I think, it’s probably just a blokey thing, like motor mechanics, it’s the pulling apart side of it, and I’d say that’s, it’s just that mindset of tinkering, I suppose (Law Enforcement Officer #4).

Maybe a lot of females don’t have the same passion for IT as blokes do. Maybe it’s that a lot of them have got lives. They don’t just spend their lives self obsessed with computers. Male offenders get totally obsessed by their life online. Women seem to have that separation where they have a life in the real world as well. Whereas guys substitute the real world life with the cyber life (Law Enforcement Officer #9).

Yeah, I suppose. I mean, it can be pretty solitary. When they sit there in front of their computers and stuff. Yeah, I think, you know, I’m no gender psychiatrist, but I think, you know, men might take more to be able to spend eight hours of the day, seven days a week in front of their computers not talking to anyone else. Maybe what women prefer is the social aspect of life, I mean, that’s a really broad generalisation, you know what I mean, like a, you know, a 19-year-old guy’s pretty, won’t think twice about sitting in front of his computer all night. Maybe women will, yeah, I do think they have better things to do with their time (Law Enforcement Officer #14).

Another theme that arose was that females might feel threatened or uncomfortable in such a masculine environment, as well as the different opportunity structure for males and females to develop peer relationships with other offenders. Chantler (1995) reports that female hackers are perceived with either complete distain or with high regard by the general hacker community. It was noted that females were treated differently than males by other hackers, and that this may discourage them from continuing:

So what happens is that when you get a girl that says she can do these things, she gets scrutinised more, people will work against her, because they hold such prejudices against her. So it’s just not worth it. So the girl can either crack the shits or say nah, this isn’t
worth it, or she'll just have to keep slugging it out. And she'll have to be better than the boys. It's probably why a lot of them just go no... It's way harder. They have to work. Like, to be a girl doing that sort of stuff, not only do you have to deal with dickheads that are constantly hitting on you, dickheads that think you're a dickhead, or just ragingly rude people that make grossly inappropriate statements that it's just not, ok, eventually you'd just have to say it would probably have been easier to pretend to be a guy, and then say that. And it's just weird (Interview #5, male hacker and fraudster, aged 22).

Well the thing is with online forums because it's such a male dominated, you know, sphere it's generally, once a girl gets on, you know, she attracts a lot of interest and because a lot of these guys are underachievers, you know I dare say that initially the girls will probably get a lot of, you know, sexist comments about them and so forth on these forums, so it's really be the ones that are absolutely dedicated who will generally stay on. And online forums are probably the primary way, there may be people who go to school together and so forth, but generally it's the online forums because you have got that added anonymity (Law Enforcement Officer #12).

However, the gender bias is not unique to computer crime, with only about 20 per cent of all crime and 10 per cent of violent crime committed by females (Hayes & Prenzler, 2007). For example:

Yeah, but it just always seems to be the way, more males commit offences than females (Law Enforcement Officer #6).

Some law enforcement officers advised that the female fraud offenders they had come across had generally suffered, or were experiencing, adverse life events:

Ah, as I said, the females that we've come across, the ones that we've done, have been, um, they tend to be, what's the term for it, it's low value, high volume. And the ones, again, the ones we've seen have been, I think have had drug habits or have been, um, in financial dire straights. And, and others have also been, they've been offended against. Like, they have been in financial troubles themselves, they've been offended against in the past and no one's helped them. And in their words, no one helped me, no one cared
about me, so they've seen that as a way of furthering themselves (Law Enforcement Officer #10).

Um, there's been a few. I think that I've dealt with, there might be one that I recall, was exactly that opportunistic thing, there'd been a, I think a relationship breakdown, she was struggling to pay the rent and it was just opportunistic. Um, she, a young, single mother, that kind of thing (Law Enforcement Officer #11).

One law enforcement officer claimed that females may be less inclined to be removed from the feelings associated with harming others online compared to males:

I think they tend to be a lot more sensitive and in touch with feelings and I think they, because they're in touch with that they respect other people's feelings more. Whereas because men aren't necessarily in touch with their, the whole touchy feely feeling side of things, they don't think of the effect on the victims, whereas I think women have that connection to emotion, which then automatically leads to consideration of other people's feelings, because you consider your own, whereas men can disconnect from their feelings, so it makes them easier to disconnect from the repercussions that are caused to the victim (Law Enforcement Officer #8).

A minority of participants pointed out that when interacting with someone in cyberspace it could be hard to identify their gender or verify whether they were misrepresenting who they were:

The internet is a big place I suppose, so everybody's anonymous on the Internet, so it is quite hard to tell who is who really (Law Enforcement Officer #14).

Of course, a lot of the ones we're, which come from overseas, it is difficult to tell what the internet, what gender they are, you know. But it's very common to have people impersonate females because it's a lot easier to get a male victim to respond and part with money (Law Enforcement Officer #2).
Age

Smith et al. (2004) compiled case studies from a sample of criminal law sentencing outcomes from a number of international jurisdictions. The median age of the 122 offenders convicted of computer fraud or unauthorised access whose age was reported by Smith et al. (2004) was 26, ranging from 15 to 53. Although the case studies were pertinent to Smith et al.’s (2004) analysis of how offenders charged with computer crime offences have been dealt with by the judicial process, it is doubtful that those who have been caught and prosecuted successfully are representative of the general population of computer crime offenders. It is expected that many who have committed computer crime offences have not been brought before a court of law. Although their actions may be considered illegal in many jurisdictions, it is believed that the majority of offenders are not prosecuted for their actions. This may be because many offenders are of a young age (Chantler, 1995), their actions may be comparatively trivial in terms of loss and damage, and the time and resources required to gather evidence and prosecute are considerable. Therefore, offenders brought before the courts would be expected to be older, and the consequences of their crimes would be more serious than the average offender.

To illustrate this, findings from other researchers are compared with Smith et al.’s (2004) age-related findings. The median age of Chantler’s (1995) respondents, none of whom had reported being charged or prosecuted with a computer related offence, was 20, and ranged from ten to 46; the average age of Turgeman-Goldschmidt’s (2005) participants was 24, ranging from 14 to 49; and Parker (1998) states that the majority of hackers are aged 12 to 24 years.
Although not all hackers are aged in their teens, it seems that many of the older ones started at this time in their life. Chantler (1995) asked his respondents at what age they commenced hacking and found that 94.2 per cent began at age 18 or below. A catalyst for hacking at this age, as reported by 87 per cent of respondents, was receipt of their first personal computer (Chantler, 1995).

The mean age of the sample for study one was calculated using either the age at the time of offending, where known \( (n=21) \), or the age at the time of the court appearance, where known \( (n=15) \). The mean age was 30.6 years, ranging from 16 to 48 years \( (SD=8.6) \). Females \( (M=33.4, SD=7.6, range=22-45, n=9) \) were on average older than their male counterparts \( (M=29.7, SD=8.8, range=16-48, n=27) \). The participants in study three were aged between 18 and 49, with a mean age of 29.7 years at the time they were interviewed \( (SD=10.7) \). The age they reported that they had started hacking ranged from 11 to 25 years \( (M=16.6, SD=5.2) \). The two participants who identified themselves as former hackers advised that they had stopped when aged 18 and 26.

Law enforcement officers concurred that many hackers that came to their attention were young, except for those that had offended during the course of their employment. Law enforcement officers also tended to agree that fraudsters were older than hackers:

> Um, younger, certainly always under 25. In fact, you know, I’ve never really given that much thought until you asked the question. But it’d probably be uncommon for us to see over 25. Um, I’m just trying to think. Certainly the younger set. And that may be, yeah, who knows why that is the case. They’re part of a generation that has grown up on computers. Certainly 35, I’m in the 35 bracket, so you know, we at school, computers were around but certainly not in the form that we know them today. Um, and generally, you know, my generation anyway, they can, you know, get on the internet and
all the rest, but I think the generation before, probably much better educated. And that might be a reason, who knows… Yeah, they may, they may evolve to an older set as the years pass by. But most commonly we would see under 25, 18 to 25, 17 to 25, that’d be a good bracket. I’ve seen, of course, when you’re looking at some of the more, and that would be an online fraudster, hacker, financially motivated, general crook. Some of the personal grievances you get managers and commercial type advantage hacks would be an older set. That wouldn’t be uncommon with a lot of crime, well a lot of financial crime anyway (Law Enforcement Officer #1).

In the ones I’ve investigated, generally the hacking type offences would be male, and late teens to early twenties. And in relation to fraud related matters, male, female, and, oh, I’d say all of them are twenty plus, probably twenty to fifty years old (Law Enforcement Officer #3).

Well, to break it down, it’s between what is your hacker terminology and people involved in e-fraud. Ah, you normally get a different kind of age starting and so forth. Basically, with your, the hackers that I’ve been involved in, um, investigations around that, they’ve normally been young to their mid-20s so, with the occasional one in their early 30s, but mostly they tend to be younger… Um, with the fraud ones, they tend to be more in your late 20s to early 30s kind of thing rather than your real young guys (Law Enforcement Officer #13).

Um, in our experience here they’re probably sub 20. Yeah, 20, 21, when we are talking about the hackers. Yeah, the guys who do the fraud, from what I know, from external stuff, they’re normally older, so over 25, professional criminals (Law Enforcement Officer #14).

Law enforcement officers also advised that offenders tended to ‘mature out’ of online crime in the mid to early twenties:

They tend to mature by 25 you realise you’re heading upriver for a holiday and now might be the time to turn your life around… Um, probably maturity you know. You make a decision at that age. I don’t think it’s unique to online crime. Probably 25’s the time you wake up to yourself and think, you know, it’s a slippery slope from here, or I go into that, you’d know better than me, probably about four per cent of the bracket we have, four per cent are recidivist offenders, you either go into that bracket or you learn your lesson, you pull your head in, you get a job and you move on with the rest of society. For that age, we see anyway, I’m speculating the sort of
age, but that tends to be the crossroads of which way you’re going in life. And then if you decide to take the low road from that point, well then you’re just a career crook, it’s in and out of jail (Law Enforcement Officer #1).

I think for a lot of them it starts off when they’re young as, you know, a way to gain kudos and, you know, probably, like a lot of things, most as they get older will grow out of it as they start getting other interests in life (Law Enforcement Officer #12).

Social economic status

Parker (1998) states that hackers come from all economic and social strata, from the very poor to the very rich. This seems to be contrary to the finding of Turgeman-Goldschmidt (2005), who interviewed 54 hackers and reported that they all came from upper-middle class families.

While the interviews conducted in studies two and three did not touch on what social economic strata offenders came from, some law enforcement officers volunteered their views that hackers came from more privileged backgrounds when compared to fraudsters:

So that’s how I’d distinguish between those two groups, one is far better educated and they tend to be from, you know, how do we say politically more sensitive, they’re from much more middle class and more educated families than just the online fraudster, financially motivated… Um, that white hat type, you know, run of the mill Joe Blow, if not above average because they’re generally tertiary educated. Ah, Johnny […] as we call them, you know, the crook that’s out stealing money, he’s like any other crook out there. I don’t know. He’s, it would be hard to speculate. He’s no different from whatever the generic demographic for average, you know, suburban struggle street is (Law Enforcement Officer #1).

Looking at online frauds I don’t really see them being much different than your traditional types of offences. Those people are, tend to come from broken backgrounds, broken families, low socio economic areas and backgrounds. Lower education. Not dissimilar to your traditional types of frauds and your traditional types of offences. With hacking and unauthorised access tends to be a
completely different kettle of fish. So those people are quite often well educated, professional people sometimes. Got good jobs. If you are talking to high end hackers, again, that’s probably different again. They tend to be your delinquent, intelligent, but sort of delinquency where, you know, prone to pushing the boundaries a little more anyway. And, ah, more inclined to engage in criminal activity using those skills (Law Enforcement Officer #2).

One hacker indicated that he was financially stable, predominantly as a result of trading on the stock market:

But, I’ve already, you know, sorted out how I’m going to retire and, yup, it’s a bit early but I’ve already set up my retirement... I’ve already got enough money... Retirement age at the moment, according to my projections, is about 46... My wins in the financial realm far outweigh the failures (Interview #7, male hacker, aged 35).

Country of origin

Hackers reportedly come from all ethnic and racial backgrounds (Parker, 1998). Broadhurst and Chantler (2006) examined the availability of the internet worldwide and reported that poorer countries had lower population percentages with internet access; however this gap, known as the “digital divide” (Grabosky, 2007b, p. 201) is closing. For example, only 2.6 per cent of Africa’s population had access to the internet in 2006 compared to 68.6 per cent in North America. However, in Africa internet access increased by 423.9 per cent between the years 2000 and 2005 compared to a 110.3 per cent increase in North America during the same period (Broadhurst & Chantler, 2006). Some countries have developed reputations for their citizens’ online criminal behaviour, including Russia and Nigeria (Choo, 2008; Smith et al., 1999). This may be due to a lack of legitimate economic and employment opportunities in these regions (Choo, 2008; Smith et al., 1999), the legality of what may be considered to be crimes in
other jurisdictions (Grabosky, 2007b), and/or corrupt or inefficient police and regulatory agencies (Smith et al., 1999).

Despite the Australian-centric nature of the data collection, there was some variation in country of origin in the samples for each study. Study one included offenders that had been born in Nigeria (Case #18, male fraudster, aged 29 at time of offence; Case #8, male fraudster, age unknown), Russia (Case #2, male hacker, age unknown), the United States of America (Case #26, male fraudster, age unknown), Poland (Case #36, male hacker and fraudster, aged 17 at time of offence), and Italy (Case #4, male hacker and fraudster, aged 32 at time of offence). Three of the seven participants interviewed in study three had immigrated to Australia from Commonwealth countries.

Law enforcement officers confirmed that some countries had poor reputations for responding to online crimes:

_The Russians had a bad rep for a long time and there was whole communities over there where law enforcement just didn’t, the impression given was that law enforcement didn’t want to know about it or wouldn’t do anything, or couldn’t do anything about it. And they were operating with impunity. But then you’ve also got places like Nigeria, Ghana, China and ah, Philippines, and all through Malaysia, all those areas. So, it’s not just Russia, Romania, Romania’s big, it’s all over the place_ (Law Enforcement Officer #10).

Another officers advised that some of the code written overseas was used locally to enable offences:

_Because they’re just script kiddies. They’ve got people in Latvia and Estonia writing the actual applications for them. And they’re buying them online or getting them on Torrent and just downloading it. They just point and click, they don’t even know what it does. So if you just point it here and you click that button, and the next thing this stuff starts coming back to you_ (Law Enforcement Officer #1).
Officers also advised that when first investigating offences it could be difficult to identify country of origin:

*Um, you do see Australian IP addresses, but the problem is you don't, the only people who are going to be using their, not concealing their identity are people who don't know what they're doing... Um, but generally if you're a criminal... you're not beaconing your true identity. You know what I mean, you're not going to tell people that I'm a criminal and here's my IP address, come and see me* (Law Enforcement Officer #10).

**Conclusion**

As demonstrated by this chapter, computer crime is a male-dominated offence category. However, variations do exist by type of computer crime, with females committing more computer fraud than other types of property crime. When females are involved in hacking it appears that they typically are not the primary offender, engage in less serious activities than males and are only transiently involved. Reasons for the lack of female involvement in highly technical crimes appear to be a combination of lack of female involvement in crime in general, compounded with the gender gap found in the computer sciences. Research participants indicated that females have different social roles and expectations than males; and that females faced barriers when seeking to become accepted by the hacking community, which will be demonstrated in subsequent chapters, is important for learning and information sharing.

More females are found to commit computer fraud compared to hacking, although the ratio of females to males is still low. Here the barriers may not be as important, as computer fraud typically requires less technical knowledge. Some of the law enforcement participants indicated that the females that they
had investigated had faced greater adversity compared to male offenders, which they believed had been a contributing factor to their offending. Female offenders were also found to be, on average, older than male offenders.

There was some indication that fraudsters came from a more economically challenged background when compared to hackers, who appeared to be more financially well off. Some variation in country of origin would be expected for a predominantly Australian sample, as the 2006 Census data indicates that 24 per cent of the population was born overseas (Australian Bureau of Statistics, 2009). However, what was interesting from the research findings is that the offenders’ countries of origin include those with reputations for high cyber crime rates, including Nigeria and Russia.
Chapter 6 ~ Motivations and Rationalisations

The aim of this chapter is to examine factors relating to online offending, particularly the motivating factors for computer crime offenders, their views of victims and how they select targets. Areas that are explored include the benefits to computer crime offenders, people or organisations that are targeted, rationalisations for offending based on victim characteristics, whether physical distance from the victim helps alleviate feelings of guilt, whether offenders believe that those who do not secure their systems or information deserve to be taken advantage of, and potential targets that are avoided due to an increased likelihood of detection or for other reasons.

Motivations

Perceived and reported motivations for hacking and computer fraud offences are many and varied, and hackers may be motivated by more than one factor. Table 6 below summarises some of these drawn from the relevant literature.
Table 6
Motivations and Rationalisations Reported in the Literature

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Key cited literature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage other countries or political parties, such as through information warfare</td>
<td>Barber (2001), Berson and Denning (2011), House of Representatives Standing Committee on Communications (2010)</td>
</tr>
<tr>
<td>External pressure, such as from terrorism organisations or organised crime groups</td>
<td>Chantler and Broadhurst (2006)</td>
</tr>
<tr>
<td>Anonymise future attacks</td>
<td>Australian Institute of Criminology (2005b)</td>
</tr>
<tr>
<td>Use system resources for personal use</td>
<td>Australian Institute of Criminology (2005b), Taylor (1999)</td>
</tr>
<tr>
<td>Fund terrorist activities or attack critical infrastructure for terrorism</td>
<td>Australian Institute of Criminology (2005b), Furnell (2002), Smith et al. (2010)</td>
</tr>
<tr>
<td>“White hat” hacking, such as testing computer and network security</td>
<td>Australian Institute of Criminology (2005b), Barber (2001), Jordan and Taylor (1998)</td>
</tr>
<tr>
<td>Be free from, or escape from, the real world</td>
<td>Chantler (1995), Taylor (1999)</td>
</tr>
</tbody>
</table>
Motivations are important when considering crime prevention techniques. For example, target hardening may not discourage offenders whose motivations are curiosity and skill testing as this may be providing them with a greater challenge. In these circumstances providing legitimate opportunities to achieve their objectives may be a more appropriate response.

Many benefits to offenders were identified in the three studies. Financial gain appeared to be the logical motivation for fraud, whereby victims are persuaded to part with their money. However, Braithwaite (1993) prompts us to question whether financial gain is in turn motivated by need, or rather by greed. To distinguish between the two, offences motivated by need are committed by those living in poverty, however those that are motivated by greed, or “insatiable wants” (Braithwaite, 1993, p. 222), are crimes of the relatively wealthy.

In order to establish whether financial gain was motivated by greed or need it was looked at how the money was applied. It is noted that this is a subjective measure, as what may be considered luxurious to some may be a necessity to others. However, it was clear that in some instances financial gain was used to meet basic needs:

*He admitted that he had received the complainant’s money and said that he had spent it on living expenses... That the proceeds of the fraud were used to meet expenses including child support payments* (Case #21, male fraudster, age unknown).

*However it seems clear that you committed these crimes because you were unable to get any money from any other sources* (Case #43, female fraudster, aged 45 at time of court appearance).

*What I do know is that you have, I mean, there’s different levels of the online auction fraud. There’s those people that have um, I guess, been selling normally, they hit a bad patch in their life in*
terms of oh, they can’t pay their rent or something, and think oh, that’s a pretty easy way to get money (Law Enforcement Officer #11).

However, there were other instances where it appeared that the gain was not used to meet the necessities of daily life:

The moneys were spent on furniture ($12,000.00), motor vehicle repairs following two accidents ($10,000.00) and the remaining sums on personal expenditure such as restaurants, clothing and other items (Case #30, female hacker and fraudster, aged 22 at time of court appearance).

At interview with the police you said you had no idea why you had stolen the money. You were not in financial need. You paid lump sums off mortgages, assisted your parents and bought things for yourself and gifts for others (Case #49, female fraudster, aged 32 at time of offence).

Financial type crooks, you know, I don’t know, I don’t think there’s anyone out there stealing to feed the family. It’s all for personal benefit, be it drugs or gambling, car, computer, whatever, it, um, you can’t cop, you know, that they’re under any real strain (Law Enforcement Officer #1).

On one occasion the fraud commenced as the offender was in a difficult financial situation, however it appeared that the offending continued beyond the rectification of this state:

In June 2006, after two years in this position, [he] was in financial difficulties as a result of over-spending on credit card purchases… By the end of September 2006, after five such transactions, he had defrauded his employer of over $68,000, and was no longer in financial difficulty. In fact he had been able to spend a lot of money modifying his new partner’s home and purchasing items for it. He ceased offending for about 15 months because he had all the money he wanted… He resumed offending in late December 2007 (Case #46, male fraudster, aged 43 at time of offence).
Law enforcement officers advised that hackers and fraudsters often differed in terms of motivation. While fraudsters were always seen as being motivated by financial advantage, this was not always the case for hackers, although this appeared to be changing as hackers were identifying ways to utilise their skill sets for illicit gain:

*Is suppose, what they’re trying to achieve, um, yeah, typically I’d think, if it’s going to be an online fraud it’s going to be money based, if it’s going to be hacking it’s not, not financially based… I think, probably the most, with the hacking I would say they’re most likely to target their previous employment* (Law Enforcement Officer #4).

*Ok. Um. I suppose, first thing really, difference between financial fraud, online fraud and hackers, I believe there is a difference. Um, hackers, hackers tend to have different motives, although what I would say is that as computer technology is progressing, you’re tending to find that there’s becoming more of a blend, um, between the two. Whereas, um, probably two to three years ago there would have been very separate lines. Um, hackers it was for the kudos of being able to compromise and develop software, um, design programs and to actually show off the programs to all the users, and ah, pretty much a lot of that is based, from what I can tell, a lot of it’s based from Romania, Russia, area. And, um, obviously they’ve got smarts and they’ve worked out they can make money by doing online fraud and using the hacking skills to do that. You know, there’s case studies out there where, um, you see people, hackers, in Russia, where in the olden days it used to just be the geeks, but now they’re driving around in the nice cars and they’re getting the money through Western Union transfers, things like that, and, um, it’s sort of blending a little bit more than it used to* (Law Enforcement Officer #5).

*It depends what fraud you’re going into. With hacking you might have an IT skill, you might want to prove yourself. You might want to get even with someone at school, so you work out how to hack someone’s, you know, a person you don’t like, you hack into their account, get their email, take their email, depends what your motivation is. The financial scammers, obviously they’re in it for money. People go from never having committed a criminal offence in their life to full time online scamming without any hesitation at all. Really there’s a distinction between the hacking and the socially engineered crimes* (Law Enforcement Officer #9).
As was identified above, one motivation for hackers is retribution or revenge against an employer or former employer (Case #7, male hacker, aged 26 at time of court appearance; Case #19, male hacker, age unknown; Case #25, male hacker, aged 24 at time of court appearance; Case #42, male hacker, age unknown) or as the result of being unsuccessful with a job application (Case #11, male hacker, aged 28 at time of offence). This aspect will be further explored in Chapter 8 in relation to offenders’ employment status. Other instances of hacking were motivated by retribution against perceived wrongdoing by someone known to the offender, for example:

But, um, besides that, I have targeted a few people, not a few, just like one or two. Um, mainly because I didn’t like them, and there was some other stuff that, um, caused a bit of shit between us. And I was quite upset with these people, so I thought, well, this is what I can do, they will never catch me (Interview #6, male former hacker, aged 18).

And you’ve got, um, we see a lot of, ah, instance of broken relationships, where someone’s upset about the breakup and it’s some sort of payback, so they’ll go and either hack their account or put a keylogger on their computers. A husband and wife break up, it’s been a terrible breakup, but for some reason hubby’s bought a computer around and he’s been like, I’ve been wrong, done the wrong thing by you, look, here’s this computer. By all means it’s yours. It’s set up for no other reason than to capture what her activity is. So they wonder why the ex is finding out everything that she’s doing on the internet (Law Enforcement Officer #10).

Oh, absolutely. Yeah. Ah, we get a lot, a lot of enquiries from members with girls’ Facebook accounts that have been taken over, or, and generally it’s their classmates who do it. You know, they’re friends one minute and then they’re enemies the next minute and, um, they are computer related offences, but, yeah, we got a lot of enquiries about that as well (Law Enforcement Officer #3).

Um, you’ve, I suppose you’ve got, um, a fear factor, you know, to target more individuals than, you know, from maybe a stalking or a fear point of view, or somebody who they believe has done
something wrong to them. You know, it doesn't necessarily have to be a company. It can be a person (Law Enforcement Officer #5).

Um, you know, to some degree revenge is a motivator for the hacking side of things too. It's not unusual for people that are involved in the hacking to be targeting a specific person, for like stalking or revenge, um, so not only is it to unauthorised access but the deliberate stalking type people, that break up with their boyfriend and want to ruin their lives, so it applies to both the ex-employee and, you know, interpersonal nature as well (Law Enforcement Officer #8).

You could hack someone because you don't like them. Or you could hack someone because, say an ex-boyfriend wants to stalk the ex-girlfriend. So he hacks, specifically hacks her computer (Law Enforcement Officer #9).

One law enforcement officer recounted an investigation whereby the offender, initially motivated by changing their university grade, had then targeted those who had realised the error as revenge:

...and he's changed his marks from fails to passes and then of course, once he's learnt that's so easy, he's been prolific... and what's happened in this specific case is he's obviously been caught, because they realised that marks had been changed because the administrators gone hang on, that student failed, why is his mark all of a sudden a pass mark. And of course, that led to reporting to the police and we investigated it and then we charged him. You know, he saw that as the professor's fault. You made me, it's because of you I got charged... So then he started stalking the professor. So he started stalking all the professors that had given evidence and all the staff that have given evidence in relation to this case, and to facilitate the stalking he compromised more accounts... And he's using facilities like that to ring up and socially engineer the details of the professors, and once he's got that, arrange for their phones to be disconnected and their power to be disconnected, so, that whole revenge motivation then comes into play and it's in full swing. You know, and he's compromised people's accounts, he's reading all their emails, he's sending emails, setting up dodgy gmail accounts in the professors' names, signing up to websites, sending them emails purporting to be a professor to gain access into other sites, it just blew out of control. Of course, he got expelled so then he's gone to another university and he's gone, you know what, this whole social engineering was quite easy last time, I think I'll give this a crack... and he's used that to gain access to his marks again,
and he’s used that to gain access to, you know, protected instructor resources for third party groups, you know, textbook providers and things like that that they have login for instructors to access exam questions and research papers and so forth, so he’s seen it as an easy way to social engineer and he’s just been prolific (Law Enforcement Officer #8).

Parker (1998) claimed that some hackers have extreme political views, including anarchist, Nazi or extreme right wing associations. However, political ideology and hactivism was identified as a motivating factor in just one hacking case that had gone before the courts:

The appellant’s conduct was alleged to be intentional and calculated to influence the US Government by intimidation and coercion. It damaged computers by impairing their integrity, availability and operation of programmes, systems, information and data, rendering them unreliable… He stated that his targets were high level US Army, Navy and Air Force computers and that his ultimate goal was to gain access to the US military classified information network. He admitted leaving a note on one army computer reading: “US foreign policy is akin to government-sponsored terrorism these days . . . It was not a mistake that there was a huge security stand down on September 11 last year . . . I am SOLO. I will continue to disrupt at the highest levels . . .” (Case #28, male hacker, aged 40 at time of court appearance).

Law enforcement officers advised that there were hackers targeting site for political reasons, but indicated that this was a small minority:

Um, look, I think it's a couple of things. I think it's mainly for money, you do see the occasional hactivist group, but it very much tends to be monetarising that skill set. Um, so, and, yeah, so that's the main cause that they come to, it's about getting the money out of the system as much as you can (Law Enforcement Officer #13).

Yeah. Look, there’s not many that’s political… you might get the odd one for political motivation that, you know, that send something to the government or do something to affect the government, or some other agency, body, they’ll do that for that sort of a gain (Law Enforcement Officer #7).
It appeared that political ideology was overrepresented in the media compared to hacking for other purposes:

Yeah. I’d say there are political reasons. Targeting sites… So we don’t have a lot of those here. Besides what we see in the media (Law Enforcement Officer #4).

Of the additional motivations identified in the literature, the data from these studies supported: to demonstrate, test and challenge skills, fun, excitement enjoyment or pleasure, curiosity and self-education, feelings of power, espionage, to obtain social status, and to anonymise further attacks. As is demonstrated here, offenders may obtain more than one benefit for their offending.

There were a number of unique motivations that were identified in this research, namely righting perceived unfairness, to commit further offences and for sexual gratification. In the following case the offender had granted members of the public relief from taxation due to perceived unfairness:

There was no financial gain to the appellant in taking this course. He did so because of a desire to expedite the process, a heavy workload and concern about suggested inconsistencies in
determinations of applications for relief (Case #1, male hacker, age unknown).

One of the hackers and fraudsters interviewed also claimed that his offending had first begun due to apparent injustice:

Oh. One of the network admins at school had, what’s it called, one of the network admins at school had Mist on his computer, or on his account. School children aren’t allowed games on their computers. That’s not fair, you’re playing it! We can play it at lunchtime. No, you’re not allowed it. That’s for me. Right. No, it’s for everyone, it’s not fair. That was the first bit… That was ah, yeah, that was the first time I think. The first time I ever did something dodgy with a computer. And then I committed fraud on his computer, signing him up to a whole bunch of stuff (Interview #5, male hacker and fraudster, aged 22).

A law enforcement officer advised how identity fraud was used to commit further offences, namely drug trafficking:

Oh, yeah, I’d say drug trafficking… Well, it helps support their operation, those particular deceptions were used, um, more so for travel arrangements. Interstate and overseas… Yeah, so the online fraud was used to purchase tickets to travel interstate for the purposes of trafficking (Law Enforcement Officer #4).

Motivations relating to sexual gratification included hosting child exploitation material on compromised servers, as well as obtaining access to photographs and impersonating another for erotic purposes:

Um, and I think that’s one other thing that we’ll see a lot more prevalence of. It’s what I, what we call dark servers, people compromise people’s servers without them realising and use them as what we call a dark server, a server that no one knows about, to store whether it be child pornography or, um, to host phishing sites… (Law Enforcement Officer #8).

Maybe they’re just simply trying to hack females accounts to see whether they’ve got personal photographs on their accounts, or just to find out what their phone numbers are, or whatever (Law Enforcement Officer #10).
He hacked in to someone’s MSN and then pretended to be the guy, pretended to be that person, and then was chatting to that person’s girlfriend, and basically it got quite lurid and stuff like that. And the girl realised it wasn’t her boyfriend and backed out sort of thing (Law Enforcement Officer #11).

No, they would, I suppose almost stalk, they were sending out emails from that account, or uploading photos or contacting other people requesting sexual favours. And, even putting it politely to start with, yeah, it was bizarre (Law Enforcement Officer #4).

It was identified that offenders may be more likely to desist from offending at an early age when the motivation was not financial:

Um, and simply because I did it simply for the novelty, it is easy for the novelty to wear off. If I was doing it for financial gain I would probably still be doing it. But because I never did it for that and it was simply for the novelty of doing it, that wears off (Interview #6, male former hacker, aged 18).

Yeah, and for skill and to make a name for themselves and so forth. You know, probably no malice involved, you know, when they first start. As I said most people grow out of it, where the ones that don’t, well they then you know, start diversifying their offending (Law Enforcement Officer #12).

Neutralisations

Offenders reportedly rationalised their actions if they perceived that there was little or no loss to individual victims:

Because they know, if they rip someone off generally the banks will reimburse them or if they’re ripping someone off on an online auction site there’s Paypal. Paypal will reimburse them. All the big organisations will cop the hit, not so much the individual. We’ve had some of them say in regards to those types of offences, they actually think they’re excuses, that they picked that site because they knew that site had a policy that if people would be reimbursed, so they didn’t want to actually target the particular victim, they just wanted the money out of the site, they knew the site would reimburse the money (Law Enforcement Officer #2).
Well, for a lot of credit card fraud it's, you know, the banks have got lots of money, the banks will give the customers the money back anyway so, yeah, they try to make out as if it's a victimless crime (Law Enforcement Officer #12).

Another rationalisation related to the technique of neutralisation 'appeal to higher loyalties', particularly where it was seen that the offenders' actions were for the common good, such as instances where there was a lack of transparency on behalf of the victim:

*I think the reality is that the people, the perpetrators of the problem, in this particular instance, the climate change debate, was the university… there was no free speech… if you've got something to hide, you know, there's a problem there* (Interview #4, male former hacker, aged 49).

Offenders also appealed to higher loyalties by claiming that their behaviours revealed vulnerabilities that would ultimately make the internet a safer place, for example:

*Sometimes you get that in the hacker space, i.e. yes, I committed an offence, but I only did it to show the world that, you know, these people should be more secure in the way they're doing their business kind of thing* (Law Enforcement Officer #13).

Another rationalisation was to condemn the condemners for the harm they had allegedly caused. This rationalisation was usually ideological in nature, such as the example provided earlier whereby a hacker left a note commenting on United States foreign policy during his targeted attacks on military computer systems (Case #28, male hacker, aged 40 at time of court appearance).
There was substantial evidence that offenders were able to resolve their feelings of guilt or remorse as they were not physically near their targets. For example:

A lot of the extortions and threats that you get online in the social networking sites, the way people talk to each other and those sorts, they wouldn’t say it to the person’s face. But, because, yeah, there is that element of being removed… they do tend to be removed from what they’re doing, removed from the consequences of their actions as well (Law Enforcement Officer #2).

The belief that offenders who do not secure their systems or information deserve to be taken advantage of relates to the neutralisation technique ‘denial of the victim’. Offenders particularly mentioned that people or organisations that had lax password management, such as not changing default passwords, were deserving of victimisation. The overall consensus by offenders could be summed up as:

There’s no defence really, if you’re too stupid to secure your information then you don’t deserve to be the custodian of that information (Interview #4, male former hacker, aged 49).

One of the hackers interviewed in study three identified that, consistent with labelling theory, the laws relating to computer crime were there to protect the interests of certain parties:

The law, I think is the worst part. The law is so blunt. It is really there to protect a, I guess, not even the way society wants the law to be, it is to protect the status quo (Interview #7, male hacker, aged 35).

One law enforcement officer maintained that high-level offenders operating in criminal syndicates did not rationalise their actions:

Um, to be honest, most of the organised crime guys, they’re not really looking for any justification, they’re there to commit fraud to
make money. It's a business. Your whole justification thing is more when you're moving into that kind of grey hat, you know, I'm a social activist who operates online kind of thing (Law Enforcement Officer #13).

Target selection

Six main themes arose when analysing the data in relation to types of people or organisations that would be targeted, namely systems known to or accessible by the offender; companies perceived as undertaking questionable activities or offending ideological reasoning; those that are perceived as having wronged the offender; those who have known vulnerabilities or are perceived as being easy targets; indiscriminate targets, based on chance; and targets providing a high reward.

Ease of access appeared to be a factor that explained why systems known to or accessible by the offender were targeted. In some instances offenders acted on opportunities presented to them, for example:

The accused was formerly a police officer and as such had authorised access to the … computer system (Case #32, male hacker, age unknown).

Denial of the victim was apparent when offenders targeted companies perceived as undertaking questionable activities or offending ideological reasoning:

I suppose you’ve got anything from ideology, you know, people who want to stop animal testing will purposely target sites, you know, pharmaceutical companies and things like that. Sort of along the same vein, if people who don’t believe in shooting animals, you know, will target a deer hunting website and graffiti that (Law Enforcement Officer #5).
Law enforcement officers also stated that offenders were targeting those that they perceived had done them wrong:

*As far as hacking, unauthorised access, we’ve had a few where they’ve been ex-employees, in general the disgruntled employee’s been dismissed for whatever reason, uses those privileges that they have, the company sometimes fails to secure the network after that person leaves and they just access it without authority later on. Either using their own credentials or using someone else’s* (Law Enforcement Officer #2).

Some targets were selected because they had known technical vulnerabilities, thereby lessening the effort required to gain unauthorised access:

*You can target an SQL database with credit card details. And they target those because they can run exploits and they can scan vulnerable, say, SQL database targets* (Law Enforcement Officer #1).

Offenders also admitted that they chose their targets based on the likelihood that their activities would go undetected:

*When you go with the bigger companies it’s easier to get what you want because, for the most part, they’re busier, their policies and procedures overlook everything. Where smaller companies tend to have more of a wire tooth comb policy. You know, they go through everything a little further. So it’s easier to deal with something big or something like that* (Interview #1, male hacker and fraudster, aged 27).

Some targets were obtained by chance, with the internet allowing offenders to obtain a large number of targets with little cost in terms of time or involvement:

*I think, what we find online is that they target so many people and so rapidly and economically, it doesn’t cost you any more to hit one than to hit thousands, it’s almost a scattergun approach. You look at, like, bot herding and bot cultivation, which is the biggest risk on the internet bar none, that’s very much a scattergun. They write their bot code and put it on YouTube and Facebook and MP3s.*
And then they just spread it online and see what comes back (Law Enforcement Officer #1).

Finally, some targets were selected due to the amount of the perceived benefit to the offender:

Yeah, basically I like to put it in the terms of a return on investment. Um, you know, we've seen countless times in logs and so forth, where they talk about this account has only got ten thousand dollars in it, I need accounts with forty thousand dollars in it. So, basically there's a cost for them to move the money and the corresponding cost if you will, the opportunity cost to exposing themselves to that risk of offending, so they are looking for a certain dollar value before they'll undertake those activities (Law Enforcement Officer #13).

Just as some targets were selected as they were seen to be deserving of victimisation, there was evidence that some targets were avoided if there was the potential for innocent parties to be harmed:

I've definitely come across a couple of cases where I've spoken to people and they've said that they'd never do that. You know, I suppose things like hacking into hospitals or medical centres, where people's lives may be affected by the data, you know, medication and things like that (Law Enforcement Officer #5).

Likewise, potential targets were spared if they were seen to be undeserving of victimisation:

It's not fair to kick them while they're down though… you don't have a deaf person that's just had five people die and given their credit card number out to the funeral home and then say oh, I need a CD player, and then, you know, try and jack that person for it. Um, it's really really bad ethics to do it in the first place, but there's still, there's at least a little bit of honour to it (Interview #5, male hacker and fraudster, aged 22).
One law enforcement officer advised that offenders were not likely to victimise those who could potentially retaliate against them:

*I don't think they would target you know, anything that could really hurt them. You know, like Russian organised crime or the Chinese government* (Law Enforcement Officer #12).

Similarly, another officer advised that offenders were not likely to target government or military sites:

*I'm pretty sure that most would steer away from .gov or .mil sort of things. You know, if they knew what they were doing. If they saw a target come up and it was like .gov or a .mil site they'd probably much prefer to go off to the you know, the Swedish web shop rather than the government installation, so there probably is a bit of self-preservation in there* (Law Enforcement Officer #14).

As mentioned above, one offender advised that he selected large businesses as fraud targets as they were less likely to detect abnormal transactions. Conversely, one hacker advised that he avoided large businesses as they were more likely to try and identify who he was:

*I would never target the government or big businesses or, I never really target people who know about that stuff as well, and could actually track me down. Like, I wouldn't target a big business because they obviously have the power to do something about it* (Interview #6, male former hacker, aged 18).

**Moral beliefs**

During the interviews with current and former offenders, participants were asked to describe their overall ethical or moral approach to life. All participants advised that they considered themselves to be moral people, for example:

*So I don't, I don't follow any religion as such. But I do feel quite strongly about morals, and I suppose if there were to be a religion that appealed to me in the slightest it would be Buddhism. Because I feel, I don't necessarily believe in karma, but I believe in, you*
know, do unto others as you would do to yourself kind of thing, in the fact that, you know, I always try to be quite positive, and I always think you should always try to do good things, you know, in that sense. So, I think everyone has a responsibility of their own actions, and that they should try and be aware of their actions and take consequence for their actions, and try and live life in a good way (Interview #2, male hacker, aged 35).

For me it’s fundamentally important that you try to be honest, that you try to be ethical, whatever that means, within a Western philosophic framework I guess, that you try to be generous and caring (Interview #4, male former hacker, aged 49).

Um, I am quite religious. Ah, I am a Christian. And, um, oh, I don’t know. My basic moralities come with that. Um, they basically just, not so much do certain things, so much as don’t do certain things, you know. Um, I’m not a big drinker, um, I guess it kind of reflects that, um, I’ve never really, oh, I’ve broken a few crimes I guess, but nothing really big. I’ve never stolen anything in my life, um, I think that is mostly from a religious point of view. And, it just goes against my morals I guess, taking something that isn’t yours (Interview #6, male former hacker, aged 18).

One participant advised that he did not consider hacking to be immoral:

I wouldn’t say it’s probably morally wrong. It’s not like you’re cheating on your wife or something like that (Interview #3, male hacker, aged 22).

Another participant stated that even though he considered himself to be an ethical person, this did not stop him from offending:

So, I say that I’m ethical in the sense that I treat people the same way that I expect to be treated... But that being said, when you’re standing in front of a bull, the bull doesn’t care if you only eat salad, it will still charge you. So if you, the way that I look at that statement is that being vegetarian and expecting an animal to not attack you because you’re a vegetarian is a very difficult concept. The animal doesn’t care. It’ll attack. It’s not going to go wow, you’re really good to our kind, then lurching at someone else, it’ll attack. So, I think the ethics are very... it’s a give and take situation, but now and then you’ve got to be prepared to take more, because someone else most definitely will... ah, the laws kind of bend, you know, and aren’t, they’re not binary to me, like I don’t
think one and zero, that’s illegal, that’s not (Interview #5, male hacker and fraudster, aged 22).

Self-perception

The current and former offenders interviewed in study three were asked to describe how they saw themselves fitting in with the concept of a hacker. The common theme emerging from the data was that participants’ self concept did not match the stereotypical hacker as portrayed by the popular culture:

I don’t, you know those movies like Swordfish and stuff, and they’re like, oh, they’re really going, that’s not what my computer looks like. I’m not that guy. I wish that I had a computer that I could go oh look, it’s got this and there’s nine screens. No, I’m just some guy in front of a computer (Interview #5, male hacker and fraudster, aged 22).

Um, the label hacker. I have never seen myself as a hacker. Simply because, um, it is kind of glorified by TV and movies where you think a hacker is some kind of mastermind, but really anyone can do it. If you know what you are doing. There is no real intelligence behind it, it is just kind of knowing what you are doing. If anyone looked into it and could find the resources and people to learn off anyone could do it. So I don’t think, I think the term hacker is a bit, um, it is a bit kind of, what is the word that I am looking for? It makes you seem like you are more than you are, I guess. That’s what I’m trying to say (Interview #6, male former hacker, aged 18).

Conclusion

While fraudsters are mainly motivated by financial gain, hackers seek a variety of benefits from their activities. The data supported a number of benefits previously reported in the literature, as well as righting perceived unfairness, to commit further offences such as drug trafficking, and sexual gratification.

There was little evidence that hacking was committed for purposes such as information warfare. In contrast, it was found that hackers would avoid
government and military targets in order to avoid focus on their activities. Whilst this may appear to contradict the wider literature which identifies these as potential targets (Barber, 2001; Berson & Denning, 2011), the offenders included in this research may be more mainstream, representing the majority of offenders rather than a minority with the appropriate skill, expertise and relevant motives for such attacks. This also indicates that, consistent with rational choice theory, offenders consider the likely costs arising from their actions.

The data also indicated that offenders are employing techniques of neutralisation, particularly denial of the victim. Companies perceived as undertaking questionable activities or offending ideological reasoning were perceived to be fair game. Revenge or retribution was also a common theme that emerged in cases where targets were selected as they were alleged to have wronged the offender. However, offenders avoided targets if they were undeserving of victimisation or if they were aware of potential harm arising from their actions that would impact innocent parties. Other targets were selected indiscriminately, based on chance. Rationalisations for offending based on victim characteristics were ideological in nature, including the loss impacting major corporations rather than individual victims. Some offenders appealed to higher loyalties when hacking in order to obtain information where it was seen that the victim lacked transparency and the release of that information was in the public’s interest. Consistent with Turgeman-Goldschmidt’s (2009) findings, there was little evidence that offenders engaged in denial of responsibility.

This study found that physical distance from the victim does help alleviate feelings of guilt and that offenders do believe that those who do not secure their
systems or information deserve to be taken advantage of. Although offenders advise that they agreed with the rules of society and had strong moral beliefs, they offended regardless, indicating that, in contrast to social control theory, this level of control did not influence their behaviours. There was also little support for the concept put forward by labelling theory that offenders behaved in the way that they did in order to fulfil expectations put on them to act in accordance with their self-concept, with hackers not labelling themselves as such, at least when compared to the stereotype portrayed in the popular media.
Many of the theories under examination in this research relate back to friendships, family, acquaintances and co-offenders. For example differential association focuses on what offenders learn from those around them, while social control theory relate to how others mediate their behaviour and rational choice theory includes how the consequences of offenders’ actions may have positive or negative effects based on the reactions of those close to us, such as esteem or loss of respect.

The aim of this chapter is to provide an overview of offenders’ social interactions. Four main areas are examined, namely offenders’ family backgrounds, their intimate relationships, social lives and their interactions with other offenders.

**Family backgrounds**

While Chantler (1995) states that the popular literature presents hackers as coming from unhappy family backgrounds, Parker (1998) advises that those who he has interviewed come from both stable as well as troubled or broken homes. Of those surveyed by Chantler (1995), slightly over half came from single parent families or families with step-parents. Chantler (1995) claims that this indicates that a high proportion of hackers come from unhappy and dysfunctional families. Supporting Chantler’s (1995) claims, many respondents reported that they infrequently communicated with their parents and 59 per cent
perceived them in a negative light, although these views may be normal for teenage males. Of the 98 per cent of parents that were employed, the majority held professional or white collar positions (Chantler, 1995). Chantler (1995) states that this indicates that parents of hackers may have little time to spend with their children. Parker (1998) claims that parents either ignore, encourage, or are unaware of hackers' behaviours.

At first it appeared that there was no common themes arising from the three studies relating to offenders' family backgrounds. Offenders were found to come from a combination of both happy and stable as well as disruptive families. However, on closer examination it became apparent that many hackers enjoyed a closer relationship with their families compared to fraudsters, and that female offenders had generally endured harsher growing up conditions than their male counterparts. For example, in relation to male hackers:

*Very close to my family, I talk to them every day, to my mum every day usually. Or at least five times a week. I usually call her in the morning on the way to work. Because the time difference is perfect* (Interview #1, male hacker and fraudster, aged 27).

*Yes, I have a good relationship with my parents. I speak with them once or twice a week, so, it would be more if my mum could help it* (Interview #3, male hacker, aged 22).

*I’d say that my homelife was relatively secure and stable… I was number five of six children* (Interview #4, male former hacker, aged 49).

However, fraudsters were reported to come from more unhappy families, with a number of law enforcement officers particularly noting the difference between the two types of offenders:
Looking at online frauds I don't really see them being much different than your traditional types of offences. Those people are, tend to come from broken backgrounds, broken families, low socio economic areas and backgrounds. Lower education. Not dissimilar to your traditional types of frauds and your traditional types of offences. With hacking and unauthorised access tends to be a completely different kettle of fish (Law Enforcement Officer #2).

In many of the cases involving female offenders, the judiciary noted the adverse conditions that they had been exposed to growing up, for example:

There was much physical violence in the family and, from an early age, she had to care both for herself and her sister who was two years younger. Because of her parents' alcoholism and chaotic lifestyle, there were always financial problems within the family and there were repeated parental separations (Case #3, female hacker and fraudster, aged 27 at time of offence).

**Intimate relationships**

Chantler (1995) indicates the stereotypical image of hackers is that they are lacking in social skills, preferring to spend their time with their computer than with others, except those who share their passion. The majority of hackers (83 per cent) reported to Chantler (1995) that they had few friends at school or university and 75 per cent did not have a boyfriend or girlfriend.

In this research the pattern for offenders’ intimate relationships was similar to what was found in relation to their upbringing and family life. One difference related to male hackers, many of whom were young and as such did not have established relationships:

No, the ones we've done, and we are talking about hackers, haven't really, if they have been in a relationship it has been dysfunctional, but normally they're just single kids in their late teens and early 20s. Sort of a bit lacking some social skills maybe (Law Enforcement Officer #14).
I've had both sides, marriage, um, married with children, and single, yeah. Probably the singles are the younger ones, so they're unlikely to be settled anyway (Law Enforcement Officer #4).

However, the older male hackers typically were married or in a de facto relationship and living in a stable family environment:

Family situations. That's right. Yeah, I think the, um, it is quite diverse. I think the younger kids are more, ah, you know, tend to do the unauthorised, the hacking as such, they tend to live at home. The older offenders, if they are involved it's usually after they're married, established, with a wife and children. So, two different scenarios (Law Enforcement Officer #8).

The applicant was then married with a dependent wife and two infant children… (Case #4, male hacker and fraudster, aged 32 at time of offence).

While offenders engaging in computer fraud were often in a relationship, typically these were considered to be less stable when compared with hackers:

Um, most of them have been in a relationship. Um, they've been, the last couple I've done have got families with kids. Yeah, they've all been involved in relationships at the time… Sometimes the family, like, the online fraud ones are generally people that obviously have big financial issues, that just get hooked up into the organised crime syndicates. Um, their, and like I said, so, those sort of, their relations are probably not as stable. Where the IT ones, or the online hackers are generally, they're in a stable relationship, they know what they're doing, they're just doing it either for a challenge or for vengeance, those sorts of things (Law Enforcement Officer #7).

... he hooks up with females but I think he uses them just for accommodation and stuff like that. Um, because when I first came across him, first arrested him, he was actually living I guess with someone of his own age group, and he'd got her pregnant, but the second time I tracked him down he'd hooked up with a much older lady. Um, she would have been late forties, fifties, and he's only in his mid-twenties. So that was quite odd. Um, but I think he just, he leaches off whoever he can. He's come from a broken home and stuff like that (Law Enforcement Officer #11).
Again, many of the females were identified as having had difficulties in their intimate relationships:

You left your husband in January 2008, and spent four weeks with your younger children in a women’s shelter, but felt obliged to return to him because you could not stay where you were and could not find any other accommodation. You would like to leave him and make a new life for yourself in another State. You still have two dependent children (Case #43, female fraudster, aged 45 at time of court appearance).

Commencing and maintaining an intimate relationship was provided as a reason for desisting from online offending, even if only for a short period of time:

…probably when my relationships started, I guess, that it got in the way and I just stopped (Interview #1, male hacker and fraudster, aged 27).

Um, no real reason to be honest. Nothing really happened that I thought I’d better stop doing this. I just kind of started spending my time doing other things… Hanging out with people in real life a lot more. Um, when I moved to [the city] I started seeing my girlfriend a lot more, so I didn’t really feel the need to do it as a pastime (Interview #6, male former hacker, aged 18).

Ah, sometimes it’s because they get a girlfriend, to be honest. Ah, that, I’ve seen that myself (Law Enforcement Officer #14).

Social life

Despite the impression given by popular media that hackers are socially inept, the use of social engineering, a technique used by hackers as a way to gain access to computer systems, often requires good interpersonal skills in order to gain trust and, in time, information (Parker, 1998). The three studies were analysed to determine the extent of offenders’ friendships with others, not including co-offenders or intimate or familial relationships. The only evidence of
positive offline social relationships came from the interviews with offenders themselves, for example:

… I mean, fifteen years ago, but we’re still in contact with each other. Those three. I’ve been to two of their weddings. They came back for another one of my friend’s weddings. It’s like, I don’t see them that often, but we’ve remained friends for life in those three guys… I think good friendships are the best thing that you can have in life. I really do, I mean, I’m lucky to have made some excellent friends over here that I know will be friends for life. Whether I live in Australia or not. But I’m also lucky to have great friends in [my home country], as I said, most of whom I’ve known for twenty years, if not more. Um, and great friendships I think are, you know, they’re what keep you going. It’s having fun with your friends, enjoying the company of good friends, they get you through the lows and help you get the highs (Interview #2, male hacker, aged 35).

This finding may be symbolic of the recruitment process, as those who are more sociable may be more inclined to agree to an interview. However, some of the offenders interviewed did admit that they had poor social skills, particularly when they were at a young age:

I don’t think I really had any friends, well, I did have some friends at school, but they were very transient. Because I don’t think, I don’t think I had the, well, I grew up on a property that wasn’t in the town, so. I don’t think I really, I think as a child I didn’t have any social skills, I didn’t have any capacity. I didn’t know what a friend was. Like, I assumed my brothers and sisters were the only people that were basically the only people not likely to beat me up necessarily. But everyone else I just assumed was probably going to beat me up for some reason… Oh, pretty much, yeah, I pretty much got beaten up one way or another every day (Interview #4, male former hacker, aged 49).

Both law enforcement officers and the judiciary identified cases where the offenders lacked social skills, which was seen as a precursor to offending:

He does not appear to have had an active social life and has become introverted and socially restricted (Case #23, male hacker, aged 29 at time of offence).
[He has a] combination of difficulties with reciprocal social relationships and social communication (Case #28, male hacker, aged 40 at time of court appearance).

One particular one that I can think of, he was married and he was in a long term relationship, but socially outside of that he was socially dysfunctional (Law Enforcement Officer #9).

It was also noted that the online environment was used as a substitute for interactions with others in the real world:

Um, as I said, I was living a lifestyle where I was spending most of my time on my computer. Um, a common misperception is that people who spend a lot of time on the computer don’t have a social life. I had a very rich social life, but not with people in the real world. Um, I think that is the real repercussions for lifestyle that comes with it. Because it is kind of, um, that thirst to be better (Interview #6, male former hacker, aged 18).

Script kiddies, it's their life. The younger hackers engross themselves in computers and the computer world. So much so that they effectively lose the ability to make normal social relationships and social contacts in the real world... Ah, I think more often than not their computers come before they start to lose a lot of their social skills. That's the average. You're going to get the exception, like the recidivist offender that I spoke about earlier who has Asperger's, who has a condition right from the outset. The most difficult thing to have social relationships. But more often than not, kids these days, everything from a very young age, you know, you've got PlayStations and you've got the TV and you've got, you know, they're less and less going out and kicking the footy in the street with their mates or going for a bike ride, you know, more and more involved in the computer world. Online social networking, Facebook, online chat, all that sort of stuff comes first, and then as they continue to live in that world, they tend to lose more and more skills in the real world for making that social connection (Law Enforcement Officer #8).

There was some indication that this online social interaction was what ultimately led to online illegal activities:

Those high end type hackers, we tend to weed out a couple sitting on forums, on multiple computers, and that's how they live their life. And relate to people better through computers than reality I think.
So I’m better off having a conversation with someone using a keyboard... They seem to be a little removed from that physical social network. Basically. They make friends online and then that therefore creates a door into criminal activity (Law Enforcement Officer #2).

Social organisation and co-offending

Meyer (1989) conducted what was probably one of the first qualitative studies relating to hackers. In 1989 computer networks and BBSs were active, however the world wide web as we know it had not yet been launched (Moschovitis et al., 1999). A masters student in sociology, Meyer (1989) was interested in the social organisation of the “computer underground”, namely those involved in hacking, phone phreaking and software piracy. While Meyer (1989) disclosed that the data contained in his thesis was obtained from BBSs, emails, telephone conversations, and hacker publications, he did not elaborate on whether such data was collected overtly or covertly, or how he gained access to research subjects.

Meyer (1989) found that while offenders committed their crimes by themselves, they associated with others to discuss matters of common interest, such as performance techniques, news and problem solving. He therefore concluded that offenders have an extensive online social network, which resulted in greater expertise and skill advancement. Meyer (1989) also found that online criminal involvement was short-lived if the offender was not successful in their early attempts. Similarly, over half (52%) of hackers reported to Chantler (1995) that they worked with others to solve problems and one-third identified as belonging to a specialist hacking group.
Offenders working with others to some extent, or being suspected of doing so, was a common theme arising from the data for all three studies:

*In addition, from time to time, you sent money to people who were not apparently family in Nigeria and others, including ... Benin, ... Singapore, ... Ivory Coast, ... Ghana, ... Malaysia and ... Thailand... Clearly, you did not act alone, but rather in concert with others (Case #18, male fraudster, aged 29 at time of offence).*

*Most of the crimes, if not all, involved accomplices... She claimed that she had been stood over by someone. She had only received between $1,500 and $2,000 for her own use, the rest going to the other person... She described herself as “the button presser”, doing what other people told her to do. She provided the names of accomplices who were with her during the transactions... She was a member of an organised group who had acquired or stolen items of identity, manipulated computer records or processes, and represented identity and acquired, or attempted to acquire, financial advantage through the knowledge and documentation possessed (Case #39, female hacker and fraudster, aged 28 at time of offence).*

*Um, no, I got onto hacking by, I guess it all started, I was just hanging around at an image board, it is quite seedy area of the Internet, ah, and I guess kind of started to make acquaintances with people. You start to talk to them a bit and, um, that's basically how I learnt, just by talking to other people and them sharing their experiences and basically teaching me how to do it. Which was, I guess, close to a forum (Interview #6, male former hacker, aged 18).*

*So, they deal in underground portals. So they all know each other. They may not have ever met each other, but they all know their own tags, and they know who’s who in the zoo, and there tends to be a camaraderie between them, and there’s also a, um, a pecking order so to speak. They know who’s in charge. So they go and meet online at these various portals and they trade in stolen data, they trade in information, they write their own codes, their own malware, they deal in malware. Um, and you can buy and sell (Law Enforcement Officer #10).*
The influence of others was identified as one of the ways offenders became initiated into online offending:

I know that, um, if you have, um, teenage kids these days, especially boys, and um, you see a lot of them play online games. And, um, you see what they get up to, and they're teaching each other. It starts with fun and games online, you know, tricking people to give up their identities or to give you property within the game and run away with it, so it all starts with fun and games. And then you find a friend who’s, guess what I did the other night, so they start talking about it, and then gee, that sounds great, and how did you do that? So they start teaching each other and it escalates. So what was fun and a game, as they get older they realise well, what I was doing here, why can't I use this out here and make a bit of coin out of it. So, kids are learning. Kids know how to get around school systems... Or they'll sit there and they'll take photos of, um, the Wi-Fi devices and find out how to monitor the activity on it, and how to, they’ll go and find out the default access details, try that, see if anyone’s changed the default access, if they haven't, well they’re in. So they’re forever trying and learning and sharing that information (Law Enforcement Officer #10).

Why they get involved. Again, that could be from a number of different reasons. If you’re talking about the advance fee fraud side of things, from what I’ve seen, it just tends to be just a, I suppose, a regional sort of thing for those types of offenders, in that they tend to mix with those people who are involved in those sorts of offences, so they are exposed to it and become involved like that. The lower end sort of offenders that we see, they’re day-to-day sort of stuff. Being exposed to it, someone knows somebody who’s involved in those sort of offences and, um, yeah, they gain the knowledge through the hand and then, again, removed from the consequences so they become involved in it... They seem to be a little removed from that physical social network. Basically. They make friends online and then that therefore creates a door into criminal activity (Law Enforcement Officer #2).

It was apparent that most of the communication with other offenders took place online rather than face-to-face, which allowed them to remain anonymous:

Yeah, I think maybe that happens, you know, it's not face-to-face and it's all online. Quite often they have never even met these people too. They've never met them for real. Oh, it's this bloke, you know, [name], this is his handle online. Never met them. They may have been involved, been in business for a couple of years
together, and swapped a load of money and all the rest, never met (Law Enforcement Officer #1).

And online forums are probably the primary way, there may be people who go to school together and so forth, but generally it's the online forums because you have got that added anonymity (Law Enforcement Officer #12).

Offenders worked together for a variety of purposes, including the actual commission of offences:

Yeah, um, uni mates, when we were getting the keylogger together. The keylogger cost twenty bucks. And we had to get it from Hong Kong. And we all got together and were like oh, this is a bit much, first year uni, everyone's broke, no one's got any brains, yeah, let's just try it. So there were a couple of us that eventually got it... oh, [the university] got slammed. No one paid for internet that semester. Everyone got it. So, yeah, there were about, a small group, four or five of us that would actively try and go to the labs together and try and not look sussed while we’re keylogging people’s stuff, but eventually about thirty people were probably finding out (Interview #5, male hacker and fraudster, aged 22).

Because those simply for financial gain source people to do some of the work they don't, you know, they aren't able to do themselves.... In fact a lot of the financially motivated crooks are very well connected online. This is what is one of the great difficulties for us, is that they are very well connected online world wide. So, regardless of what their problem may be they always have someone that can help them... In fact, you can go to some of these channels where they share online and trade, but there’s a genuine sort of underground economy in that they bandy it around. If I wanted to get involved in, whatever the case may be, if I wanted to get involved in phishing a bank or something that everybody knows, but I don't know how to write the actual page, someone will write it for me online and reasonably cheaply I can ask them to do it. And if I'm not too sure how to host it, they'll host it for me on one of the bots for a part payment. And if I don't want to get involved in cashing out and receiving the money because that's a little bit too risky, there's guys doing cash out services all over the world who you can talk to and meet online. There's a whole community out there of thousands of people that can solve any one of the problems online or make up any link of the chain if you don't want to get involved... And of course the internet being what it is these guys can score world wide. They don't necessarily need to be local. And in fact, it would be uncommon, it would be, if not, you'd never seen
all the components occurring in this state (Law Enforcement Officer #1).

Online portals were also used to learn and to teach others how to hack and commit fraud:

Ah, I probably just learnt about it through IRCs, you know. I got on IRC and just learnt how to do it and ah, because I had a computer and things like that I wanted to make the most of my time… (Interview #1, male hacker and fraudster, aged 27).

…if I want to get involved in armed robbery and I’m not too sure how to do it, I can’t walk down the street and, excuse me mate, you done any stickups before and I was just wondering, what happens if they put the screen up at the bank and what should I do? You can’t do that, oh, you haven’t done any, oh sorry mate, I’ll go and ask someone else what he knows about stickups. You haven’t got the medium to do that. If you go online to an IRC channel and look at online fraud, there’s a myriad of people you can ask, exchange ideas and information and tools and, it’s all there for you to get involved. And you start communicating and the next thing you become, you know, the second, third, fourth time, and the next thing you’re giving advice and your paypal and your money there’s laundering going on and you’re into business. Because it’s there. And I think it’s probably unique in that crime type (Law Enforcement Officer #1).

They can, ah, send you complete instructions. Or, it’s like MSN or instant chat, you can sit there and talk, you can post a comment. So even if they’re not there, you can say listen, such and such, I’m having troubles with this, it’s not working. I’ve done this, any suggestions, and they’ll write back and they’ll just talk them through on how to set up (Law Enforcement Officer #10).

More the, when you’re talking young you’re taking more script kiddies, who, ah, just like to sort of play with code and do very basic command-prompt, DDoS attacks, which really don’t do much damage. But, um, what happens is they get into these forums and they start speaking with other hackers and, you know, they start learning, you know, through these international forums and, ah, to a point some people even purchase code, you know, so they can sort

---

of see, you know, cause it’s, obviously code for hacking software is a valuable resources, you know, people actually buy it... Um, and some of them get on it late in life. You know, there’s forty year olds who’ve never touched a computer before and they discover Facebook, and then they discover forums and then they start learning, and then they speak to people, people tell them how to hide IP addresses and different things like that, and it just escalates, so you’ve got a forty-five, fifty year old with some basic knowledge of how to evade the police and to do something which may be illegal (Law Enforcement Officer #5).

Portals were also identified as being a point of sale for code used to commit offences, compromised data arising from hacks that could be used for fraudulent purposes, and for particular skill sets:

The last type of offending relates to selling software that had the capability of doing what you did. You advertised and promoted this software on a particular website which is described as an “Internet criminal bazaar dedicated to largely hacking and information stealing, as well as the online trade in stolen personal information”. You advertised and offered for sale proscribed data, being malicious software designed to compromise computers and manage or control compromised computers (Case #54, male hacker, aged 19 at time of offence).

Oh, anything. Any illegal activity. Whether it be carding, malware, um, buy and sell... you can buy and sell your own DDoS attacks, like you can, they trade in malware, so you can go there. It’s like a one stop shop. You can, if you’re interested in getting into some sort of illegal activity, criminal activity, on the net, all you’ve got to do is find one of these websites, become a member, and you can go in and they’ll give you complete how to’s. You can download certain programs, you can buy other programs, and they’ll give you complete instructions on how to operate them. If you can’t do it yourself you can get people to tune it for you, to fix it up. You can, if, and something we have seen a couple of times, if that if you have a um, ex-employee again, um, left the company and hired a DoS attack from the Russians. So he’s obviously been to one of these underground networks and hired a, um, an individual or a group to do a DoS attack on his ex-employer. And that was sustained, that I’m aware of, for at least four to six weeks. So, they couldn’t use their systems and they just kept getting attacked. And generally it starts with, um, you’ve been a naughty, something along the lines of you’ve been a naughty boy, you’ve upset a friend of mine, because of that, um, cop this (Law Enforcement Officer #10).
The number of people that offenders worked and communicated with varied from small groups of one or two others, up to hundreds. However, it was identified that there was a degree of social organisation that results in limited access for some offenders:

*Probably hundreds, two hundred people. Cause I was a member of three different trading groups… Ah, there’s one that I will see when I’m on a holiday that I’m going on soon. Or two. None of the rest are close friends… Acquaintances, yeah* (Interview #1, male hacker and fraudster, aged 27).

*Hard to say. Um, when you start sort of breaking them down into charts, it’s surprising, you have your inner group and your inner groups sprouts off maybe another group of twenty, and that group can sprout off another group of twenty, you know. Where do you draw the line, you know, do you just say it’s the first group of twenty, but then you’ve got, you know, other contacts* (Law Enforcement Officer #5).

Meyer (1989) maintained that the information traded by hackers on BBSs was constrained. As hackers were in some respects in competition with each other, the information traded was general in nature, and details of targets are not disclosed. Additionally, social norms dictated that some information was not to be shared too widely to ensure that it did not come to the attention of law enforcement agencies (Meyer, 1989). It appears that Meyer’s (1989) findings can also be applied to modern online forums (Glenny, 2011; Holt, 2007). In the study with law enforcement officers it was identified that many online trading portals took steps to control access so as to minimise law enforcement infiltration and disrupt investigations:

*Particularly, a lot of these forums, you have to be vouched for. You can be police. You need to get vouched for to by a member of this group. To do so you probably have to commit crimes to get vouched for by another member… There’s a number of reasons for credibility of members, but it stops the law enforcement interaction*
with them, and all those reasons. So, depending on what group you want to go, you know, if you can get involved in the vouched for groups it’s much better creed (Law Enforcement Officer #1).

Um, but if you don’t commit wholeheartedly, well then they start to be concerned. Because police work eight hours a day, you’re, you know, there’s certain hours, they’re not living on it. So they get suspicious of people who aren’t giving as much um, attention to the portal as what everyone else is... Like, if you buy and sell and you get a bad reputation, people can post and say, you know, watch out for such and such, he’s failed to deliver on this, or the product he provided was crap. They have their own feedback for each other as well. So, it goes up in rankings (Law Enforcement Officer #10).

There’s hacker groups out there who, as an entrance exam to get into these forums, you have to produce some code. You know, and it’s, if the code’s good, then you might get in, you know. And that’s just how it works (Law Enforcement Officer #5).

It was identified that there was a level of control over how people communicated on the information sharing sites:

And they love to assert their skills over other people, you know. Someone not as knowledgeable asks a dumb question or if there’s, you know, postings by somebody who’s off their mark in their knowledge or whatever, they tend to flame them fairly quick you know (Law Enforcement Officer #2).

Yeah, there was another case I have dealt with, he was on, he was on sites, discussion sites, but, um, he was, it was quite bizarre, because he was on these discussion sites, but from what I saw of it, they were actually hanging a lot of crap on him himself (Law Enforcement Officer #4).

There was a perception among law enforcement officers that offenders worked together as a way to frustrate police investigations or provide legal defences:

...we’ve seen them working in groups, because it allows for a long list of defences around the mental element of the offence, i.e. the person taking the money out, who is closest to the offence, the first step in the chain, then has a defence of, well, it’s not my money, I was, you know, doing a favour for Bob. You go to Bob and he says,
you know, well Tom owed me money, and I don't know where he got the money from. So there's built in defences straight away when they're starting to deal with those proceeds (Law Enforcement Officer #13).

Many of the law enforcement officers advised that their investigations involved aspects of organised crime:

*Oh definitely, the big organised ones that come in that run some of the serious money making schemes are a business. They are a top-down business and, you know, they're well, the information that you see, it's out there in a lot of papers and stuff as well, they are sort of setup like a business. They have their own sectors and little areas, they know what they're doing and have a certain job, and they outsource certain things, like if one part of it can't do, you know, x, they will outsource to another group that can do that* (Law Enforcement Officer #14).

*More the organised crime aspect. They recruit, recruit people with skills in certain areas and they sort of use them to commit the crime on their behalf… Um, I really wouldn't put it past organised crime to control a few forums themselves just from a recruitment point of view* (Law Enforcement Officer #5).

However, it was noted that when offenders worked together it was not always considered to be organised crime, particularly with younger, less experienced offenders. Sometimes it was “just dudes hanging out”:

*Oh definitely, it's just dudes hanging out... Um, well, for, just because it's fun, it's something to do, because they get on and they chat and it is, a lot of the time, it is a social network as well. You know, these other guys, or guys and girls, whatever it is, that you find online have similar interests to what you do, be it, you know, hacking websites, stealing credentials, whatever it is, you start talking to them and you get on there and chat to them as you would to your friends. And as you chat to them you will, you know, you'll be chatting about your day as well as about whatever, you know, websites you've found that are vulnerable to whatever exploits or how many credit cards you've got, that sort of stuff. It's just a social thing... Um, I've never personally seen them in the same location but, it makes total sense that they would, you know, you go over to your mate's place to play video games don't you, so you probably go to your mate's place to hack... It is the same thing, you know,
they don’t see it as a criminal activity per se, it's just having fun with your mates (Law Enforcement Officer #14).

We see them as young as 13, 14… But they tend to be just inquisitive I suppose, for want of a better word. They’re involved in gaming sites or social networking sites talking to people all over the world, other kids, and they share information and some of that ends up being criminal information. They commit other offences, hack each others’ accounts, commit online fraud and also, we even have kids sharing botnet28 remote control servers with each other. So, they might attack the school, attack the school website. So, yeah, it can start quite young. That’s just the nature of the internet I think, the information sharing’s out there, and if you’re inquisitive and you’re interested in that sort of thing, it tends to be a bit of a cool interest and a thing for the kids online to dabble in without ever thinking about the consequences, that they are actually committing a criminal offence… Yeah, kids. So in terms of, a lot of kids get involved with keylogging on public computers, so they can do internet banking rips and stuff like that. They tend to share stuff offline with mates, you know, physically passing thumbdrives with, um, details on, either data from keylogs or, you know, information on how to do certain things online. But, um, we’ve seen instances where kids sort of share that information. You know, share information on vulnerabilities on websites and things like that amongst each other (Law Enforcement Officer #2).

Conclusion

The data indicates that hackers and fraudsters differ in relation to their relationships. While hackers had closer relationships with their families and intimate relationships, fraudsters were in more tenuous relationships and had generally experienced a more adverse upbringing. Females were also more likely to have been raised in adverse family environments and having less stable

---

28 Botnets are networks of “zombies”: compromised computers that have been infected with malware so that they can be controlled remotely to orchestrate DDoS attacks, send spam, facilitate phishing and click fraud, host illegal data and disseminate malware (Choo, 2007).
relationships, aspects which indicates an absence of social bonds through attachment to others.

Hackers have well developed online communities, which were used for learning and sharing information. These were strong elements that supported differential association, and there identified as providing a pathway into offending. Participants are able to stay anonymous while using these portals, which also allow offenders to operate across jurisdictional boundaries, frustrating law enforcement efforts to investigate these matters. This supports rational choice theory, lowering the likelihood of detection.

There were some differences found across the three studies. For example, active and former offenders interviewed in study three indicated that, for the most part, they experienced positive social relationships. On the other hand, law enforcement officers and the judiciary were more likely to focus on offenders’ poor social skills. While this difference may be due to the bias in the sampling design, it may also reflect an attempt on the part of those interviewed to make a good impression, which highlights the importance of data triangulation inherent in the research design. The additional benefit of the interviews with law enforcement officers is that they were in a position to compare their experience with different offence types, specifically highlighting the family differences for hackers and those involved in computer fraud.
Chapter 8 ~ Work and Play

This chapter relates to how offenders spend their time, including their work and education history and recreational activities. Areas explored in this chapter include offenders’ educational achievements, experiences and skill development. The relationship between offending and employment is examined, particularly whether being unemployed leads to offenders seeking illegitimate income and whether employment provides opportunities to offend.

Education

Prior research indicates that many hackers have had a good education (Chantler, 1995; Wong & Wong, 2005). However, the three studies for this research identified that offenders had a wide variety of educational achievements, ranging from dropping out of high school to completing post-graduate studies. Where known, these are detailed in Table 7.
Table 7

*Educational Levels, Where Known*

<table>
<thead>
<tr>
<th>Education level</th>
<th>n</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not complete high school</td>
<td>2</td>
<td>Case #39, female hacker and fraudster, aged 28 at time of offence; Case #54, male hacker, aged 19 at time of offence</td>
</tr>
<tr>
<td>Completed high school</td>
<td>1</td>
<td>Interview #2, male hacker, aged 35</td>
</tr>
<tr>
<td>Did not complete vocational education</td>
<td>1</td>
<td>Interview #6, male former hacker, aged 18</td>
</tr>
<tr>
<td>Did not complete university</td>
<td>2</td>
<td>Case #10, male fraudster, aged 24 at time of court appearance; Case #23, male hacker, aged 29 at time of offence</td>
</tr>
<tr>
<td>Completed vocational education</td>
<td>2</td>
<td>Case #18, male fraudster, aged 29 at time of offence; Case #47, male fraudster, aged 28 at time of offence</td>
</tr>
<tr>
<td>Currently at university</td>
<td>1</td>
<td>Interview #3, male hacker, aged 22</td>
</tr>
<tr>
<td>Completed a university degree</td>
<td>2</td>
<td>Case #4, male hacker and fraudster, aged 32 at time of offence; Interview #5, male hacker and fraudster, aged 22</td>
</tr>
<tr>
<td>Completed post-graduate studies</td>
<td>4</td>
<td>Case #31, male hacker and fraudster, aged 27 at time of offence; Interview #1, male hacker and fraudster, aged 49; Interview #7, male hacker, aged 35</td>
</tr>
</tbody>
</table>

Many of the law enforcement officers identified a difference in the education levels for the difference offence types, with hackers more likely to have a tertiary education, compared to fraudsters, who were more likely to be educated to a high school level (Law Enforcement Officer #8; Law Enforcement Officer #10). One reason provided for this difference in education level was the skills required to commit the different offences:

Yeah. I’d say hacking is more computer-based courses. Computer security courses, things like that. Um, with the fraud it’s, generally, they’ve got to have some knowledge to commit the online fraud, but it’s nowhere near the level what a hacker would need, you know, to write code and things like that. You know, because you’ve got your basic frauds, it depends on what you’re talking about. eBay fraud, you know, carsales.com.au, you know, copying ads and changing things around, you know, they’re not that hard to do. Somebody with limited skills could do that (Law Enforcement Officer #5).
If you’re doing high end hacking of corporate databases then you’ve got to have quite a lot of education, whether it’s tertiary or self taught. If you’re doing low end social engineering you don’t have to have a lot of training at all. Or qualifications… Oh, there’s a huge difference between those involved in online fraud and hacking (Law Enforcement Officer #9).

It was also identified that due to the young age of many of the offenders, they were still at school or university at the time of their offending:

Yeah, I’m currently studying [IT] and just finishing off my degree… Um, I’ve failed one or two classes, but otherwise, yeah, it’s been fairly good (Interview #3, male hacker, aged 22).

Although some offenders’ tertiary education related to information technology and computer sciences (Case #4, male hacker and fraudster, aged 32 at time of offence; Interview #3, male hacker, aged 22, Interview #7, male hacker, aged 35), this was not always the case:

Um, the ones that I’ve been involved with, they are more of the, I guess, almost university age. And we are just talking about the hacking side of things, so finishing, either just finished high school or a couple of years into university. Or even, or some other tertiary qualifications like TAFE or something like that… I think there was one that was psychology, another one that was doing [legal studies]… And, um, yeah another one was sort of looking at getting into a science related, you know, field. But not specifically computers (Law Enforcement Officer #15).

It was apparent that some of the participants did not enjoy a happy time while at school, with a number of reports of being bullied:

From your early teens, it appears that you found attending school difficult due to experiences of bullying and concentration difficulties… From form 3 you were bullied by your peers, causing you much distress and absence from school periodically. This resulted in the deterioration of your academic results and the display of problematic behaviours. You then had the counselling to which I have referred, but you left school without any formal qualifications (Case #36, male hacker and fraudster, aged 17 at time of offence).
Well, my first response, my first tendency is to say that I thought school was a hugely unpleasant experience. Um, I pretty much got bullied constantly. I pretty much didn’t understand what was going on or why. I didn’t understand why people would want to do that. And I just thought the whole experience, I just couldn’t wait, I just counted down, I remember counting down knowing that I was stuck at school. It was just such an unpleasant experience for me (Interview #4, male former hacker, aged 49).

Um, I look at boarding school, like, retrospectively, going, well, it wasn’t that hard, but at the time I remember it being absolutely brutal, living with people that bully you, assault you, every day getting up and then having to go to school, surrounded by people that are horrible, almost professionally, to you. That was pretty hard, like, getting up every day and just going fuck, what’s next. And having to go to class every day, that was the worst... To go and just get attacked daily. For twelve to fourteen hours. And then have to go to bed next door to the person that’s attacking you. And then get up the next day and do the whole thing (Interview #5, male hacker and fraudster, aged 22).

Truanting from school was also commonly reported by offenders:

Um, halfway through grade 11 I started missing a lot of school. Just wagging with mates, and that is when I really started falling behind. In grade 12 I only passed three of my subjects. I probably shouldn’t have graduated but I did. I didn’t get an OP. By the end I was probably only going to school two days a week, unbeknownst to my family. Um, I was driving to school by them, so I just wouldn’t turn up. I would go hang out at the park or work extra shifts at my casual job, just for a bit of extra money (Interview #6, male former hacker, aged 18).

The active and former offenders interviewed in study three advised that they had been in trouble at school. This included for acting up in class, truancy, being caught with drugs, in relation to accusations of theft and for selling pirated movies:

…I kind of got into an argument with my teacher and she just, now I realise at this point that she, she just didn’t know how to handle me, right. But for the most part what she said was just like shut up, and for the most part she said the only place you’re ever going to end up in is in jail. Right, so, I mean, almost since that point I’ve just, I
really didn't like that lady for that, you know... So it made me, for the longest time, think that I couldn't succeed or couldn't do things as well (Interview #1, male hacker and fraudster, aged 27).

I was forced to write right handed until I was nine. And I couldn't. And as a result I couldn't do anything at school. So I had to get into trouble. So in third class I went to the form master every day, I got the cane every day... fifth class was an absolutely horrible man. And he spent his entire time, in my opinion, trying to make me understand why my behaviour was inappropriate. Not that I understood what my behaviour was. So I regularly got paraded by my fifth class teacher, either in front of the class or in front of the school, for things that I had no idea about. I don't remember. Like, I got accused of theft regularly, and I don't even know why. I don't even know, I have no idea what they're talking about. But it didn't seem to matter much, because he was convinced that I'd done it (Interview #4, male former hacker, aged 49).

I got busted for a piracy ring at school, in Grade 9, nine or eight, where boys were downloading movies on these crappy modems. We were working together, we just eventually correlated a list of movies that we had and we were just selling them around the school. Some kid that thought it would be good to be in the teachers' good books told on us. We got, ah, they caught us. Ah, what's it called, CD wallets, full of movies. All just, we got caught and they said we know that you're doing it, you need to stop, blah blah blah (Interview #5, male hacker and fraudster, aged 22).

I got in a lot of trouble, me and some friends were caught with marijuana and I got suspended for that... Um, I was a pretty good student, um, didn't muck up or anything like that, didn't get into any fights, um, but I did get in quite a bit of trouble for not turning up (Interview #6, male former hacker, aged 18).

**Employment**

Of the hackers Chantler (1995) surveyed, only 27 per cent were employed, mainly in menial casual or part time positions, although this low employment rate would also be a reflection of the young age of his respondents. An analysis of media articles relating to computer crime in China identified that most offenders were young IT professionals, including computer operators, IT
system administrators and computer programmers (Wong & Wong, 2005). This exposure to computers not only provided the necessary skills to conduct the offence, but also provided them with the opportunities to do so (Wong & Wong, 2005).

The three studies identified that only a small number of offenders were unemployed at the time of their offending. The law enforcement officers advised that some of the hackers they came across were unemployed due to their young age and school obligations:

*There is social benefits or unemployed in some respect or students. Tertiary students… For instance, we had a young fellow who was, he was operating malware, he had a bit of a botnet going, and he was doing it to, um, troll for gaming tags and passwords… He was still a kid, yeah, at high school or something* (Law Enforcement Officer #10).

However, it was apparent that the reason many of the offenders were working at the time of the offence was because they had offended in the course of the employment, for example:

*In March 1988 the respondent was employed by [a bank] in its Information Systems Department. He started work as a computer operator in the Network Operations of that department of the bank - which has responsibility for running the bank's automatic teller machine network. In November 1990 he was transferred from the Network Operations to the Problem Control Area of the Information Systems Department. That area had its offices in a building connected by a walk-way to the Network Operations. Entry to both these areas was restricted and could be obtained only by using special keys and codes but when the respondent was transferred to

29 Case #21, male fraudster, age unknown; Case #28, male hacker, aged 40 at time of court appearance; Case #43, female fraudster, aged 45 at time of court appearance; Case #50, male fraudster, aged 22 at time of the offence; Case #54, male hacker, aged 19 at time of offence; Interview #6, male former hacker, aged 18; Law Enforcement Officer #5; Law Enforcement Officer #10; Law Enforcement Officer #15.
the Problem Control Area he was still able to go into the Network Operations using the key and codes which the bank had issued to him (Case #24, male hacker and fraudster, age unknown).

[You] utilised your position, a position of trust within the [Department] and you through your rights to use of that Department’s computer system, manipulated that system and the funds that were meant for the credit of others within that system in such a way to enable your co-offenders to access those funds as they duly did (Case #38, male hacker and fraudster, aged 28 at time of court appearance).

Another common theme that emerged was offending that took place as revenge by disgruntled former employees or unsuccessful job applicants:

The appellant, an engineer, had been employed by [the Council] as its site supervisor on the project for about two years until resigning with effect from 3 December 1999. At about the time of his resignation he approached the Council seeking employment. He was told to enquire again at a later date. He made another approach to the Council for employment in January 2000 and was told that he would not be employed (Case #11, male hacker, aged 28 at time of offence).

As far as hacking, unauthorised access, we’ve had a few where they’ve been ex-employees, in general the disgruntled employee’s been dismissed for whatever reason, uses those privileges that they have, the company sometimes fails to secure the network after that person leaves and they just access it without authority later on. Either using their own credentials or using someone else’s. Pretty common, as you probably understand, in offices people share passwords and that with your friends and it comes back to bite you in the proverbial (Law Enforcement Officer #2).

Most times it’s been, um, when they’ve been working in IT support… Um, and effectively when their contract has ended, or they’ve parted ways with the support company, they’ve basically hacked back into the company and either shut things off or damaged things and basically just in spite for losing, for not continuing that work, if that makes sense (Law Enforcement Officer #3).

As a general, I would say that the cases that we deal with, I’ve sort of mentioned system administrators before, but, we get a lot of jobs where they’ve been fired or they’ve left on bad terms, um, and they
use the skills and generally passwords which have never been changed to access the systems and cause damages, um, you know, modify data and things like that. Um, we do tend to get quite a lot of that, and unfortunately it seems to be a growing trend, you know, it's almost like graffitiing business and things like that, you know, they'll break into the website and try and shut them down. A bit of espionage these days as well, between businesses, you know (Law Enforcement Officer #5).

Law enforcement officers advised that many of the technical hacking cases they came across involved offenders that worked in the IT industry:

It certainly, we probably, it's more common for us to see employed offenders... At a lot work in the industry. In fact, the vast majority work in the industry one way or another (Law Enforcement Officer #1).

I mean, from what I know about him, he just worked, he had a government job, um, there was nothing necessarily, you'd put him at middle class sort of, he certainly wasn't lower class. He had like a full time working job. He did work in IT, so maybe he thought he was a bit tricky (Law Enforcement Officer #11).

Most of the offenders we see, hackers, have high end computer skills. Generally self taught. However, some do have some degree of computing background, but from what I've seen, generally low end of the IT industry, help desk, IT systems, things like that (Law Enforcement Officer #2).

However, it was also acknowledged that as the necessary skills required for hacking became more common and malware became more widespread this was changing to include other skilled offenders working in different business sectors:

There is, like, it's really changing a lot since I guess, even five years ago when I was first looking, 5 to 10 years ago when I was first looking into this sort of stuff, where it would be, you know, computer experts doing this sort of stuff because that's, you know, because that's where their skills layed. These days it is not easy to do it, but it's much easier to do it. So you haven't actually got to be a super duper technical person to commit online crime these days. In fact, you can be quite dumb and, you know, read the right blog posts on
the right forums and get the right tools and go on and get yourself a botnet somewhere. So it's not, like, they're not all employed as IT administrators, but some do work for IT companies in IT sort of roles (Law Enforcement Officer #14).

When fraudsters were not offending in the course of their employment they were often not working. However, the reasons for unemployment were not the same as for unemployed hackers, who tended not to be working due to their young age and still being at school:

...online auction fraud as opposed to your computer hackers, I wouldn't be surprised that most of them are employed or are students or whatever, as opposed to your online auction frauds. Probably a good proportion of them are unemployed or employed in low paying jobs and they're doing it to get, especially opportunists, they're doing it to get money to, I mean, some of them are saying, it's to pay the bills and stuff like that. Others, it's just to buy crap (Law Enforcement Officer #11).

Yeah. Um, probably, I would say the fraud one, probably less likely to be employed (Law Enforcement Officer #4).

For online fraud and that you mean?... No, they wouldn't generally be employed... Yeah, I reckon [hackers] generally are. You'll have students or they'll be employed (Law Enforcement Officer #7).

I'd say ninety per cent [of fraudsters] are not employed. They use that as their source of income. And it's quite a lucrative source of income... No, most, if we're talking, most hackers, once again, it depends on the motivation, as I said the age group, the younger ones would usually be the students, or still living at home unemployed. The older ones are usually either recently terminated and looking for a job, or have found another job and are doing a revenge thing... Predominantly, yeah, as far as the unauthorised access side of it, yes. It's, ah, usually web administrators, IT administrators, system administrators, a lot of the unauthorised access is predominantly someone that is employed in the IT sort of environment (Law Enforcement Officer #8).

There have been instances where hackers have subsequently gained employment in the computer security industry. For example, in 2008 a New
Zealand teenager charged with illegal use of a computer system was reportedly approached by potential employers (Macrayne, 2008). However, Parker (1998) vehemently argues that such offenders should not be provided with the chance to access systems, even legitimately. This view is challenged by Taylor (1999), who believes that hackers will stop their illegal behaviours if given the opportunity to fulfil their curiously without resorting to crime. The law enforcement officers interviewed during the second study advised that they sometimes saw offenders cease once they had gained meaningful employment:

_Um, sometimes they just realise that, you know, now they’ve got a good job and it is not worth it for them any more because they might get caught. Sometimes someone that they know got caught. Um, that sort of thing. Maybe when they grow up a little bit they sort of realise that there is more to life…. Some of them go into working in actual security jobs, you know, for security companies, computer security companies, and use what they have learnt to make some real cash and still have fun while they are doing it_ (Law Enforcement Officer #14).

**Skills**

While some level of technical skill is required (Skinner & Fream, 1997), this may vary according to the type of hacking being conducted (Parker, 1998). For example, virus creation kits, phishing kits, DDoS kits and botnet management kits are freely available on the internet (Australian Institute of Criminology, 2006), while other hackers may target known vulnerabilities (Choo, 2008). In addition, many types of computer fraud do not require the same level of technical competence as accessing a restricted computer without authorisation.

Holt (2007) found that hackers had a deep connection to technology, which included a devotion to the development of skill and knowledge. The
hackers included in his study were self-taught through trial and error, used online forums and developed on- and offline social connections to further their education.

The judiciary often expressed views about the high technical level of the offenders' behaviours:

*The district court found that [he] “was skilled at accessing and manipulating computer systems”* (Case #13, male fraudster, age unknown).

*There were before the court, as there are before this Court, a number of very high class references (if I may say so) from medical and technical sources expressing admiration for [his] technical ability in the computer field and for the uses to which his skills are ordinarily put, particularly in the fields of medical record-keeping and security* (Case #17, male hacker, aged 36 at time of court appearance).

*[his] code is considered by international cyber crime investigators to be amongst the most advanced bot programming encountered* (Case #37, male hacker and fraudster, aged 16 at time of offence).

*She was an integral member of the “team” using her knowledge of computers, data processing and electronic banking systems to achieve the group purpose… Her computer skills might have been central to at least three of the schemes, but in other respects she was but a minor “player”* (Case #39, female hacker and fraudster, aged 28 at time of offence).

*It is clear however… that you have a passion and an aptitude with working on computers. You developed an obsession with computers and hacking. Because you had nothing to do and all day to do it, your passion for computers led to hacking and these offences… You are obviously very skilled in the use of computers and you should endeavour to put those skills to good use in a legal way* (Case #54, male hacker, aged 19 at time of offence).
While a number of law enforcement officers advised that the offenders they dealt with had high-level skills, one officer advised that the judiciary over-estimated the amount of skill required to commit the offences:

*Because the judges don't understand how easy it is to commit these crimes online and they hold all these kids up as being some kind of geniuses. And they are not, they're just kids who read a couple of forum posts and, you know, learnt how to compile a bot and install it, there is, like I said before, there is no genius any more in a lot of this, you know, low-level hacker offending, it's just point and click but the judiciary still sees IT as being black magic, so they treat these kids as geniuses who have gone the wrong way... Yeah, it gets up my nose every time I read it. Some of them are, like genuinely smart kids, don't get me wrong. But they are not geniuses who have gone down the wrong track. They are just kids who decided to commit crimes, but the judges see it as being, you know, a genius who has gone off the rails. And if you do go good you could become, you know, the next Bill Gates, when he is not, he is just a 16-year-old kid living in 2011. Yeah, so that is something that I wouldn't mind mentioning* (Law Enforcement Officer #14).

Many of the offenders reportedly used tools available to them in order to offend, rather than writing their own code:

*Most of the time it's pretty easy. Because someone else has already gone and done everything for you, so. You just download that and run the application using the instructions that you're given* (Interview #3, male hacker, aged 22).

*Um, I started what is called kiddie scripting, which is basically just using a trojan to get into someone's computer. Um, a trojan that someone else has made, it's not so much hacking as just kind of using the resources available to you* (Interview #6, male former hacker, aged 18).

*Ah, with the ones that I've dealt with, they're at the lower end. They are just sort of exploiting, you know, basically grabbing code, just doing small modifications or things like that. They're not, sort of, writing it from scratch. So I guess what you would define as a script kiddie* (Law Enforcement Officer #15).

*We've had cases of people in their middle age having hacking tools, like metasploit. Metasploit makes it so easy. It's all console driven,*
you don't have to have the IT skills, you don't have to know Linux, you don't have to go searching the vulnerabilities of the system yourself to see whether a browser's patched or not, that does it all for you (Law Enforcement Officer #9).

Law enforcement officers identified a clear distinction in relation to the types of skills employed for hacking and fraud:

No, they're different. As I said, the online fraudsters I'd tend to put more in the category of your traditional offender. They come from sometimes broken backgrounds and less inclined to have any computing knowledge, or high end computer knowledge. They might understand your online auction sites and those sorts of things. Well enough to trick the average user into, you know, believing that it's true. You do get a more technical side where they start phishing sites and stuff, but, ah, the ones we see and the level we see, they tend to be just posting fake ads or pretending to be someone they're not, etc, to get the money out of the victims... The high end hackers tend, obviously they've, generally it's self taught, you know, and they share a lot of information on forums. Information on how to hack is available to anyone on the internet. But they tend to take each other to more secluded forums where they can exchange information a lot more freely. So their skills are quite high. They have particular areas of expertise and knowledge. Um, but the online fraudsters, no, doesn't need to be, and doesn't tend to be that high end. Probably, when you're talking, when you're comparing average public knowledge of a particular area of computers, it's probably a little bit higher (Law Enforcement Officer #2).

With the fraud type ones, um, not a great deal. Unfortunately they're just, they're playing on people's greed, um, and being gullible, which tends to make it fairly easy. And the computer hacking ones, um, it's a bit of a mix bag. I'd say, look, some are highly skilled, um, and others are basically, you know, you hop on google and you can find tools that will do it for you in five minutes. But certainly, you know, the hacking type has to be a computer type person. Yeah, they couldn't just grab a plumber off the street and get him to start computer hacking, because he wouldn't have the mindset to do it. You know... The fraud type situations can be, yeah, it's not hard to create an account on eBay and sell a fake boat and get the cash, I mean, you know, it's fairly straightforward (Law Enforcement Officer #3).

In online fraud, not very much. They're just, ah, tenacious. It's persistence pays off. So there's probably not a lot of skill involved
in that, it’s just very much create an account, post an ad, you know, any layman could do it, it’s just that they’re doing it prolifically and constantly and it’s the old shotgun approach. You use a shotgun, something’s going to hit. Whereas the, as far as the hacking goes, there’s a lot more knowledge required, a lot more understanding of how a computer works, how programs work, how scripts work, how software works, there’s a lot more knowledge required to do the hacking for the younger generation, you know, where there’s no association to the target. The ones where there is an association to the target, more often than not it’s, I already knew the password, so I go in under something I already knew. So there’s not, they have a lot of knowledge in their field, but not necessarily in relation to hacking. So, I know I keep differentiating the two groups of hackers, but in my experience, they are two distinct offender groups. The actually deliberate hacker that, you know, wants to go in, needs a fair bit of knowledge and understanding. And the, you know, the unauthorised access hacker has really not a huge amount of knowledge. They might be IT administrators and know a lot about computers, but the method that they use to commit the offence is purely just enter my username and password (Law Enforcement Officer #8).

As was identified in Chapter 5, hackers are generally younger than those involved in computer fraud and as such are often attending school or tertiary education. It was also identified that those involved in offline offending are often moving to computer fraud:

Yeah. We do tend to see that, um, the traditional criminals that were stealing or robberies or the drugs, they tend to be steering away from those types of offences and moving towards the cyberworld. Whether it’s because it’s easier to commit, it’s easier to get away with, and also, if you are caught the courts tend to give lesser penalties, you know, no one’s physically hurt. Now, you’ve got less chance of actually physically hurting someone (Law Enforcement Officer #10).

Therefore, this difference in age and offence type may be indicative of what offenders are exposed to in terms of learning about how to commit offences. For example:

I’d say that with hacking you need to have some sort of um, knowledge of how to hack systems. You know, the networking,
how systems work and how to get into operating systems and use hacking programs. So I suppose the younger generation would be more exposed to that as they’ve grown up, you know, during modern times. So they’re more aware of what’s out there and get more involved. Whereas the older offenders tend to be more just using the internet as a tool to commit fraud. You don’t need to have any sort of technical abilities, you just get a computer, go online and they don’t even tend to try and hide themselves too much these days (Law Enforcement Officer #10).

Recreational activities

Chantler (1995) portrays hackers as having few additional interests outside of computers and technology, spending on average four hours a day in front of a computer. Similarly, Holt (2007) found that hackers could be characterised by a strong commitment to their activities, devoting time and effort to further their knowledge. In support of this, a strong interest in computing, to the detriment of involvement in other activities, was a theme that emerged from the data for the three studies:

When I was involved in hacking... An average day would probably be, I would get up around 12, one in the afternoon, um, play a couple of video games, fiddle with my computer, I fiddle with my computer quite a bit. It is an older computer because I don’t really have the finances to upgrade it, but it runs like a new computer because I take care of it, just fiddle with it, little things make the biggest difference. Um, when I was really involved with hacking I guess, do the basics, check all my e-mails, read a few forums, check on the computers that I had a link with, see what they are up to... Um, that was basically a basic day I guess. Ah, I spent pretty much all day on my computer, yeah. I’d go to bed at about three in the morning (Interview #6, male former hacker, aged 18).

[Hacking] is my life, so it is hard to say it is interfering with my life (Interview #7, male hacker, aged 35).

It’s more something they do when they’re at home after work sort of thing, it’s like a social activity really, for them. Some people have their social activities, go out and play sport or whatever. They, they like to hack (Law Enforcement Officer #7).
In fact, computer gaming was identified as a gateway that led to online offending by a number of participants:

*Ok. I used to bite at World of Warcraft, really hard. I played tonnes of it. I was addicted to it. I used to have like four World of Warcraft accounts, four bots, constantly running, just jibbing this game. I got, like most of them got busted, I’ve got one account left that’s got tonnes of stuff on it though. And that’s the one I’m planning on using. I quit, because it’s just ruined my life* (Interview #5, male hacker and fraudster, aged 22).

*Um, I think a lot of people get an interest in computers through gaming, and through that interest in computers then you start to, um, because that is how I got into it, um, because that is where I really kind of became interested in my computer. Um, but I know a lot of people who got interested in their computer through that, my interest was mainly because my computer was a piece of crap and I wanted to run certain games so I had to figure out how the computer works to make it run better for these games, and therefore how to open it all up. And, um, yeah, I reckon that is where most people’s interest in computers comes from. Not all, of course, but a majority* (Interview #6, male former hacker, aged 18).

Yeah. So, at the same time they’re playing video games, you know, chatting with their friends, that sort of stuff… Some, like there is a pretty burgeoning computer game hacking scene, you know, where they cheat at online games and people involved in that, that’s, you know, you can really see how that’s a gateway to more serious offending, because then you learn how computers work, and you’ll learn what exploits are and you will learn how to alter code, that sort of stuff, just to try and get a better score at whatever game you’re playing. And then you realise that what you know there can quite easily be, you know, transferred across into running a botnet, that sort of stuff (Law Enforcement Officer #14).

However, additional interests were identified, particularly in relation to sport and other outdoor recreational activities such as hiking and martial arts, as well as music, including attending gigs and festivals:

*But I still go out and play sports too. So, I mean, that’s like contrasting I guess, hey* (Interview #1, male hacker and fraudster, aged 27).
While I was at [university] I boxed. I played at the [football club] Touch Team, I regularly go to the gym, I play squash and surf and snowboard (Interview #5, male hacker and fraudster, aged 22).

But yeah, realised I really enjoyed music, and that’s always been an important part of my life… Um, general good times, I mean, when I was back in [my home country] I used to always go, religiously go to … Festival every year. And every year without fail that used to be an overwhelmingly fantastic experience. Getting there late at night on the Wednesday, setting up the tent and walking down into the festival area. Amazing, amazing experience. So many gigs I’ve been to as well, and things like that. There’s so many that would stand out as just, I felt on top of the world at those points. I mean, is there anything, you know, just generally good things that I enjoy… I mean, music’s always been a big part of my life, I love listening to music. I don’t go clubbing as much now as I used to, but I love going to gigs, festivals, listening to music when I'm working, it’s, you know, I do quite a lot of travel with my work, I couldn’t live without an iPod. Well, not necessarily an iPod. But I couldn’t live without being on a plane with music. You know, yeah, I love that (Interview #2, male hacker, aged 35).

I do enjoy surfing and all of that sort of stuff (Interview #5, male hacker and fraudster, aged 22).

I've always had some kind of sporting activity. Prior to lawnbowls it was martial arts. So I've got a black belt in tae kwon do, a blue belt in kung fu, that is Wing Chun kung fu, so I think I've got a yellow belt in karate too (Interview #7, male hacker, aged 35).

Conclusion

Hackers were identified as having a higher level of education than fraudsters, although they were often bullied. In support of labelling theory, there was some indication of informal labelling occurring at school, with offenders getting into trouble when young. As they were younger, hackers were more likely to still be in school than fraudsters, and thus not working. While according to social control theory, involving in conventional activities such as employment will restrict illegal behaviour is it provides a bond to society, the data indicated that
many offenders were gainfully working, and instead the workplace provided opportunities to offend, or motivations when relationships with employers soured. The data also indicated that hackers have a strong interest in computers and technology, which ultimately led to their online offending.

One difference arose from the data in the three studies; with the judiciary tending to have a different view about the technical skills required to commit the offences. In comparison, the view from law enforcement was that, while they did deal with highly technical matters, the degree of skill required by, or held by offenders, was often over-stated. This is particularly the case when offenders used the automated tools available to them.
Chapter 9 ~ Life Events

Events that occur in one’s lifetime are theorised to play a part in the pathway to later offending. For example, according to labelling theory, those who have previously had experiences with the criminal justice system are more likely to reoffend. Structural strain theory purports that when people are unable to achieve their life goals due to lack of means and the adverse life conditions that they have experienced, which leads to strain and, in some cases, crime. This chapter explores offenders’ previous criminal history, as well as examines areas where they may have experienced strain, namely physical and mental health, addictions, and financially.

Prior criminal history

Parker (1998) states that most hackers would never commit crimes in person, however are freed from social norms due to the distance provided by the computer. However, Parker (1998) also states that some offenders will resort to burglaries in order to obtain technical manuals and equipment.

The data relating to prior criminal history were examined to identify any differences between the active and former offenders and those who had been before the courts and investigated by the police. Of the interviewed offenders two had experienced interactions with the police, however neither had been prosecuted nor convicted. The first matter was connected to online offending, in which a warning was recorded, however the second was unrelated:
I remember getting busted by the police when they came to my house about the computer fraud stuff. When I was younger. That didn’t go over so well with the folks. And it intimidated me a little bit. Another time I was caught by the police was with pot. That intimidated me a little bit for awhile… Ah, that was a warning. Yeah, I had the federal police at my house as a result of me accessing different sites, specifically NASA had made a complaint to the [police] about, which is the North American Space Agency, about me playing around on their computers. And, ah, they paid a visit to the house and had a look around on the computer and talked to my folks and pretty much talked to me… [I was] fifteen… Um, basically they took down my information, put it in their notebook, and that’s all it was. It doesn’t even exist any more (Interview #1, male hacker and fraudster, aged 27).

Have I been arrested? Once, but that was when I was working in [country], I got arrested for illegally working. Soon sorted out, spent the afternoon in a cell absolutely shitting myself. Soon sorted out when the new policeman that had arrested me, new to the area, hadn’t realised that my boss was best mates with the chief of police. Um, other experiences, oh, I’ve had, I’ve been searched at raves and had minor amounts of drugs taken off me, but due to the nature of so many people they were searching and finding stuff on, didn’t even get a caution (Interview #2, male hacker, aged 35).

There were many instances in which the judiciary noted no evidence of prior criminal history when sentencing offenders. One law enforcement officer advised that compared to other crime types, offenders typically did not have a criminal background:

Um, the ones I’ve charged, no. There’s been no history of violence. No history of drug use or abuse. Um, I’m just trying to think. No. Quite, I mean, some have had minor, very minor involvements, like with intervention orders… Intervention orders can be, you know, your next door neighbour that’s, you know, stalking you, I mean, magistrates tend to give intervention orders for anything and everything. Um, but quite often it’ll either be with a domestic partner, family members, um, but majority I would say are first time offenders or fairly, certainly not your normal, typical criminal (Law Enforcement Officer #3).

In relation to the matters that had gone before the judiciary in study one, there were a number of prior convictions identified that were unrelated to online
offending or fraud. These included weapons related offences (Case #20, female fraudster, aged 36 at time of offence), drink driving (Case #46, male fraudster, aged 43 at time of offence), and stealing (Case #53, male fraudster, aged 30 at time of offence). Only two of the offenders had been identified as having engaged in violent offending:

You have three prior convictions, namely, for unlawfully possessing a firearm, possession of a knife in a public place and male assaults female. All relate to a psychotic episode you experienced at your home in 2005. You were convicted and discharged on the former two and received a sentence of supervision for the latter (Case #36, male hacker and fraudster, aged 17 at time of offence).

Your only prior offending has been dealt with in the Youth Court and is unlike anything with which I must deal. Some of your offending relates to damaging property with graffiti, plus an aggravated assault in 2006 for which you were given one month suspended detention (Case #54, male hacker, aged 19 at time of offence).

Numerous offenders had prior histories that were similar to their current offence, either offending online or behaving dishonestly in the offline environment, for example:

[He] had previously appeared in the Youth Court on charges of accessing computer systems for dishonest purposes and obtaining money or services by false pretences. Five offences were dealt with on 5 July 2004 and three on 14 October 2004. On all of those charges, the Youth Court Judge admonished and discharged [him]… The Judge was familiar with [his] past offending. He was the Youth Court Judge who had dealt with [him]. He described the way in which [he] was dealt with by that Court as "lenient and rehabilitative". Yet, soon after, [he] was re-offending. Some of that offending occurred while he was on bail, awaiting trial on the initial 80 charges. The Judge said: The impression that one could justifiably gain from that course of behaviour, …, is that you are a serious recidivist computer criminal (Case #34, male hacker and fraudster, aged 17 at time of offence).

The applicant had an earlier conviction for a computer offence. This related to obtaining access to a Commonwealth computer which the
applicant broke into at the Australian National University. The applicant was convicted for that offence in 1993 and was punished by way of fine (Case #7, male hacker, aged 26 at time of court appearance).

Ah, quite a few. And that’s I guess the advantage of doing this triage process, whilst we just don’t have the resources to investigate them all ourselves, the advantage of having all of the complaints come into the one office allows us to identify the recidivist offenders… I’ve been here and the same name will come up every year or so, there’s one up in, I think, a guy up in [region] area or somewhere up that way, and does it on the same forum, but just creates a different name or something like that, and just every year or so, the same name. Oh, him again. I arrested, I was looking for him back in 2006 when I first came here, and there’s definitely some names that come up continually (Law Enforcement Officer #11).

However, consistent with labelling theory, it is possible that recidivist offenders are identified as they are more closely monitored:

A lot of people get a big wake up call, but we do get recidivist offenders, yes… I wouldn’t say a huge group, but it is something you see, once they’ve come to police attention we can sort of monitor them a little bit more, so, you know, there’s a higher probability that we’ll find them doing the wrong thing again (Law Enforcement Officer #5).

Again, a number of law enforcement officers identified a difference between those involved in hacking and those involved in computer fraud, with fraudsters reportedly more likely to have a prior offence history, including for offline fraud:

On the e-fraud side of the house, they tend to, they do have property crime backgrounds, a few of them. Around your more traditional fraud offences, obtaining benefit by deception. And this is just an area that they’ve kind of moved into to further supplement that kind of income stream… [Hackers] normally, um, they haven’t, other than, you know, maybe some marijuana use, but that’s only what they’ve admitted to, they haven’t actually been formally charged or convicted of those kinds of offences, so um, yeah,
definitely on the hacker side, yeah, not so much (Law Enforcement Officer #13).

Hackers, I don’t know. Fraudsters will basically just, they’re onto anything and everything that will earn them a dollar. I’ve got no link between them and ah, say drugs, for example. But, you know, fraudsters, they will lie to anyone. That’s online or offline. It doesn’t make any difference (Law Enforcement Officer #9).

While overall there were few female offenders, one law enforcement officer advised that when they are engaged in these types of offences they tend to be involved in fraud, repeatedly so:

Well there’s a big difference. We don’t see too many females. I haven’t seen too many females whilst at this unit. There have been a few, and those that have come to our attention have been, um, recidivist offenders. So they’re, um, they’re basically full on. And they haven’t had any female hackers, they’ve just been online auction fraud type offenders (Law Enforcement Officer #10).

Evidence of extensive criminal histories, particularly in relation to dishonesty, was identified for some of the female offenders that went before the courts (Case #39, female hacker and fraudster, aged 28 at time of offence; Case #43, female fraudster, aged 45 at time of court appearance; Case #52, female fraudster, aged 35 at time of offence). In one case, the offender had a significant record spanning ten years, including burglary and stealing, making off without payment, unlawful possession of property, selling and possession of a controlled drug, obtaining goods by a false pretence, forgery, uttering, receiving stolen property, and breaching bail conditions (Case #39, female hacker and fraudster, aged 28 at time of offence).
Physical and mental health

Strain experienced by offenders included physical and mental health problems. A number of offenders were identified as having experienced significant medical conditions, for example:

The appellant referred to other medical conditions from which he suffered. These include renal problems and encephalopathy. Further, on 19 February 2001 he fractured his fibula… He referred to [a doctor's] opinion that the appellant "by any standard is a very sick man" and that the appellant had "a substantially shortened lifespan". His Honour recognised that the appellant would find custody a difficult and onerous experience. He stated that he took into account the fact that the appellant's "psychological and medical health and age may increase the hardships that he will undergo while in custody" (Case #12, male hacker and fraudster, age unknown).

He suffers from several medical complaints – (i) moderate to severe facial psoriasis which is disfiguring; (ii) psoriatic arthritis which restricts his mobility particularly on waking in the mornings; (iii) hypertension; and (iv) ongoing liver dysfunction, due to heavy alcohol consumption. Standard medical treatment for psoriasis has been rendered less effective by the applicant's liver dysfunction (Case #35, male fraudster, aged 40 at time of court appearance).

[The doctor], a consultant nephrologist, testified that the applicant suffered from glomerulonephritis, a condition that had progressed to end stage renal failure. He said that the applicant was in a group whose mean life expectancy was better than 15 years but that his condition certainly involved a dramatic shortening of life expectancy compared to what would otherwise be expected in someone of his age. The applicant was suffering from hypertension. At an earlier stage he had suffered from accelerated or malignant hypertension but that had been brought under control. Dialysis had begun in late 1997 and at the time of sentence was taking place three times a week, each session being of some five hours' duration. Dialysis might continue in its present form (haemodialysis) for the rest of the applicant's life. Alternatively he might undergo a renal transplant if that became available or a different form of dialysis, known as peritoneal dialysis, might be undertaken. At the time of the plea he was a category 2 patient, who would not be offered a kidney transplant, but [the doctor] was hopeful that he might become in time a category 1 patient. He considered that, potentially, the
applicant was an ideal candidate for a transplant. The average waiting time for a category 1 patient was approximately four years (Case #6, male fraudster, aged 34 at time of court appearance).

But, yeah, I've always had a significant stress issue that, in my twenties I had a heart arrhythmia that, um, the heart specialist said that if I didn't do something radically I would die. He said I had about three weeks to make my mind up. Otherwise I would have a heart attack and die... Yeah, well, I got to see Sydney's second best heart specialist in about fifteen minutes from being diagnosed. Like, the doctor rang him up and he said get him into a taxi and send him over. And I was there. And, ah, so, I didn't have to wait to see a heart specialist. So I guess it was serious, in hindsight (Interview #4, male former hacker, aged 49).

In at least one occasion the offender's health problems was used as a reason for the offending behaviour:

The appellant maintained that he was sick and confused and under pressure at the relevant times (Case #31, male hacker and fraudster, aged 27 at time of offence).

In addition to medical problems faced by offenders, some were identified as having to care for sick family members:

The appellant pointed out that his wife suffered from medical problems that were relatively serious. She is an insulin dependent diabetic. She was described by a treating doctor as being "in a very disabled state". She experienced insomnia and "self-recriminatory thoughts". The appellant asserted that his wife required "a lot of care and attention" and this was borne out by medical reports (Case #12, male hacker and fraudster, age unknown).

Their daughter has a genetic disorder, spinal muscular atrophy. She is wheelchair bound and needs artificial ventilation to help her breathe for some of the day and every night when in bed. Her care is extremely demanding. Apart from a carer at school, trained medical staff and regular help from the appellant's mother, the child's parents shared responsibility for looking after her (Case #39, female hacker and fraudster, aged 28 at time of offence).

A number of offenders were identified as suffering from depression (Case #21, male fraudster, age unknown; Case #30, female hacker and fraudster, aged
22 at time of court appearance; Case #36, male hacker and fraudster, aged 17 at time of offence; Interview #4, male former hacker, aged 49). Another recurring mental health problem was disorders that lay in the autism spectrum, which was identified as being a reason for the offending behaviour:

The presence of an Autism Spectrum Disorder leaves [him] vulnerable to the stress of social complexity as well as anything that is unfamiliar or novel to him… If he finds himself in circumstances where he is unable to withdraw from complex environments into something more autism-friendly, he is likely to develop a pathological anxiety state and, given the presence of the developmental disorder, he will be prone to develop an acute, psychotic disorder (Case #28, male hacker, aged 40 at time of court appearance).

[His] mother advised that as a child [he] was tentatively diagnosed as having a mild form of Asperger’s syndrome. A report by [a] registered psychologist dated 14 July 2008, provided by the defence for the purposes of sentencing, tends to confirm that diagnosis… [the psychologist] notes that [his] symptoms have reduced considerably and some have effectively disappeared over the last year or so, since his social interaction has increased. But he says the reported history strongly suggested that [he] suffered from some form of minimal brain dysfunction specifically affecting his gross motor and co-ordination development. In his opinion that developmental condition was likely to have contributed significantly to [his] offending (Case #37, male hacker and fraudster, aged 16 at time of offence).

Personality disorders were identified in three offenders that appeared before the courts, including:

You have had psychiatric problems since adolescence… [a psychiatrist] diagnoses you as having a borderline personality disorder and probably an underlying susceptibility to bipolar disorder, with recurrent depression and, at times, hypo-manic episodes. It is his opinion that medication given to you for depression at the end of 2008 is likely to have caused such an episode and that it was having some effect on you and your judgment during the time of this offending (Case #48, male hacker and fraudster, aged 31 at time of offence).
One former hacker interviewed in study three advised that he suspected that he had suffered from schizophrenia, and this condition was also raised in relation to another offender:

My brain just does things. Before I went to uni I always had a little voice in my head. And it always said things like, it’s ok, you just have to wait until such and such. Or, just do this now and you’ll be ok and all that sort of stuff. In hindsight I realise that it was probably a stress induced schizophrenia, but, ah, the only reason that it’s not is because the little voice was never destructive. The little voice was always constructive. It always led to a better outcome if I listened to it (Interview #4, male former hacker, aged 49).

Oh, this second bloke, who lives at home, he suffers from schizophrenia and, um, what’s the other mental illness that’s similar? Um, I can’t remember now. But he suffers from mental illness (Law Enforcement Officer #6).

Drugs, gambling and other addictions

Addictions to gambling, drugs and computers were common themes that arose in the three studies. In relation to gambling, this was identified as a causal factor for fraud, whereby they committed the offence in order to fund their compulsion. While gambling was only apparent in relation to offenders committing fraud, drug use and abuse was identified in relation to both hackers and fraudsters:

Between the ages of about 15 and 17 years you mixed with the wrong group, started taking drugs and committed a number of offences mainly relating to graffiti (Case #54, male hacker, aged 19 at time of offence).

30 Case #20, female fraudster, aged 36 at time of offence; Case #22, female fraudster, age unknown; Case #35, male fraudster, aged 40 at time of court appearance; Case #48, male hacker and fraudster, aged 31 at time of offence; Case #50, male fraudster, aged 22 at time of the offence; Law Enforcement Officer #1; Law Enforcement Officer #7.
Ah, predominantly cannabis. And mushrooms. I had someone put acid in my drink at graduation at high school and I didn’t know until I went home and I was off my face. Ah, that wasn’t good. That was about eight hours of hell. Um, I think ecstasy once maybe, half tab. I’m not a fan of chemical drugs, I’ve seen how they’ve been made and things like that, so kind of disgusting. Um, I’m trying to think if there’s anything else over the years… Ah, [I smoke cannabis] probably on and off, but it’s consistent. I mean, if someone offered me to smoke a j today I’d probably take them up on it. Because it’s been a while. I’d be like, oh yeah, cool. So I’m not anti narcotics, if that’s the attitude. If it were to come down to me I’d smoke cannabis more than I drank. I drank five times last year, maybe total. I don’t really like alcohol and its effects on me. I’d rather smoke cannabis because I’m more under control (Interview #1, male hacker and fraudster, aged 27).

But I mean, in my raving days I used to take a lot of amphetamines, a lot of speed, ah, used to do ecstasy regularly as well… But, I’ve dabbled in other things, like LSD, I did quite a bit of that when we were young, um, the thought of taking that now scares the life out of me… I’ve tried things like ketamine, never again. Magic mushrooms I suppose a few times. But I think the main drug of choice for me was always marijuana (Interview #2, male hacker, aged 35).

Some of them have been druggies. Ah, drug addicts. Some of them are, that we’ve come across have actually been using the money they make from auction fraud to finance drugs. So they use it to get their money, which they then buy drugs with and sell (Law Enforcement Officer #10).

One law enforcement officer advised that female offenders were particularly likely to use drugs:

Ah, as I said, the females that we’ve come across, the ones that we’ve done, have been, um, they tend to be, what’s the term for it, it’s low value, high volume. And the ones, again, the ones we’ve seen have been, I think have had drug habits or have been, um, in financial dire straits (Law Enforcement Officer #10).
This was supported by a relatively high number of females identified by the judiciary as having a problematic drug addiction:

The appellant had been using amphetamines on a daily basis and was dependent on them. As so often happens with addicts, that led to her committing crimes of dishonesty to sustain her addiction… A psychological assessment of the appellant was also tendered which recounted a history of substance abuse confirmed by her conviction in 2004 for two drug related offences (Case #39, female hacker and fraudster, aged 28 at time of offence).

You began using amphetamines, initially orally, but later as a daily intravenous user. At one stage you were into smoking crystal amphetamine, or “ice”. Your heaviest use of amphetamines was around 2007 to 2008. You spiralled down in 2007 as the result of the breakdown of your five year relationship with your partner. You then moved to yet another relationship and were introduced, or re-introduced, to the intravenous use of drugs, particularly amphetamine (Case #45, female hacker, aged 32 at time of court appearance).

While some of the active and former offenders interviewed in study three denied that they were addicted to computers, others did not. There was some evidence arising in all three studies that there was an element of computer and internet addiction:

By April 1994 he had no duties of substance but was given access to a data base, apparently containing details relating to all Australian taxpayers. He began playing with it in order to test its capabilities. He became addicted to the system for the purpose of stress release (Case #23, male hacker, aged 29 at time of offence).

The internet as a whole, I feel that I’m addicted to quite heavily. I was, yeah, it’s really bad. I love the internet, it’s amazing… Ah, when I was at [university] I was heavily into it, because you were constantly doing horrible things, or you needed internet, yeah, like an addiction, you were able to just, you know, justify, yeah, let’s go find out, let’s go see, let’s find some accounts, let’s get some accounts (Interview #5, male hacker and fraudster, aged 22).

Oh yeah. Yes. I still am. Um, that is my main pastime. Simply because I have always been quite knowledge hungry. And, with the
computer, everything you need to know is kind of at your fingertips. Um, and I am a big fan of videogames, online gaming, which is quite addictive. Um, yeah, and just the fact that everything you could ever want is kind of at your fingertips (Interview #6, male former hacker, aged 18).

Yep. For sure. Take computers off them, as we tend to do, when you get arrested. And, so this is a penalty worse than death to them (Law Enforcement Officer #1).

Ah, some of them are. You know, I've been to warrants where the guy wasn't particularly worried about getting arrested, he was more worried about us confiscating his computer (Law Enforcement Officer #12).

However, even when admitting that they were addicted to computers, those interviewed in study three denied that this was the reason for their offending or should be used as a legal defence:

Nup. There's no reason. I mean, being curious isn't a defence, well, it depends on what sort of crime, but, you know, addiction to drugs is different to an addiction to, you know, almost the adrenalin that you get at a computer, it's different, it's not the same. It's a very, it's a slippery slope I think, the way that I'd put it. If you were to allow someone to defend themselves using that, you know, if I were to get busted, by all means, I'd use it, but I wouldn't actively admit it. It's like a sex addiction, it's not real, don't try and sell something that's non-existent (Interview #5, male hacker and fraudster, aged 22).

No, I don't see why it would be a legal defence unless it is something to do with insanity (Interview #7, male hacker, aged 35).

Financial issues

Financial problems was another commonly occurring theme that arose in the data in relation to fraudsters, but not for those involved in hacking:

While you were visiting family in Nigeria in 2006, your wife had accumulated approximately $96,000 in credit card debts and failed to make monthly mortgage repayments on the two properties in Perth. Upon your return, the financial circumstances which
confronted you were stressful and you began to gamble at the casino in order to make payments (Case #18, male fraudster, aged 29 at time of offence).

In June 2006, after two years in this position, [he] was in financial difficulties as a result of over-spending on credit card purchases. He decided to solve his problems by using his employer's computerised accounting system to transfer money electronically into his own bank account, disguising the payments as payments to one of the company's suppliers (Case #46, male fraudster, aged 43 at time of offence).

He has a history of poor financial management. He has been bankrupted once in the past (Case #47, male fraudster, aged 28 at time of offence).

You then discovered the vulnerability of POLi and began this scheme as a means of building up a fund to clear debts which by then amounted to some $40,000 (Case #50, male fraudster, aged 22 at time of the offence).

What I do know is that you have, I mean, there's different levels of the online auction fraud. There's those people that have um, I guess, been selling normally, they hit a bad patch in their life in terms of oh, they can't pay their rent or something, and think oh, that's a pretty easy way to get money... Probably a good proportion of [fraudsters] are unemployed or employed in low paying jobs and they're doing it to get, especially opportunists, they're doing it to get money to, I mean, some of them are saying, it's to pay the bills and stuff like that (Law Enforcement Officer #11).

Sometimes the family, like, the online fraud ones are generally people that obviously have big financial issues, that just get hooked up into the organised crime syndicates (Law Enforcement Officer #7).

In total, four of the 42 males in study one (9.5%) were reported to have suffered financial problems. In contrast, four of the 12 females in study one (33.3%) were found to have landed in financial difficulties:

It appears that she had a long history of compulsive spending which was based on a chaotic early childhood. Some four or five years ago she took out a loan from a finance company without her husband being aware of it. Thereafter, she was always in debt. She
had not been able to manage money for family needs because of her inability to control spending, especially in recent years. Only in those more recent years did the impulse to spend become really uncontrollable (Case #3, female hacker and fraudster, aged 27 at time of offence).

The psychiatric report ... indicated that her loss of control over the spending of money had arisen from a general depression caused by absence from her family and an inability to confront reality. As the report indicated, "She had assumed the financial decision making in the household since moving from Sydney, and she was able to conceal the increasing financial difficulties from her husband". Her reckless spending pattern led her to devise the scheme of defrauding her employer. I was informed by her counsel that an additional motive in her spending of moneys was the provision of luxuries for her husband (presents, restaurant meals, etc.) to compensate for her inability to have a child, the only prospect of child bearing being through an IVF programme (Case #30, female hacker and fraudster, aged 22 at time of court appearance).

Your counsel told me that your husband never lets you have any money at all – even money that you have inherited and money that you are entitled to receive from Centrelink. The Crown prosecutor told me that your husband does not trust you with any money because he believes you have a gambling problem. I am not in a position to decide whether that is correct. However it seems clear that you committed these crimes because you were unable to get any money from any other sources (Case #43, female fraudster, aged 45 at time of court appearance).

The motivation appears to have been that she was living beyond her legitimate means (Case #52, female fraudster, aged 35 at time of offence).

Conclusion

Computer crime offenders typically do not have any prior criminal record. When a prior criminal history is present it is more likely to be in relation to a fraudster rather than a hacker. There was little evidence that offenders also engaged on violent offending, with offences typically similar to those for which they were before the courts in relation to, including fraud conducted without the
use of computers. Therefore, labelling theory may be more applicable to offences involving fraud rather than unauthorised access.

Strain was identified in a number of areas, particularly in relation to mental health and drugs, gambling and computer addictions. Gambling addictions were more common for fraudsters, while hackers admitted to being addicted to computers and the internet. Drug use and abuse was found amongst both hackers and fraudsters. Female offenders were again found to have more adverse backgrounds, with experiences of drug addiction, financial problems, and were more likely to have prolific offending histories. While the conceptualisation of strain as adverse personal circumstances is consistent with other research testing Merton’s strain theory, it does depart from the original formulation that it is the structural organisation that sees some being systematically denied access to legitimate means.
Chapter 10 ~ Apprehension and Punishment

According to rational choice theory, views about the chances of apprehension and the severity of punishment are influential factors as to whether people will offend. This chapter examines what offenders think about the likelihood of detection, and what how severe they perceive the potential costs of being caught to be. In addition, this chapter examines techniques that offenders may use to escape law enforcement attention and their attitude towards the police.

Views about detection

The active and former offenders interviewed in study three advised that they perceived the chance of being caught as very low:

Um, I don’t think I will get caught, because I don’t actually advertise. Well, except for now. I trust my friends, I’m mean, and it’s not really like I’m doing it to make money, so I don’t really think that the police would come after them, it’s just for my personal usage… But I’m really just small-time so I don’t really expect anyone to come looking for me (Interview #3, male hacker, aged 22).

Oh, no, not particularly [worried about being caught]. We didn’t really do anything that mattered, as far as we were concerned… In fact, I basically assumed that I would never get caught, which was a fair assumption, I never got caught (Interview #4, male former hacker, aged 49).
Law enforcement officers agreed that offenders did not think that they were likely to be detected:

[Their perceptions of being caught are] slim to none. I think, because, like I was saying, it takes a little while before they come to our attention, and obviously we have to look at the ones that are going to be, you know, that are the most serious threats out there, so a lot of them can offend for a long time without anything happening to them. And, you know, so they are quite surprised when we come through their front door in the morning (Law Enforcement Officer #14).

We've seen, sort of, evidence where they think that really law enforcement aren't sort of well-equipped to, you know, look into this space. That they are anonymous and that the chances of them getting caught due to the sheer number of people online are quite low and so forth (Law Enforcement Officer #15).

They think there's no chance of getting caught (Law Enforcement Officer #9).

The environment in which offenders were operating provided many opportunities for them to cover their tracks and therefore minimise their chances of detection. These were often technical, for example:

Having gained access to those accounts he installed unauthorised remote access and administrative software called "remotely anywhere" that enabled him to access and alter data upon the American computers at any time and without detection by virtue of the programme masquerading as a Windows operating system. Once "remotely anywhere" was installed, he then installed software facilitating both further compromises to the computers and also the concealment of his own activities (Case #28, male hacker, aged 40 at time of court appearance).

The appellant deleted and added files, put on messages, made sets of his own users and operated them for his own purposes, changed the passwords of authorised users, enabling himself to use the system as if he were they, and regularly deleted the filed "Accounts Journal" and "Systems Journal," which would have recorded his activity and at the same time the activities of others. On one particular occasion he was astute to detect a special programme, inserted by the legitimate operator to trap him, and deleted it. He
successfully attained the status of “SYSMAN” of particular computers, enabling him to act at will without identification or authority. Furthermore, having attained SYSMAN status he left it open for any other user to take advantage of it if they discovered it was available. The computers failed, were unable to operate properly, or had to be shut down for periods of time (Case #29, male hacker, aged 21 at time of court appearance).

[He] arranged for the audit trail on the … computer to be shut down, thus making it difficult for a check to be made on what he was about to do (Case #31, male hacker and fraudster, aged 27 at time of offence).

The FBI's international investigations revealed the extent of your efforts to remain unidentifiable. You set up an international banking account at Egold.com using a false identity and instructed the complainant to deposit the US$10,000 into this account. You also subscribed to Findnot.com which provides untraceable internet access to prevent you from being identified or located when sending emails (Case #36, male hacker and fraudster, aged 17 at time of offence).

Another bot code allowed [him] to operate through other computers as a proxy, making it harder for his activity to be traced back to him (Case #37, male hacker and fraudster, aged 16 at time of offence).

Offenders also changed their physical location as a measure to escape the attention of law enforcement:

... the Appellant was considering relocating to Tunisia in order to avoid the United Kingdom authorities... efforts were made to locate the Appellant and his wife in the United Kingdom but it was discovered that they had relocated to Tunisia (Case #17, male hacker, aged 36 at time of court appearance).

Yeah, the online fraudsters, um, it would be difficult to say without really, we've got the high end that just do it all the time, and they jump jurisdictions, across states. You know, they'll come to [state] and hammer every type of online fraud you can think for a short period of time, couple of months, and then they'll go, by the time we start figuring out information about the offences they've moved on... It's very difficult to then coordinate an investigation between multiple jurisdictions (Law Enforcement Officer #2).
In addition, offenders were perceived as taking advantage of the problems faced by law enforcement officers when investigating cross-jurisdictional offences by purposively operating across borders:

Yeah, you know, multiple jurisdictional makes it, unfortunately, police across the world haven’t caught up, you know, criminals don’t have jurisdictional boundaries, we do, and we operate within them. And they know that, so, they know that a way to avoid getting caught is to distribute the network and distribute the offences across jurisdictional boundaries (Law Enforcement Officer #8).

Another way offenders attempted to evade detection was to ensure that the proceeds of their crimes did not go directly to them, but rather was laundered using a variety of methods:

Yeah, basically, so you’ll have a couple of cut outs before the money goes to the person who’s actually committed the actual e-fraud offence. And by the, even if you are able to track the money back to them, proving their knowledge that those monies were the proceeds of a crime can be extremely difficult. Simply because they’re removed from the actual dealing with the cash by two or three steps (Law Enforcement Officer #13).

Um, probably because it’s harder to track, you know, money is going all over the place, if one person puts the ad, another person takes the money and forwards it, another person receives it, the more links in the chain there are, the harder it is to get caught. And put it all together, and be held responsible for the entire fraud. So I think it’s a mitigation, circumstance, and it’s also a spreading of the workload… There’s a fair bit of organising involved, so I think many hands make light work, and it’s also it’s a mitigation of the workload and also a mitigation of getting caught and culpability (Law Enforcement Officer #8).

Offenders also selected targets that they perceived as being less risky to avoid detection or investigation:

No, ah, when you go with the bigger companies it’s easier to get what you want because, for the most part, they’re busier, their policies and procedures overlook everything. Where smaller companies tend to have more of a wire tooth comb policy. You
know, they go through everything a little further. So it’s easier to
deal with something big or something like that (Interview #1, male
hacker and fraudster, aged 27).

It’s the old line of low value fraud at high volumes, so, um, which
traditionally has always been an issue. Whilst for policing agencies
more broadly I guess, if you get a ten million dollar fraud or
something, the chances are it’ll be investigated. If you get ten
thousand one thousand dollar frauds, you know, it’s a great deal
more effort trying to link them and to make sure they get the
corresponding resources (Law Enforcement Officer #13).

Not really. I mean, again, like you said before, the risk of getting
caught, so most of the younger ones wouldn’t go after big financials,
that sort of stuff because they know that there’s a possibility that
that big financial is going to have good logins or will be able to work
with us quite quickly, whereas if they went up to some random web
shop, just score a couple of dozen credit cards, chances are that
that web shop is not going to have very good logins or anything like
that, so they won’t get caught (Law Enforcement Officer #14).

Oh, I think it’s probably primarily like, um, you know, I would
suggest more the lower end, like people don’t secure their systems
and so forth. I guess the small-time hackers wouldn’t go for big-time
targets because, and this is in my opinion, they would be subject to
more scrutiny. Whereas if they are sort of, you know, hacking into
people’s MySpace accounts and so forth, they are not going to be
subject to a greater scrutiny (Law Enforcement Officer #15).

One law enforcement officer advised that fraudsters were more likely to try
and evade detection using non-technical methods such as physically moving
location, while hackers were more likely to try and anonymise their activities
using unsecured Wi-Fi and proxy servers:

But what [fraudsters] do is they use, um, various systems which
make it harder for the police to actually locate where they are. So
they’re not going to sit in a house and use the dedicated landline to
connect to the internet and commit offences because they know
that’s going to be tracked back to them. What they tend to do is
they’ll use 3G wireless modems so they it actually can’t be tracked
back to a physical location. Even if it’s in their name, we can’t
physically track them down, so by the time we actually become
aware of them, and start trying to locate them it can be three, four,
five months down the track before we actually manage to catch
them at a particular residence… They move around, they tend to move around a lot just because they know the police are going to be after them. Whether it be with friends or relatives… Hackers, they can um, hackers tend to have a lot more ability with what they’re doing. Um, they don’t need to move around, I mean, they can operate from their own homes. They will either, again, you know, use the situation or the circumstance which we’ve seen, but, um, the ones we have seen, they operate from home, they’ll either use proxy servers to conceal their identities, so they move around different points to compromised computers or proper proxies throughout the world before they actually hit their target, so it can’t be tracked back to them. Or what they’ll do is they’ll use, ah, open Wi-Fi from neighbours. They have a lot more skill and, generally speaking, it’s, you’ll only catch that hacker if their systems stuff up. Like if something that they’re using to conceal their identity, for whatever reason, fails and they’re sending their true IP address. Or um, if, their motivation is to create havoc because of bad will, you know, there’s been a fall out, so they’ve been flagged as a suspect in the first place. Or they’ve made comments or they’ve admitted to it. If you have a true hacker, you’re not going to catch them. We had a, we had one offender which we caught in Brisbane who was actually an international offender and another international jurisdiction had been chasing him for a number of years and hadn’t been able to catch him. And it was only because his systems failed on one particular occasion that his IP address was identified. And they asked us to get involved and lo and behold, we managed to catch the guy. Just through pure bad management on his behalf. He was actually operating from home (Law Enforcement Officer #10).

Views about punishment

During studies two and three it was apparent that offenders and law enforcement officers had different views about punishment. The active and former offenders perceived the punishments as severe:

Um, it is hard to get caught. The penalties are severe but, I mean, the chances of getting caught are quite low, especially if you take the proper precautions (Interview #6, male former hacker, aged 18).
Offenders were also concerned about other potential negative impacts detection would have, in relation to work chances as well as other aspects of their lives:

*It would probably also affect my chance to get residency in this country* (Interview #3, male hacker, aged 22).

*I'd probably lose my job, obviously. I don’t know, effectively my whole, I couldn’t work, because every job that I would go for, I don’t think, I might be able to have a blue card, but, you know*… (Interview #5, male hacker and fraudster, aged 22).

*Um, I guess the biggest penalty would just be having a criminal record. That is something that can really ruin your life* (Interview #6, male former hacker, aged 18).

Offenders also indicated that if caught they probably would not reoffend:

*...I was penalised and it was significant, I wouldn’t… Yeah, probably I wouldn’t continue. No* (Interview #1, male hacker and fraudster, aged 27).

However, law enforcement officers perceived the penalties handed down by the courts as being insignificant when compared to other crime types:

*The online fraudster, that can be very rudimentary, some of them have just realised that you can make much more money with far less risk and the penalties are severely reduced. If you run into a service station to stick them up today, 300 dollars, top dollar, you’re going to get out of it, from what’s in the till. You might do an eight or ten year lag for armed robbery, you know, why would you do it? You know, they can make five, ten, 15, 20 thousand dollars a day if they wanted to online, with far less chance of detection. And if they do get caught then the penalties are significantly reduced* (Law Enforcement Officer #1).

*Whether it’s because it’s easier to commit, it’s easier to get away with, and also, if you are caught the courts tend to give lesser penalties, you know, no one’s physically hurt. Now, you’ve got less chance of actually physically hurting someone… No, I think the courts, they don’t, I think that’s why a lot of the traditional crooks are moving to the cyber areas, because traditional forms of um, crime,
break and enter, robberies, those sorts of things, you get, not only are there a potential to hurt someone, but there’s also greater penalties involved. Cyber related offences, no one’s hurt so the courts don’t tend to give as much weight as other offences, so the penalties are lesser (Law Enforcement Officer #10).

Ah, however the courts have yet to, I’ve never had a custodial sentence, put it that way. The courts just do not take it seriously at all (Law Enforcement Officer #12).

Ah, well, just basically that sentencing for these types of offences are, you know, have been very low. And it’s not until, because word travels very fast on the Internet, so things will change, I mean guys are getting 10 years in the US for things that they’re not even getting a conviction recorded for here. So I think, you know, if the sentencing regime picks up then that will have a great effect on the Australian environment. Particularly with the younger ones… Oh, a lot of them think, you know, I’ll just get a slap on the wrist kind of thing. Yeah, or they’ll get sentenced and go online and go, yeah, slap on the wrist, good behaviour bond (Law Enforcement Officer #12).

And the problem we have also is there is, no one’s really been made an example of. You know, to be brutally honest our sentencing sucks. You get someone who admits to attacking the government online and gets no conviction recorded and a $500 fine, I mean, what the hell is that about, they admitted to attacking the government and nothing happens. So, and with that sort of thing going on there is no disincentive. And because there is so many of these people out there and there are so few of us it is quite hard to make a real sort of generational impact… They are always talking about it. Especially the ones who are up before the court, they’re always online talking about their upcoming court dates and how their lawyer just reckons they’ll get a fine and they’re going to be fined et cetera (Law Enforcement Officer #14).

Like, even that bloke that got seventy thousand, he, um, even though he lost all the property he, um, he only got a, I can’t remember what he actually got now, but, it was something similar to just a suspended sentence. You know, it was only for say, six months, so it wasn’t a harsh penalty at all (Law Enforcement Officer #6).
Attitude towards law enforcement

Holt (2007, p. 194) described hackers’ attitudes towards law enforcement as “antagonistic”. However, in many cases the judiciary noted offenders had cooperated with law enforcement by way of making admissions, answering questions, assisting with details about accomplices and providing passwords. For example:

He also submitted that the phishing scams would have been particularly difficult to detect, had you not confessed on your own accord… Furthermore, it was you who approached the Police and confessed to the second set of offending which could otherwise have remained undetected (Case #36, male hacker and fraudster, aged 17 at time of offence).

You co-operated with the police investigation, particularly by providing the police with the passwords to your computers so they could have access to them (Case #54, male hacker, aged 19 at time of offence).

Some of the law enforcement officers supported the view that computer crime offenders could be cooperative, particularly when compared to other crime types:

Yes, they will, they’re so, the online crook is a much, there’s no politically correct way to say it, but um, they’ll roll over much much easier than a harder core street crook. Like, a street crook would stand up and say do your best and let’s see what you’ve got. But a lot of these guys come in, and I was going to say lean on them, but we don’t even lean on them, you can mildly raise your voice. Or simple the presence of a couple of detectives at the table, they’ll start to go, well it was these guys that did this and these guys did that and, um. So it’s a bit like shelling peas with some of those guys, they tend to, I don’t know, it’s not, it’s not, sort of, they’re more willing to probably cooperate in that regard, probably not in regard to, they’re not willing to confess all themselves (Law Enforcement Officer #1).

Yes, and also, to be honest, some have you know, assisted police as well. You know, so they kind of got dragged into it, and once
you've knocked on their door they've gone oh, ok, well these are my account logins and this is how I do my business and so forth (Law Enforcement Officer #13).

Nonetheless, law enforcement officers also advised that not all offenders were cooperative:

*What they all tend to do, they all think they’re pretty much smarter than us. A lot of them do. I don’t know why you bait the police and carry on with the excuse. You don’t see it in other crime. You don’t get your armed robber, you’ll never catch me dickheads, you don’t hear that because they go well how about we just keep a low profile and stop taunting the police and go about our crimes. They’ll find things to taunt us. And even do at times online, or via emails and. Hence, we locked a guy up for denial of service on us in [another state], it’s going to court shortly and it’ll be big, but he bombarded us with about one point two million emails saying you need to show more respect to those smarter than you. He did send so many of them his bots crashed [the other state’s] computer servers. Um, so we see that, the taunting and we’re much smarter than you, which I think, they often think that* (Law Enforcement Officer #1).

*They don’t tend to open up too much when we interview them. They either, um, give you half truths or, um, don’t want to tell you anything* (Law Enforcement Officer #10).

*Ah, no, for example, if, you know, we’re looking at a, say an unauthorised access, um, so they’ve hacked into someone’s server, they’ll sort of say oh, I only did it the once, you know, I just went in and I was annoyed so, you know, I deleted this file and that was it. And, you know, we’ve got logs showing, you know, them coming in and out, in and out, in and out, so, and then when you present that to them, they’re sort of oh, ok, yeah ok, well I did this at this time and did that, so they won’t come out and say oh yes, I hacked in forty-two times in that one month. Um, again, they will only, you know, they’ll limit their involvement* (Law Enforcement Officer #3).

The interviews with active and former offenders revealed that there was a generally low opinion of law enforcement’s ability to investigate these types of offences, for example:

*Ah, no. No, they have no ability whatsoever. Police tend to be recruited from a certain part of the population that typically do not
explore technology areas too much. So, um, they are not the right people, I mean, it is certainly within the police's jurisdiction to investigate it, but I don't think they recruit the right people to do it (Interview #7, male hacker, aged 35).

Conclusion

While police officers did not perceive the punishments handed down by the courts were severe enough to achieve a deterrent effect, offenders were concerned about negative consequences if they were caught. Negative consequences were not limited to criminal sanctions, but also included impacts on their career and residency status.

While offenders did perceive the potential consequences as serious, they did not see them as being a deterrent from offending, as it was believed that there was a low likelihood of being detected. The online environment offers a variety of ways for offenders to anonymise their attacks and to operate across jurisdictions in order to impinge on the ability of law enforcement to conduct investigations. This leads to a sense of being able to operate with impunity as long as precautions to hide their identities are adhered to. In relation to routine activity theory, therefore, it would appear that when considering the cost of offending in the online environment, the likelihood of detection is a much stronger influence than punishment severity.
Chapter 11 ~ Synthesis

The aim of this research is to develop a theoretical understanding of computer crimes that compromise data and financial security. To achieve this aim, this thesis examines how well existing theories of criminal behaviour account for computer crime, whether a new theoretical model is required, and if so, what an integrated model should look like. This research contributes to our knowledge about, and understanding of, crimes that occur in the online environment by applying established theories that have been used to explain offences such as property crime, violence, delinquency and drug use.

The results of the research have been presented in the previous six chapters. The selected theories informed the data collection, which examined factors within offenders' lives such as social interactions, including with fellow offenders, family upbringing, employment, education and skill development, life events, including adversity and strain, as well as motivations for offending and views about apprehension and punishment. This chapter shall begin by applying the research to the theories outlined in Chapter 3 to assess their ability to explain these types of offences.

In this chapter a new theoretical model of computer crime incorporating offender initiation, maintenance and desistance is proposed. Understanding the factors that are conducive to offending, as well as those that are associated with a reduction or cessation of offending, can assist with proactive offender-oriented crime prevention methods. These include providing legitimate opportunities to
obtain the benefits otherwise achieved through offending, targeting potential offenders early in their life course, and targeting the circumstances that offenders or potential offenders may be in that are conducive to crime. This chapter therefore explores recommendations for the detection and prevention of computer crime offences, as well as outlines areas for future research.

**How well do existing theories of criminal behaviour account for computer crime?**

Sutherland’s (1949) theory of differential association relates to how criminal behaviour, and the definitions favourable or unfavourable towards committing crimes, is learnt in association with others. The operationalisation of definitions relating to criminal behaviour included beliefs about when it is ok to break the law, whether it is morally wrong to commit offences, whether the offending behaviours are serious, as well as the attitude of family and friends towards these activities. Associations with others included friends and those known to the offender who had engaged in hacking or computer fraud, and whether friends or family would approve of their involvement or support their decisions.

In relation to differential association, it was found that the offenders studied had poor offline social relationships, however had cultivated extensive online communities, which led to computer crime through the influence of others. It was also identified that being involved in an online gaming community was a pathway to associating with other offenders. Offenders worked together to commit offences, to learn and teach others how to hack and commit fraud, and to
trade tools and sell credit card information. The differences in age for those involved in computer fraud and hacking, with fraudsters generally being older, may reflect the “who” and “what” they are exposed to. The internet allows offenders to further the reach of their social groups, interacting with others across jurisdictions that they otherwise are unlikely to come into contact with. Therefore, definitions that are favourable towards offending, as well as the necessarily technical knowledge and skills, can reach a greater audience.

According to Hirschi’s social control theory, crime occurs when social control is loosened due to the weakening of social bonds (Vold et al., 2002). The first social bond is attachment to others, operationalised as the relationship with parents, spouses and partners, children, friends and co-habitants. Commitment to society was operationalised as commitment to education and work, while involvement in conventional activities included employment, religious undertakings and the time spent on extra-curricular activities. The fourth social bond, moral beliefs, was operationalised to include respect for the police, when criminal behaviour is acceptable, and attitudes towards victims.

Some elements of social control theory were found to apply to the computer fraudsters studied in this research. For example, fraudsters were generally found to have weak attachments to others, including disruptive families and poor intimate relationships. However, hackers generally reported having a close family, and enjoyed good intimate relationships if they were of that age, although, as mentioned before, their offline social skills outside these areas appeared to be lacking. Hackers also appeared to be committed to society, with interests in other activities, although their interests in computers sometimes
overtook these. Offenders appeared to be involved in conventional activities, such as work or education, according to their age. According to social control theory, involvement in conventional activities restricts criminal behaviour, however in relation to computer crime the workplace was found to provide opportunities for crime. Finally, in relation to moral beliefs, offenders tended to agree with the rules of society, but offended regardless.

It is argued that along with social change, there have been changes in what are considered to be conventional activities. In today's digital environment, interactions with others, employment and even recreational activities, such as gaming, are conducted online. It appears that, while social networking sites may strengthen social bonds, the internet also increases opportunities to offend, the reach of deviant peer networks, and can provide a disinhibiting influence with the perceived anonymity and the physical distance between offender and victim.

The five techniques of neutralisation are theorised to enable offenders to drift in and out of criminal activities by justifying their actions (Sykes & Matza, 1957). Denial of responsibility was operationalised as offending behaviour being out of the offender's control due to computer addiction or the influence of drugs or alcohol. The denial of injury neutralisation technique was operationalised as beliefs that offending is acceptable when there is no damage to computer systems or data, or when the victim is insured or can afford to cover the loss. Denial of the victim included who are suitable targets or deserving of victimisation, as well as how the internet mediates feelings of guilt due to the physical distance between the offender and the victim. The conceptualisation of the technique condemnation of the condemners included how offenders viewed...
their own behaviour compared to that of governments and policing agencies, while appeal to higher loyalties included offences that were claimed to have been committed for the benefit of others.

There was some evidence that offenders engaged in techniques of neutralisation, particularly denial of injury when there was no loss to individual victims, and denial of the victim where they did not secure their systems, were undertaking questionable activities, or were perceived to have done them wrong. Offenders also avoided targets when it was seen that they were undeserving of victimisation or there was the potential for innocent parties to be harmed. Use of condemnation of the condemners as a technique of neutralisation was evidenced where it was accused that the victim had caused harm, such as military targets. Offenders also appealed to higher loyalties when their actions were seen to be in the common good, such as increasing transparency or revealing vulnerabilities. However there was little evidence of denial of responsibility, with hackers advising that even though they considered themselves to be addicted to computers, they did not perceive this as warranting a legal defence.

Many of these variations in techniques of neutralisation, while not necessarily unique to the digital environment, do seem to be common to these types of offending when compared to offline offences. In particular, these techniques related to incidents involving vulnerable computer systems that would otherwise be more difficult to compromise. In these situations, targets were seen as deserving of victimisation and the offenders perceived their actions as being for the greater good, as it would ultimately encourage others to improve their computer security.
According to rational choice theory, offending occurs when the perceived benefits outweigh the perceived costs (Cornish & Clarke, 1987). For this research, the concept of benefits included those that were actually obtained, as well as those that were perceived to be achievable. Costs were conceptualised as personal costs, such as guilt or lost time, as well as the likelihood of detection by police, victims, family and friends, and the severity of punishment that would be expected, including legal sanctions, loss of job opportunities, or disappointment expressed by those close to the offender.

Rational choice theory was found to be a strong explanation for computer crime, particularly due to the nature of the internet. The benefits for fraudsters were mainly financial gain, particularly when this was used to feed drug and gambling additions. Hackers had additional benefits, including retribution and revenge, testing their skills, and pleasurable feelings arising from excitement, power over others, social status and sexual gratification. Offenders appeared to calculate the cost of their activities, and as such selected targets based on the likelihood of detection and perceived benefit, avoiding those likely to retaliate and focusing instead on those who were perceived to be low risk. The nature of the internet allows offenders to gain access to a large pool of potential targets with little cost while hiding their true identity. Offenders also were perceived to take advantage of the challenges faced by law enforcement by crossing jurisdictions.

Although offenders observed the potential penalties as severe, they had a low opinion about the ability of law enforcement’s capability to investigate these matters and therefore saw the chance of detection as being low, as there are steps that can be taken to hide or mask someone’s identity and to launder funds
in order to obfuscate the money trail. Offenders were concerned about other negative outcomes relating to detection, such as having a criminal record and decreased employment opportunities. There was also evidence that offenders ceased their activities when they gained meaningful work or entered a relationship, which could reflect the increased cost their actions could have on their lives. Therefore, the results indicate that it is the likelihood of detection, rather than the severity of punishment, that is likely to have the greatest effect on offending.

According to Becker’s (1963) labelling theory, those who are labelled as criminal adopt this label and therefore offend in order to act in accordance with how they are perceived. Labels may be applied to certain groups, such as young males, which explains initial lawbreaking, while subsequent labelling explains why offending continues. There are a number of people and institutions that may label offenders as such. Labelling by the criminal justice system was conceptualised as whether participants had been stopped, charged or arrested by police, or convicted of, or punished for, a crime. Other formal labelling included labelling from educational facilities, while informal labels included those bestowed by family and friends, as well as deviant peers. The research also examined offenders’ self-concept, such as whether they identified themselves as being a hacker or fraudster.

There were mixed results for labelling theory. It was claimed that that the laws reflect the interests of certain powerful parties. There was also some evidence of labelling by the criminal justice system, although this was limited to fraudsters, who were more likely to have a prior criminal history than hackers.
Previous offending related both to unrelated offences and similar offences, including dishonesty in the offline environment. Law enforcement advised that they were more likely to monitor those that they had already detected offending. There was also evidence of other formal labelling, with offenders reporting that they had been in trouble at school. Also in support of labelling theory, it was identified that informal labelling was a benefit to offenders, as one of the identified motivations for hackers was to gain kudos and respect from the online environment. However, there was little evidence of informal labelling beyond what took place when communicating with other offenders online, and those interviewed advised that they did not perceive themselves to be hackers as portrayed in the popular culture.

The lack of formal labelling by the criminal justice system is likely to be reflective of the challenges faced by law enforcement when investigating and prosecuting online offences. Rather than having contact with the criminal justice system increasing later offending, these problems facilitate offending in accordance with rational choice theory, as offenders perceive the costs of offending to be negligible due to the low chance of detection.

According to structural strain theory, criminal behaviour occurs when culturally defined goals, such as wealth, cannot be met with the available means (Merton, 1968). Offenders may innovate, in that they find criminal ways to obtain the goals, retreat and therefore reject the goals and the means, or rebel against the societal goals and replace them with their own. For this research, strain was operationalised as the offenders’ perceptions about the chances of achieving
their goals, such as educational, employment or wealth, and what frustrations they had encountered that stopped them from goal attainment.

Structural strain theory was found to apply only to fraudsters. Hackers were more likely to have the means available to them to achieve their goals, with better education and, when of age, stable employment and generally being better off financially. Although many of the fraudsters had jobs, they often offended in the course of their employment. There was evidence of other types of strain among the sample of fraudsters, such as medical conditions and mental health issues. Addictions to drugs, gambling and computers may indicate that offenders had replaced their goals and retreated.

The internet offers many opportunities for innovative fraudsters. Existing businesses, such as online trading sites, can be utilised for illegitimate means. Scammers have a wide audience to reach, and the means to do so cheaply through the use of email, social media sites and banner advertisements. Scammers can also increase the perceived legitimacy of their offending, such as the development of professional looking websites, that may actually replicate known and trusted brands and organisations.

The findings from this research confirmed that, within the three studies, there was a low female involvement in computer crime, however this was more pronounced for hacking than fraud. Although females were involved in less serious, less technical and peripheral roles they were often prolific offenders. The female offenders were also identified as being older than their male counterparts, suffering more adverse life events, having less happy families, being addicted to drugs or gambling, and more likely to be financially strained.
Reasons for the lower involvement of females included a lack of interest in computers, a lack of involvement in crime in general, societal factors shaping how females are expected to behave, and barriers stopping them from being accepted by the online community.

A number of differences were identified between those who were involved in hacking only, and those that were engaged in fraudulent behaviours. For example, fraudsters were more likely to be older and more females were engaged in fraud compared to hacking. Hackers were found to come from more privileged backgrounds with closer family relationships, have greater computer skills and as such use more technical methods to avoid detection. Due to hackers’ young age when compared to fraudsters they were less likely to be employed or in an intimate relationship and more likely to still be in school. In contrast, fraudsters were more likely to be offending during the course of their employment or be unemployed, have a prior criminal history and have experienced financial strain.

The internet amplifies and enhances factors that are theorised to be conducive to crime. These include interactions with deviant peers, opportunities to offend, and a low likelihood of detection. However, it is not only the online environment that affects online offending, with other factors also being present. Adverse social and economic conditions were also found to be relevant; these were particularly pronounced for fraud type offences that are motivated by financial gain.
Is a new theoretical model needed to better explain computer crime?

Many of the theories that have been examined in this research provide unique insights into computer crime offending, however none provided a full explanation of why both hacking and computer fraud occur. However, some theories did offer partial explanations as to how offenders initiated their behaviour, maintained their behaviour and finally, desisted from crime. Some parts of theories were found to be compatible, for example, although labelling theory and rational choice theory have different implications in terms of crime prevention, in relation to hacking the findings indicate that they could both be applied. They were compatible in that informal labelling by the hacking community may lead to further offending, as gaining kudos and esteem was identified as a benefit to offenders, one of the components of rational choice theory.

The development of an integrated theory that explains both hacking and computer fraud is considered to be necessary as it will assist in developing crime prevention approaches for these interconnected offence types. These exploratory findings are used to inform the theoretical model, which can later be tested empirically. The following section will integrate compatible parts of the theories to create a new theory of computer crime offending.

What should an integrated model look like?

An integrated model, borrowing heavily from rational choice theory as well as differential association, techniques of neutralisation and structural strain theory, is proposed. The aim of this integrated theoretical model is to explain
both hacking and computer fraud. To begin with, from the research findings it is proposed that there are two pathways to computer crime, namely presented opportunity, such as in the workplace, and differential association, or the influence of others. However, maintenance and desistence from computer crime follow similar trajectories regardless of the initial path taken.

In relation to initiation, those operating alone, such as fraudsters offending in the course of their employment or on online auction sites, were found to begin due to opportunities that were presented to them. These opportunities were taken advantage of when the offender was experiencing some type of strain, such as economic problems, job loss, mental health issues, or gambling and other addictions. While these offenders may operate alone, their methods and inspirations may be acquired elsewhere.

However, those operating with others were found to have a different pathway to offending, namely through differential association. These offenders were more likely to be involved in offences requiring technical expertise or organised crime. With an interest in computers, technology or gaming, would-be-hackers began by communicating online, during which they learnt the techniques to commit computer crime as well as shared the definitions and techniques of neutralisation that enabled offending to occur. Similarly, fraudsters involved in organised crime began by associating with others who are engaged in criminal activities, including offending off-line before turning to the online environment.

These trajectories go some way to explaining the gender imbalance. For example, more females were involved in opportunistic fraud as they may have similar types of opportunities presented to them as males. The research found
that many of the females that were involved in fraudulent behaviour had experienced substantial strain prior to their offending. However, in relation to hacking, females may be less likely to have an interest in computers and technology due to societal factors such as sexual stereotyping, and may be less likely to be accepted by the online community, which was found to be a male-dominated environment.

The trajectories also explain the age differences, with female offenders, who were more likely to be operating alone, generally being older than the male offenders. Similarly, those involved in computer fraud were older than hackers, who again were more likely to be male. Those who are older have had greater exposure to scenarios that may induce strain, and have a larger range of opportunities presented to them. In relation to the second pathway to offending, young people, particularly males, were exposed to a subculture of gaming and online interaction that related to their age.

Common to both trajectories, offending behaviour was maintained due to the low likelihood of detection offered by operating in the online environment, as well as the benefits available to offenders. The research found that offenders generally perceived the likelihood of being detected as low, and this held greater weight than the harshness of the available punishments. Benefits obtained from offending were, for fraudsters, mainly financial, while hackers enjoyed a greater range of benefits. These included skill development, fun and excitement, social status, power and sexual gratification.

Offenders desisted from computer crime when they no longer receive benefits from offending or when the costs outweighed the benefits. For example,
offenders may no longer experience excitement or obtain a sense of achievement from their activities. As offenders believed that the likelihood of being detected is low, costs associated with offending were mainly social in nature, for example, the amount of time they were engaged online, which may interfere with legitimate employment or intimate relationships. This model is presented below in Figure 1.

\[\text{Figure 1. Initiation, maintenance and desistence}\]

For example, someone experiencing strain, such as mental health or substance abuse problems or adverse life experiences, may find that they have opportunities afforded to them to partake in offending. These opportunities may
be presented in the workplace, or online, such as trading or commerce sites. This explains how solo offenders initiate their offending. The alternative pathway to offending is to first associate with other offenders. This association may begin on the online environment, for examples, through forums dedicated to technology interests or online gaming, although involvement may also occur offline, such as at school. During their interactions they become exposed to definitions favourable to criminal behaviour, as well as learning how to commit offences. Regardless of the pathway to offending, the behaviour is maintained while the benefits continue to be obtained and the offenders perceive the likelihood of detection as being low. Again common to both trajectories is desistance, which occurs when the benefits are no longer apparent or the perception or actuality of being caught increases.

The theoretical model proposed here falls under Garland’s (1996) concept of “criminology of the self”. Rather than offending behaviour arising from some pathological state of the offender, it is assumed that offending behaviour can commence, and cease, depending on the particular circumstances surrounding an individual. These circumstances may include what access they have to technology, the types of influences they experience, their opportunities, both legitimate and illegitimate, and those that they are in contact with, both online and in the physical space. It just so happens that individuals are subjected to different experiences, such as the female fraudsters that were found to have come from more adverse backgrounds than their male hacker contemporaries. Just as societal influences may impact on the likelihood of offending, such as the
kudos provided to skilled hackers, so may policy or technological developments that change the likelihood of detection.

Although computer crimes are not unique, in that they reflect crime that previously took place in physical space, it is the environment, or the “bottle”, to borrow Grabosky’s (2001) analogy, in which offenders operate that makes these types of offences distinctive. This environment provides many opportunities to offenders and creates a number of challenges for those who attempt to make cyber space a safer place.

**Recommendations for the detection and prevention of computer crime**

This research has informed the following recommendations by providing a greater understanding of the factors that are conducive to offending. These recommendations include providing legitimate opportunities to obtain the benefits otherwise achieved through offending, targeting potential offenders early in their life course, and targeting the circumstances that may lead to victimisation.

Target hardening is unlikely to discourage offenders whose motivations are curiosity and skill testing, as it provides them with a greater challenge. An additional crime prevention strategy is to provide legitimate opportunities to achieve their objectives instead. An example of a legitimate opportunity is mashup competitions, in which members of the public use and combine publicly available data to create new applications (Government 2.0 Taskforce, 2009). These opportunities allow highly skilled individuals to showcase their talents and be recognised in a way that can lead to greater life opportunities, rather than a criminal career. Also, as recommended by the Government 2.0 Taskforce (2009)
non-sensitive public sector data should be made freely available under a creative commons licence, which will enhance accountability and reduce criminality in this area as government data can be accessed legitimately.

Targeting potential offenders early, when they first become involved in online communities and gaming, would assist in fostering a culture of responsibility about one’s online behaviours. This would focus on countering the techniques of neutralisation and the definitions favourable towards online offending. This is a long-term strategy that could take some time to be successful. It is recommended that this be commenced at schools and incorporated into the curriculum relating to computer science. It is expected that forthcoming evaluations of intervention programs delivered in schools that address other technology-related behaviours, such as cyberbullying and sexting (Pearce, Cross, Monks, Waters, & Falconer, 2011; Slonje, Smith, & Frisen, 2013), would be useful in informing such initiatives.

The research indicated that increasing the likelihood of detection would have a greater impact on offending rates than increasing the costs of offending through harsher criminal penalties. Offenders acknowledged that the punishments for offending were already high, both in terms of punishments handed down by the criminal justice system, as well as how it may impact other areas of their lives, such as their future careers.

It was noted during the research that law enforcement faces significant challenges and hurdles when investigating computer crime offences. These include having the necessary resources and powers to investigate complex matters, the time required to conduct cross-jurisdictional investigations and
obtain evidence using current procedures, the lack of legislative uniformity across different jurisdictions, and recruiting, training and retaining personnel with the appropriate skills (Smith, 2001). The interviews with law enforcement officers identified coordinating investigations across jurisdictions as a particular issue that negatively affected their ability to detect offenders. Providing greater resources for investigating and prosecuting computer crime offences, as well as improving extradition and across-jurisdiction cooperation is required so that law enforcement can stake a significant claim in the cyber realm.

Crime detection can be improved by implementing a national reporting system that can be used to identify offenders that are operating across state boundaries. It is noted that the Australian Government is planning to undertake a feasibility study in relation to establishing a national reporting facility for cybercrime (Department of the Prime Minister and Cabinet, 2011). Smith (2008) states that, in relation to fraud, a national reporting centre allows for the development of an improved response in relation to prevention and intervention. This would allow for the collation of information domestically, which can then also be shared with the international community. Data collected by a national reporting centre can be used to raise awareness of victimisation, enable resources to be allocated to effectively and appropriately, evaluate intervention and prevention strategies, compile intelligence which can be used for policing and prevention activities, provide feedback to those who have detected and reported matters, enable information on new crime methodologies to be shared with others at risk of similar types of activities, and compile statistical data for trend identification, data mining and analysis (Smith, 2008).
While target hardening may not discourage offenders motivated by curiosity and skill testing, it is still an efficient crime prevention technique to stop attacks that use known vulnerabilities. Business surveys indicate that computer security is often not a high priority, particularly for small businesses that may not have the knowledge and skills to adequately secure their systems (Richards, 2009). Therefore, businesses should be informed about checks and balances they can implement to reduce criminal opportunities and ensure fraudulent activities are detected, and encouraged to take these up. Businesses should also be encouraged to ensure that their computer systems are secure and informed about how they can go about doing this.

It is also recommended that there be further education of potential victims, particularly the elderly who may be turning to technology for the first time, and those less technically adept. This could include an ongoing advertising campaign using a variety of media to ensure that individuals are aware of how their data are used, what their online activities may be placing them at risk of, and how they can protect themselves online.

**Future research**

Future research to test the proposed model could include comparing offenders with non-offenders to determine if the model explains why some people offend while others do not. Also, the model could be used to compare computer crime offenders with other crime types to determine if the theory is applicable only to crime that occurs in this environment. Future research may also apply the integrated theoretical model to other types of computer crimes, such as
cyberbullying, online child exploitation offences, including child pornography and 
cybergrooming, and software and music pirating. Separate research into hackers 
and fraudsters may also be undertaken to account for their distinctive patterns of 
offending.

As political ideology and hactivism was identified as a motivating factor in 
just one case included in this research, applying the theoretical model to these 
offenders, such as Anonymous, the spinoff group LulzSec, as well as nationalist 
hackers, would provide a greater understanding into this crime type. While this 
research indicated that hackers were less likely to target large and powerful 
organisations due to the perceived risks, nation states are frequently the target of 
hactivist organisations, and the immediate benefits to the offender may be less 
obvious.

There is also a need for further computer crime surveys. The last national 
survey of computer crime offending was published in 2009 by the Australian 
Institute of Criminology (Richards, 2009). This survey used data from the 2006- 
07 financial year. There is a need for further reliable data that is balanced and 
fair. Research design is very important to ensuring that figures reflect as closely 
as possible the extent of victimisation experienced by individuals and 
organisations. This research also needs to be applied to ensure that crime 
prevention initiatives are targeted and make the best use of available resources.

Crime prevention initiatives that have been recommended in this chapter 
should also be evaluated to determine their effectiveness and ensure that they 
deliver the best results for the amount of cost involved.
Appendix A ~ Australian State, Territory and Commonwealth

Unauthorised Access-Related Offences
<table>
<thead>
<tr>
<th>Prohibited conduct</th>
<th>New South Wales</th>
<th>Victoria</th>
<th>Queensland</th>
<th>Western Australia</th>
<th>South Australia</th>
<th>Tasmania</th>
<th>Northern Territory</th>
<th>Australian Capital Territory</th>
<th>Commonwealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical element</td>
<td>Unauthorised access or modification of restricted data held in a computer</td>
<td>Unauthorised access to or modification of restricted data held in a computer</td>
<td>Use of a restricted computer without the consent of the controller</td>
<td>Unauthorised use of a restricted access computer system</td>
<td>Unauthorised operation of a restricted access computer system</td>
<td>Unauthorised access to a computer, system of computers or any part of a system of computers</td>
<td>Unlawfully abstracting confidential information from a computer</td>
<td>Unauthorised access to or modification of restricted data held in a computer</td>
<td>Unauthorised access to or modification of restricted data held in a computer*</td>
</tr>
<tr>
<td>Fault element</td>
<td>Intent to cause access or modification and knowledge that this is unauthorised</td>
<td>Intent to cause access or modification and knowledge that this is unauthorised</td>
<td>Intent to cause access or modification and knowledge that this is unauthorised</td>
<td></td>
<td>Intention</td>
<td>Intent to cause loss, to gain benefit or to publish</td>
<td>Intent to cause access or modification and knowledge that this is unauthorised</td>
<td>Intent to cause access or modification and knowledge that this is unauthorised</td>
<td></td>
</tr>
<tr>
<td>Penalty</td>
<td>2 years</td>
<td>2 years</td>
<td>2 years</td>
<td>2 years</td>
<td>$2,500</td>
<td>$2,000 or 2 years</td>
<td>3 years</td>
<td>2 years and/or $2,000</td>
<td>2 years</td>
</tr>
<tr>
<td>Aggravated access</td>
<td>s408E(2) Criminal Code Act 1899</td>
<td>s440A(3)(b) Criminal Code</td>
<td>s44 Summary Offences Act 1953</td>
<td>s276B Criminal Code Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical element</td>
<td>Use of a restricted computer without the consent of the controller</td>
<td>Unauthorised use of a restricted access computer system</td>
<td>Unauthorised operation of a restricted access computer system</td>
<td></td>
<td>Unlawful access or use of data unlawfully accessed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prohibited conduct</td>
<td>New South Wales</td>
<td>Victoria</td>
<td>Queensland</td>
<td>Western Australia</td>
<td>South Australia</td>
<td>Tasmania</td>
<td>Northern Territory</td>
<td>Australian Capital Territory</td>
<td>Commonwealth</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
<td>----------</td>
<td>------------</td>
<td>------------------</td>
<td>----------------</td>
<td>---------</td>
<td>-------------------</td>
<td>-----------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Fault element</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Causes or intends to cause detriment or damage, or gains or intends to gain a benefit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penalty</td>
<td>5 years</td>
<td>5 years</td>
<td>$2,500 or 6 months</td>
<td>10 years</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* There must be a connection with a Commonwealth computer, a computer where data is held on behalf of the Commonwealth, or the access, modification or impairment must be via a telecommunications service.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source: Adapted from Bronitt &amp; Gani (2005).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix B ~ Australian State, Territory and Commonwealth

Data-Related Offences
<table>
<thead>
<tr>
<th>Prohibited conduct</th>
<th>New South Wales</th>
<th>Victoria</th>
<th>Queensland</th>
<th>Western Australia</th>
<th>South Australia</th>
<th>Tasmania</th>
<th>Northern Territory</th>
<th>Australian Capital Territory</th>
<th>Commonwealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical element</td>
<td>Unauthorised modification of data</td>
<td>Unauthorised modification of data</td>
<td>Unauthorised modification of computer data</td>
<td>Damaging data or obstructing its use</td>
<td>Unlawful modification of data</td>
<td>Unauthorised modification of data*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fault element</td>
<td>Knowledge that unauthorised and intent to impair data or access to it/recklessness as to impairment</td>
<td>Knowledge that unauthorised and intent to impair data or access to it/recklessness as to impairment</td>
<td>Knowledge that unauthorised and intent to impair data or access to it/recklessness as to impairment</td>
<td>Intention</td>
<td>Intent to impede access to or adversely affect reliability, security or operation of data</td>
<td>Knowledge that unauthorised and intent to impair data or access to it/recklessness as to impairment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penalty</td>
<td>10 years</td>
<td>10 years</td>
<td>10 years</td>
<td>$2,000 or 2 years</td>
<td>$2,000 or 2 years</td>
<td>10 years and/or $10,000</td>
<td>10 years</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Data modification**

<table>
<thead>
<tr>
<th>Physical element</th>
<th>Introducing into a computer system false information as data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault element</td>
<td>Dishonesty</td>
</tr>
<tr>
<td>Penalty</td>
<td>$2,000 or 2 years</td>
</tr>
<tr>
<td>Prohibited conduct</td>
<td>New South Wales</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Physical element</td>
<td>Unauthorised access, modification or impairment of electronic communication</td>
</tr>
<tr>
<td>Fault element</td>
<td>Knowledge that unauthorised and intent to commit or facilitate a serious indictable offence</td>
</tr>
<tr>
<td>Penalty</td>
<td>Maximum applicable to serious indictable offence</td>
</tr>
<tr>
<td>Prohibited conduct</td>
<td>New South Wales</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Physical element</td>
<td>Unauthorised impairment of electronic communication</td>
</tr>
<tr>
<td>Fault element</td>
<td>Knowledge that unauthorised and intent to impair/recklessness as to impairment</td>
</tr>
<tr>
<td>Penalty</td>
<td>10 years</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Possession or control of data</th>
<th>New South Wales</th>
<th>Victoria</th>
<th>Queensland</th>
<th>Western Australia</th>
<th>South Australia</th>
<th>Tasmania</th>
<th>Northern Territory</th>
<th>Australian Capital Territory</th>
<th>Commonwealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault element</td>
<td>Possession or control of data</td>
<td>Possession of data</td>
<td>Possession or control of data</td>
<td>Possession or control of data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possession or control of data</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td>Intent to commit or enable a serious computer offence</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penalty</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years and/or $3,000</td>
<td>3 years</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Possession or control of data**

<table>
<thead>
<tr>
<th>Possession or control of data</th>
<th>New South Wales</th>
<th>Victoria</th>
<th>Queensland</th>
<th>Western Australia</th>
<th>South Australia</th>
<th>Tasmania</th>
<th>Northern Territory</th>
<th>Australian Capital Territory</th>
<th>Commonwealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault element</td>
<td>Possession or control of data</td>
<td>Possession of data</td>
<td>Possession or control of data</td>
<td>Possession or control of data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possession or control of data</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td>Intent to commit or enable a serious computer offence</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penalty</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years and/or $3,000</td>
<td>3 years</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prohibited conduct</td>
<td>New South Wales</td>
<td>Victoria</td>
<td>Queensland</td>
<td>Western Australia</td>
<td>South Australia</td>
<td>Tasmania</td>
<td>Northern Territory</td>
<td>Australian Capital Territory</td>
<td>Commonwealth</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
<td>----------</td>
<td>------------</td>
<td>-------------------</td>
<td>----------------</td>
<td>---------</td>
<td>-------------------</td>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Producing, supplying or obtaining data</td>
<td>s308G Crimes Act 1900</td>
<td>s247F Crimes Act 1958</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
</tr>
<tr>
<td>Physical element</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
<td>Producing, supplying or obtaining data</td>
</tr>
<tr>
<td>Fault element</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td>Intent to commit or facilitate a serious computer offence</td>
<td>Intent to commit or facilitate a serious computer offence</td>
</tr>
<tr>
<td>Penalty</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years</td>
<td>3 years</td>
</tr>
</tbody>
</table>

* There must be a connection with a Commonwealth computer, a computer where data is held on behalf of the Commonwealth, or the access, modification or impairment must be via a telecommunications service.

Source: Adapted from Bronitt & Gani (2005).
Appendix C ~ Australian State, Territory and Commonwealth

Fraud-Related Offences
<table>
<thead>
<tr>
<th>Prohibited conduct</th>
<th>New South Wales</th>
<th>Victoria</th>
<th>Queensland</th>
<th>Western Australia</th>
<th>South Australia</th>
<th>Tasmania</th>
<th>Northern Territory</th>
<th>Australian Capital Territory</th>
<th>Commonwealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical element</td>
<td>Obtains property belonging to another or obtains any financial advantage or causes any financial disadvantage</td>
<td>Obtains property by deception</td>
<td>Gains a benefit or advantage for any person or causes a detriment to any person, pecuniary or otherwise</td>
<td>Gains a benefit for any person or causes a detriment to any person, pecuniary or otherwise</td>
<td>Dishonestly benefits him/herself or a third person or causes a detriment to another person</td>
<td>Using a computer (including by manipulating data or obstructing its use)</td>
<td>Obtains the property of another or a benefit by deception</td>
<td>Obtains property by deception</td>
<td>Obtains property belonging to a Commonwealth entity by deception</td>
</tr>
<tr>
<td>Fault element</td>
<td>Intention to permanently deprive</td>
<td>Intent to defraud by deceit or any fraudulent means</td>
<td>Intent to defraud</td>
<td>Intent to defraud</td>
<td>Intent to permanently deprive</td>
<td>Intent to permanently deprive</td>
<td>Intent to permanently deprive</td>
<td>Intent to permanently deprive</td>
<td>INTENT TO PERMANENTLY DEPRIVE</td>
</tr>
<tr>
<td>Penalty</td>
<td>10 years</td>
<td>10 years</td>
<td>5 years</td>
<td>7 years</td>
<td>15 years</td>
<td>$2,000 or 2 years</td>
<td>14 years</td>
<td>10 years and/or $10,000</td>
<td>10 years</td>
</tr>
<tr>
<td>Prohibited conduct</td>
<td>New South Wales</td>
<td>Victoria</td>
<td>Queensland</td>
<td>Western Australia</td>
<td>South Australia</td>
<td>Tasmania</td>
<td>Northern Territory</td>
<td>Australian Capital Territory</td>
<td>Commonwealth</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
<td>----------</td>
<td>------------</td>
<td>------------------</td>
<td>----------------</td>
<td>----------</td>
<td>-------------------</td>
<td>-------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Physical element</td>
<td>Obtains financial advantage by deception</td>
<td>Gains a benefit for any person or causes a detriment to any person, pecuniary or otherwise to the value of $30,000 or more</td>
<td>Dishonestly manipulates a machine to gain a benefit or cause a detriment to another</td>
<td>Obtains goods by false pretences</td>
<td>Obtains financial advantage by deception</td>
<td>Obtains a financial advantage from a Commonwealth entity by deception</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fault element</td>
<td>Intent to defraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penalty</td>
<td>10 years</td>
<td>12 years</td>
<td>10 years</td>
<td>$2,000 or 2 years</td>
<td>10 years and/or $10,000</td>
<td>10 years</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>s252A Criminal Code Act 1924</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical element</td>
<td>Acquiring a financial advantage by deception</td>
<td>Engages in organised fraud and derives a substantial benefit</td>
<td>Obtains a financial advantage from a Commonwealth entity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fault element</td>
<td>$2,000 or 2 years</td>
<td>15 years and/or $165,000</td>
<td>12 months</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penalty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prohibited conduct</td>
<td>New South Wales</td>
<td>Victoria</td>
<td>Queensland</td>
<td>Western Australia</td>
<td>South Australia</td>
<td>Tasmania</td>
<td>Northern Territory</td>
<td>Australian Capital Territory</td>
<td>Commonwealth</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
<td>----------</td>
<td>------------</td>
<td>-------------------</td>
<td>-----------------</td>
<td>----------</td>
<td>-------------------</td>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Physical element</td>
<td>Intent to defraud by false or misleading statement</td>
<td></td>
<td>Personation in general</td>
<td>Personation in general</td>
<td>Uses another’s personal identification</td>
<td>Personation in general</td>
<td>Personation in general</td>
<td>Does something to dishonestly obtain a gain from someone in the Territory</td>
<td>Does something to dishonestly obtain a gain from a Commonwealth entity</td>
</tr>
<tr>
<td>Fault element</td>
<td>Intent of obtaining property belonging to another or obtaining a financial advantage or causing a financial disadvantage</td>
<td>Intent to defraud any person</td>
<td>Intent to defraud any person</td>
<td>Intends to commit or facilitate the commission of a serious criminal offence</td>
<td>Intent to defraud</td>
<td>Intent to defraud any person</td>
<td>Intent</td>
<td>Intent</td>
<td></td>
</tr>
<tr>
<td>Penalty</td>
<td>5 years</td>
<td></td>
<td>3 years</td>
<td>3 years</td>
<td>Maximum applicable to serious offence</td>
<td>$2,000 or 2 years</td>
<td>3 years</td>
<td>5 years and/or $5,000</td>
<td>5 years</td>
</tr>
</tbody>
</table>
Appendix D ~ Australian State, Territory and Commonwealth

Identity-Related Offences
<table>
<thead>
<tr>
<th>Prohibited conduct</th>
<th>New South Wales</th>
<th>Victoria</th>
<th>Queensland</th>
<th>Western Australia</th>
<th>South Australia</th>
<th>Tasmania</th>
<th>Northern Territory</th>
<th>Australian Capital Territory</th>
<th>Commonwealth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dealing with identification information</td>
<td>$s192J$ Crimes Act 1900</td>
<td>$s408D$ Criminal Code Act 1899</td>
<td>Obtaining or dealing with identification information</td>
<td>Purpose of committing or facilitating the commission of an indictable offence</td>
<td>10 years</td>
<td>3 years</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical element</td>
<td>Dealing with identification information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fault element</td>
<td>Intent of committing or facilitating the commission of an indictable offence</td>
<td>Purpose of committing or facilitating the commission of an indictable offence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penalty</td>
<td>10 years</td>
<td>3 years</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possession of identification information</td>
<td>$s192K$ Crimes Act 1900</td>
<td>$s140$ Criminal Law Consolidation Act 1935</td>
<td>Possession of a false document knowing it to be false</td>
<td>Possession of a false document</td>
<td>7 years</td>
<td>15 years</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical element</td>
<td>Possession of identification information</td>
<td>Possession of a false document</td>
<td></td>
<td>Possession of a false Commonwealth document</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fault element</td>
<td>Intent of committing or facilitating the commission of an indictable offence</td>
<td>Intent to dishonestly induce another to accept it as genuine and obtain a gain or cause a loss</td>
<td></td>
<td>Intent to dishonestly induce another to accept it as genuine and obtain a benefit or cause a loss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possession of identification information</td>
<td>7 years</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penalty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prohibited conduct</td>
<td>New South Wales</td>
<td>Victoria</td>
<td>Queensland</td>
<td>Western Australia</td>
<td>South Australia</td>
<td>Tasmania</td>
<td>Northern Territory</td>
<td>Australian Capital Territory</td>
<td>Commonwealth</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------</td>
<td>----------</td>
<td>------------</td>
<td>------------------</td>
<td>----------------</td>
<td>----------</td>
<td>-------------------</td>
<td>-------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Forging a document or uttering a forged document</td>
<td>Forging a document or uttering a forged document</td>
<td>Creating or falsifying a document</td>
<td>Forging a document</td>
<td>Forging a document</td>
<td>Forging a document</td>
<td>Making a false Commonwealth document</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intent of inducing another person to accept it as genuine</td>
<td>Intent to defraud</td>
<td>Intent to defraud</td>
<td>Intent to deceive or exploit another to obtain a benefit or cause detriment</td>
<td>Intention to defraud</td>
<td>In order to obtain a benefit</td>
<td>Intent to dishonestly induce another to accept it as genuine and obtain a gain or cause a loss</td>
<td>Intent dishonestly induce a third person to accept it as genuine and obtain a gain or cause a loss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penalty</td>
<td>10 years</td>
<td>3 years</td>
<td>7 years</td>
<td>15 years</td>
<td>$2,000 or 2 years</td>
<td>7 years</td>
<td>10 years and/or $10,000</td>
<td>10 years</td>
<td></td>
</tr>
</tbody>
</table>
Appendix E ~ Study Two Interview Schedule
Background information

This research project relates to computer crimes that compromise data and financial security, specifically hacking and online fraud. The interview will begin by learning more about your experience investigating these types of crimes within the last five years.

Overall, could you tell me about your experience with investigating these types of offences?

How long have you investigated these types of offences?

How many investigations have you been involved in?

What did you do before investigating these types of offences?

Offenders’ backgrounds

I will now ask you to tell me about the average computer crime offender. I will also be interested in any differences between hackers and those that are involved in online fraud in relation to these questions. Also, whether there would be any differences for male and female offenders.

Any identifying information relating to offenders will be replaced with a pseudonym during when the interview is transcribed so that they cannot be identified in any publication.
What are the characteristics of the typical offender?

Generally, how old are offenders when they come to the attention of police?

What do you think offenders’ family situations are like?

Are they generally married or in a long term relationship?

Do they generally have any children?

In general, are offenders employed at the time they were offending?

What type of job?

Do employed offenders generally offend in the course of their employment?

Do unemployed offenders support their lifestyle through their online offending?

To your knowledge, are many offenders religious?

How much time and effort do offenders dedicate to their activities?

How much skill and expertise do offenders usually have?

Do you know of any females that have engaged in hacking or online fraud?

Why do you think so few females engage in hacking or online fraud?
I am interested in understanding offenders’ levels of participation in other crimes, including violent crimes, property crimes, and drug use. What other types of crimes other than hacking or fraud do these offenders generally become involved in?

Do offenders engage in these crimes at the same time they engage in hacking or fraud? Before? After?

How do you know whether they are engaged in other types of crimes?

How old do you think offenders are when they first start hacking or committing fraud, before they come to the attention of the police?

Do offenders generally hack or commit fraud with other people?

If so, how often do they do that?

Why do they work with others?

How large are the groups?

Do they work together from the same location?

How do you know?

Why do you think offenders come to the decision to start hacking or committing fraud?

Instrumental needs (e.g. money for subsistence, to commit another crime)?

Influence of others – specify?

Presented opportunities – specify – e.g. how did the opportunity come about?
How do you think offenders choose the target(s) that they do?

Low risk? High reward? Ease? Ecological, political or ethical reasons ("hactivism")? Revenge (e.g. former employer)?

What do offenders gain from hacking or fraud?

Fun?

Advanced career?

What is the financial gain of [hacking/online fraud]?

What do offenders think about the chances of getting caught?

How do you know this?

What do offenders initially think the penalties will be when they get caught?

Do they think the penalties are severe?

Are offenders concerned about other negative outcomes such as dismissal from university, loss of respect from close friends, lost respect of family, dismissal from work, or diminished job prospects?

Do offenders exhibit guilt or shame after being caught?

Do offenders generally re-offend after being caught?

How upset are offenders after being caught?
Do offenders ever indicate that there are people or organisations that they would not target?

Why? Morals? High risk? Low reward? High difficulty?

Do you think offenders like the label “hacker”?  

How do offenders learn how to hack and commit fraud?

Do they develop contacts to get information?

Do they provide information to others?

Do you think offenders are “addicted” to computers?

Do offenders offer “computer addiction” as an explanation for their offending?

Why do you think offenders stop hacking or committing online fraud?

What reasons do offenders provide for why they offended?

Do offenders ever state that those who do not secure their systems or information deserve to be taken advantage of?

How morally wrong do offenders generally think hacking or online fraud is?

How serious do offenders generally think hacking or online fraud is?

Do offenders often implicate other friends or acquaintances who hack or commit online fraud?
Do offenders have a lot of respect for the police?

What types of strain might offenders have been under before they commenced offending?

What is your opinion about hackers and those that commit online fraud?

What is the general attitude of offenders’ families towards hacking or online fraud?

How much schooling do offenders usually have?

Did they finish high school?

Did they go to university?

Did they finish university?

**Conclusion**

Is there anything further that you would like to add?

Thank you for your time and for being straightforward and honest. Everything that you have told me will be kept confidential.

Do you have any questions?
Appendix F ~ Study Three Interview Schedule
Introduction

Have you read the informed consent package?

Do you have any questions?

Do you consent to this interview?

To begin with, have you been involved with hacking, online fraud, or both?

Do you consider yourself to be an active or former [hacker/fraudster]?

This is an interview about the story of your life. As a social scientist, I am interested in hearing your story, including parts of the past as you remember them and the future as you imagine it. The story is selective; it does not include everything that has ever happened to you. Instead, I will ask you to focus on a few key things in your life – a few key scenes, characters, and ideas. There are no right or wrong answers to my questions. Instead, what I’m asking is that you simply tell me about some of the most important things that have happened in your life and how you imagine your life developing in the future. I will guide you through the interview so that we finish it all in about two hours or less.

Please know that my purpose in doing this interview is not to figure out whether there is something wrong with you or to do some kind of deep clinical analysis. Nor should you think of this interview as a “therapy session” of some kind. The interview is for research purposes only, and its main goal is simply to hear your story. Everything you say is voluntary, anonymous, and confidential.

Do you have any questions?

A. Life Chapters

Please begin by thinking about your life as if it were a book or novel. Imagine that the book has a table of contents containing the titles of the main chapters in the story. To begin here, please describe very briefly what the main chapters in the book might be. Please give each chapter a title, tell me just a little bit about
what each chapter is about, and say a word or two about how we get from one chapter to the next. You may have as many chapters as you want, but I would suggest having between about 2 and 7 of them. We will want to spend no more than about 20 minutes on this first section of the interview, so please keep your descriptions of the chapters relatively brief.

[Note to interviewer: The interviewer should feel free to ask questions of clarification and elaboration throughout the interview, but especially in this first part. This first section of the interview should run between 15 and 30 minutes.]

B. Key Scenes in the Life Story

Now that you have described the overall plot outline for your life, I would like you to focus in on a few key scenes that stand out in the story. Consider a key scene to be a moment in your life story that stands out for a particular reason – perhaps because it was especially good or bad, particularly vivid, important, or memorable.

1. High point. Please describe a scene, episode, or moment in your life that stands out as an especially positive experience. This might be the high point scene of your entire life, or else an especially happy, joyous, exciting, or wonderful moment in the story. Please describe this high point scene in detail. What happened, when and where, who was involved, and what were you thinking and feeling? Also, please say a word or two about why you think this particular moment was so good and what the scene may say about who you are as a person.

2. Low point. The second scene is the opposite of the first. Thinking back over your entire life, please identify a scene that stands out as a low point, if not the low point in your life story. Even though this event is unpleasant, I would appreciate your providing as much detail as you can about it. What happened in the event, where and when, who was involved, and what were you thinking and feeling? Also, please say a word or two about why you think this particular moment was so bad and what the scene may say about you or your life.
3. **Turning point.** In looking back over your life, it may be possible to identify certain key moments that stand out as turning points -- episodes that marked an important change in you or your life story. Please identify a particular episode in your life story that you now see as a turning point in your life. If you cannot identify a key turning point that stands out clearly, please describe some event in your life wherein you went through an important change of some kind. Again, for this event please describe what happened, where and when, who was involved, and what you were thinking and feeling. Also, please say a word or two about what you think this event says about you as a person or about your life.

4. **Positive childhood memory.** The fourth scene is an early memory – from childhood or your teen-aged years – that stands out as especially positive in some way. This would be a very positive, happy memory from your early years. Please describe this good memory in detail. What happened, where and when, who was involved, and what were you thinking and feeling? Also, what does this memory say about you or about your life?

5. **Negative childhood memory.** The fifth scene is an early memory – from childhood or your teen-aged years – that stands out as especially negative in some way. This would be a very negative, unhappy memory from your early years, perhaps entailing sadness, fear, or some other very negative emotional experience. Please describe this bad memory in detail. What happened, where and when, who was involved, and what were you thinking and feeling? Also, what does this memory say about you or your life?

6. **Vivid adult memory.** Moving ahead to your adult years, please identify one scene that you have not already described in this section (in other words, do not repeat your high point, low point, or turning point scene) that stands out as especially vivid or meaningful. This would be an especially memorable, vivid, or important scene, positive or negative, from your adult years. Please describe this
scene in detail, tell what happened, when and where, who was involved, and what you were thinking and feeling. Also, what does this memory say about you or your life?

C. Future Script

Now, we’re going to talk about the future.

1. The next chapter. Your life story includes key chapters and scenes from your past, as you have described them, and it also includes how you see or imagine your future. Please describe what you see to be the next chapter in your life. What is going to come next in your life story?

2. Dreams, hopes, and plans for the future. Please describe your plans, dreams, or hopes for the future. What do you hope to accomplish in the future in your life story?

3. Life project. Do you have a project in life? A life project is something that you have been working on and plan to work on in the future chapters of your life story. The project might involve your family or your work life, or it might be a hobby, avocation, or pastime. Please describe any project that you are currently working on or plan to work on in the future. Tell me what the project is, how you got involved in the project or will get involved in the project, how the project might develop, and why you think this project is important for you and/or for other people.

D. Challenges

This next section considers the various challenges, struggles, and problems you have encountered in your life. I will begin with a general challenge, and then I will focus in on some particular areas or issues where many people experience challenges, problems, or crises.

1. Life challenge. Looking back over your entire life, please identify and describe what you now consider to be the greatest single challenge you have faced in your life. What is or was the challenge or problem, how did it develop
and how did you address or deal with it? What is the significance of this challenge or problem in your own life story?

2. Health. Looking back over your entire life, please identify and describe a scene or period in your life, including the present time, wherein you or a close family member confronted a major health problem, challenge, or crisis. Please describe in detail what the health problem is or was and how it developed. In addition, please talk about how you coped with the problem and what impact this health crisis, problem, or challenge has had on you and your overall life story.

3. Failure, regret. Everybody experiences failure and regrets in life, even for the happiest and luckiest lives. Looking back over your entire life, please identify and describe the greatest failure or regret you have experienced. The failure or regret can occur in any area of your life – work, family, friendships, or any other area. Please describe the failure or regret and the way in which the failure or regret came to be. How have you coped with this failure or regret? What effect has this failure or regret had on you and your life story?

E. Personal Ideology

Now, I would like to ask a few questions about your fundamental beliefs and values and about questions of meaning and morality in your life. Please give some thought to each of these questions.

1. Religious/ethical values. Consider for a moment the religious or spiritual aspects of your life. Please describe in a nutshell your religious beliefs and values, if indeed these are important to you. Whether you are religious or not, please describe your overall ethical or moral approach to life.

2. Political/social values. How do you approach political or social issues? Do you have a particular political point of view? Are there particular social issues or causes about which you feel strongly? Please explain.
3. **Change, development of religious and political views.** Please tell the story of how your religious, moral, and/or political views and values have developed over time. Have they changed in any important ways? Please explain.

**F. Life Theme**

Looking back over your entire life story with all its chapters, scenes, and challenges, and extending back into the past and ahead into the future, do you discern a central theme, message, or idea that runs throughout the story? What is the major theme in your life story? Please explain.

**Discussion topics to cover if not brought up:**

- Relationship with parents.
- Marital status.
- Dependants.
- Employment status.
- Living arrangements.
- What an average day was like when involved in hacking/fraud.
- Involvement in clubs and other activities.
- Relationships with others involved in hacking/fraud, including:
  - How they interacted;
  - Whether they hacked/committed fraud together;
  - Why worked with others;
  - Size of the group; and
  - How many considered to be close friends.
• Whether family/friends were aware of hacking/fraud, and what they think/would think about it.

• Time per day spent hacking/committing fraud.

• Involvement in other illegal behaviour such as violent crime, property crime and drug use.

• Experiences with the police and the criminal justice system.

• Age when started hacking/committing fraud.

• How came to the decision to start hacking/fraud.

• Whether thought of not doing it.

• How targets were chosen.

• What was gained.

• Perceptions of getting caught and penalties.

• How much of a problem the penalties would be, including other negative outcomes.

• Whether would reoffend if sanctioned.

• How felt before, during and after offending.

• Whether felt guilt.

• Whether there were people or organisations that would not be targeted.

• The best and worst parts of hacking and/or fraud.

• Self perceptions.

• How others see you.
Theory and Crime: Does it Compute?

Appendix F ~ Study Three Interview Schedule

- Whether skills have improved and how.

- The extent that hacking/fraud interferes with participation in other activities.

- Computer addiction – whether experienced and whether should be a legal defence.

- When is it ok to hack/commit fraud and when is it not.

- **Former:** Why stopped.

- **Former:** At what age stopped.

- Opinions of those who do not secure their systems or information.

- How morally wrong/serious hacking/fraud is.

- Whether hacking/fraud should be against the law – including if no data or computer systems were damaged.

- Whether downloading information is copying or stealing.

- Whether would turn in a friend or acquaintance.

- Friends’ involvement in hacking/fraud and other types of crime.

- Whether know of any females that have engaged in hacking/fraud.

- Why think so few females engage in hacking/fraud.

- How serious police officers consider hacking/fraud to be.

- Whether have respect for police.

- How learnt to hack/commit fraud.

- Opinion of school.
• Education level.

• Whether got into trouble at school.

• What barriers might stop them from achieving goals.

**Conclusion**

Is there anything further that you would like to add?

Thank you for your time and for being straightforward and honest. Everything that you have told me will be kept confidential.

I would really appreciate it if you could pass on my details to anyone else who may be interested in participating (particularly any females).

Do you have any questions?
Differential Association

Definitions favourable to criminal behaviour:

- Believe that it is ok to get around the law if can get away with it.
- Believe that it is ok to do some things that are not right in order to get ahead.
- Believe that those who do not secure their systems or information deserve to be taken advantage of.
- Do not believe that it is morally wrong to hack or commit computer fraud.
- Do not thinking hacking or computer fraud is serious.
- Do not believe that it is always wrong to damage, destroy or take another’s property.
- Like to take chances.
- Attitude of family members towards hacking and computer fraud.
- Attitude of friends towards hacking and computer fraud.

Associations with others who have definitions favourable to criminal behaviour:

- Number of close friends who have engaged in hacking or computer fraud.
- People known to them who have been in trouble for hacking or computer fraud.
- Whether friends approve or disapprove if they knew of involvement in hacking or computer fraud.
- The extent that those closest would support the decision made.
Social Control Theory

Attachment to others:

- What family situation was like growing up.
- Whether have a good relationship with parents.
- Whether married or in a long term relationship.
- Whether dating.
- Whether have any children.
- Who live with.
- Whether would like to be the kind of person their mother or father are.
- Whether believe spending time with family is important.
- Popularity in high school.
- Popularity of friends in high school.
- Affection or attachment felt towards school.

Commitment to society:

- How important getting good grades is.
- Whether tried hard in school.
- How much education would like to get.
- Whether like or dislike school.

Involvement in conventional activities:

- Whether employed.
• Whether religious.

• Whether attend church.

• How much time spent on homework per day.

Moral beliefs:

• Whether have a lot of respect for the police.

• Whether it is ok to get around the law if can get away with it.

• Whether believe that those who do not secure their systems or information deserve to be taken advantage of.

Techniques of neutralisation

Denial of responsibility:

• Addiction to computers.

• Whether computer addiction should be a legal defence.

• Whether feel guilty about hacking or computer fraud if were drunk or stoned and couldn't control.

Denial of injury:

• Whether hacking should be against the law of no data or computer systems were damaged.

• Whether would feel guilt if the victim was insured.

• Whether downloading information without permission is copying or stealing.

• Whether would feel guilt if the victim can afford it.
Denial of the victim:

- People or organisations that would not be targeted.
- Feel guilty about hacking or computer fraud if the victim makes a lot of money off other people.
- Believe that those who do not secure their systems or information deserve to be taken advantage of.
- Whether physical distance between the victim helps avoid feelings of guilt.

Condemn the condemners:

- Neutralise behaviours by comparing to that of other governments, police, etc.

Appeal to higher loyalties:

- Hacked/committed computer fraud for a gang or to gain money for family, etc.

**Rational Choice Theory**

**Benefits:**

- Targets selected (e.g. perceived benefit).
- Benefit gained.

**Costs:**

- Guilt felt
- Worse part of hacking or computer fraud.
- Types of targets avoided.
Likelihood of detection:

- Chances of getting caught.
- Likelihood that activities would be reported to the police.
- Who is seen as the greatest risk, e.g. police, regulators, victims, family or friends.

Severity of punishment:

- Penalties if caught.
- Perceptions of severity.
- How upset family and friends would be if arrested.
- How upset would be if arrested.
- If would reoffend if punished.

**Labelling Theory**

Labelling by the criminal justice system:

- Whether have been stopped, charged or arrested by police.
- Whether have ever been convicted of a crime.
- Whether have ever served time for a crime.
- Whether have ever received another punishment, such as community service or probation, for a crime.

Other formal labelling:

- Whether have been expelled or suspended from school.
- Whether have ever been thrown out of a classroom.
Informal labels:

- Whether have been labelled as a hacker or fraudster.
- Whether have been a member of a gang.
- Number of friends that have engaged in a violent attack.
- Number of friends that have used illegal drugs.

Self-concept:

- Whether consider self to be a hacker or fraudster.

**Structural Strain Theory**

Goals:

- How much education would like to get.
- Whether would like to make a lot of money.
- What kind of job would like to have.

Means:

- How much education ended up getting.
- Whether it is necessary to lie to parents in order to keep trust.
- How much education expect to get.
- Whether it is necessary to play dirty in order to win.

Strain:

- Whether the chance of making a lot of money in lifetime is good.
- Whether satisfied with the amount of money available to live on.
- Chances of getting ideal job.

- Whether believe that if you have the right connections would be more successful.

- Whether believe that someone or something stops them trying to achieve something.

- Whether believe have been frustrated in efforts to get ahead in life.

**Feminist Critiques**

The generalisability problem:

- Why think so few females engage in hacking or computer fraud.

The gender ratio problem:

- Whether know any other females that have engaged in hacking or computer fraud.
References


269


