The final publication is available in K. Jaishankar & N. Ronel (eds), Global Criminology: Crime and Victimization in the Globalized Era (pp. 93-114). Boca Raton: CRC Press.

Hacking and Fraud:
A Qualitative Analysis of Online Offending and Victimisation

Alice Hutchings

Introduction and Aim

This research relates to computer crimes that compromise data and financial security, namely hacking and online fraud, focussing on offenders' perceptions of victims. Very little is known about those who commit computer crimes. This is despite the increase in offending rates that have corresponded with the wider availability of computers to the general public from the 1980s and the introduction of the World Wide Web in 1991 (Moschovitis, Poole, Schuyler, & Senft, 1999). These technological advances have increased the reach of offenders as well as the vulnerability of potential victims. Cybercrime offenders constitute a hidden and hard-to-access population. This qualitative analysis draws from interviews with self-identified offenders, law enforcement officers who investigate these offences, and court documents.

The aim of this study is to examine factors relating to online victimisation. Rational choice theory and techniques of neutralisation have been identified as suitable theoretical frameworks to achieve this aim. Therefore, areas that are explored in this analysis include: offenders' motivations; 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. This work contributes to the literature relating to online victimisation, providing insight through the lens of offenders, law enforcement officers and the judiciary.

Nature of hacking and 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. Misuse of legitimate access to a computer system, or insider abuse of access, occurs when the hacker abuses the trust they have been given, such as an employee or contractor accessing or altering an employer's data (Shaw, Ruby, & Post, 1998). Computer frauds refer to the use of information and communication technology to manipulate others into providing money or identity information.

Some of the activities pursued by computer enthusiasts have been labelled as criminal. One example is "hacking", an umbrella term that, these days, encompasses a variety of pursuits that compromise computer security, but overall refers to gaining unauthorised access to a computer system with or without a further criminal motive (Brenner, 2007; Wall, 2007). Once access has been gained hackers may obtain confidential information, such as credit card details, or "deface" websites. Hackers may employ social engineering techniques as well as technical methods to gain access to computer systems.

There have been a number of studies that have examined the hacker subculture. For example, Meyer (1989) found that hackers had an extensive social network, which was used for expertise and skill advancement. Holt (2007) examined how hackers learnt how through these online social networks, as well as through trial and error, the use of forums, and offline connections. 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 1 below summarises some of these drawn from the relevant literature.

Table 1

Motivations Reported in the Literature

Motivation	Key cited literature
Curiosity and self-education	Barber (2001), Chantler and Broadhurst (2006), Jordan and Taylor (1998), Standing Committee on Communications (2010), Taylor (1999)
Ecological, political and ethical activism ("hactivism")	Australian Institute of Criminology (2005), Barber (2001), Chantler and Broadhurst (2006), Furnell (2002), Standing Committee on Communications (2010), Taylor (1999)
Financial gain, such as through extortion, espionage or fraud	Australian Institute of Criminology (2005), Barber (2001), Chantler (1995), Chantler and Broadhurst (2006), Coleman (2006), Furnell (2002), Shaw et al. (1998), Standing Committee on Communications (2010)
Feelings of power	Australian Institute of Criminology (2005), Jordan and Taylor (1998), Taylor (1999)
Damage other countries or political parties, such as through information warfare	Barber (2001), Berson and Denning (2011), Standing Committee on Communications (2010)
Demonstrate, test and challenge skills	Australian Institute of Criminology (2005), Chantler (1995), Furnell (2002), Goode and Cruise (2006)
Obtain social status	Australian Institute of Criminology (2005), Chantler (1995), Jordan and Taylor (1998), Standing Committee on Communications (2010), Taylor (1999)
External pressure, such as from terrorism organisations or organised crime groups	Chantler and Broadhurst (2006)
Anonymise future attacks	Australian Institute of Criminology (2005)
Settle personal grievances	Australian Institute of Criminology (2005), Chantler and Broadhurst (2006), Coleman (2006), Furnell (2002), Shaw et al. (1998)
Use system resources for personal use	Australian Institute of Criminology (2005), Taylor (1999)
Fund terrorist activities or attack critical infrastructure for terrorism	Australian Institute of Criminology (2005), Furnell (2002), Smith et al. (2010)
"White hat" hacking, such as testing computer and network security	Australian Institute of Criminology (2005), Barber (2001), Jordan and Taylor (1998)
Addictive compulsion	Chantler (1995), Furnell (2002), Jordan and Taylor (1998), Taylor (1999)
Be free from, or escape from, the real world	Chantler (1995), Taylor (1999)
Fun, excitement, enjoyment or pleasure	Chantler (1995), Furnell (2002), Jordan and Taylor (1998), McQuade (2006)

Computer fraud, for the purpose of this research, involves a large number of frauds that are conducted in the online environment. Online fraud may be conducted to manipulate others into providing money or identity details. This

may use a variety of mediums, including email, social networking sites, such as chat or dating websites, and online trading sites (Brenner, 2007; Finch, 2007). There are many types of online computer frauds, including identity fraud, card-not-present fraud, internet auction fraud, investment fraud, advance fee fraud and phishing.

There is a relationship between the two offence types considered in this study as hacking may facilitate 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, Holt, & Ahn, 2010; Franklin, Paxson, Perrig, & Savage, 2007; Holt & Lampke, 2010; Motoyama, McCoy, Levchenko, Savage, & Voelker, 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.

Multiple victims may be involved in scams, such as an individual whose identity or account details has been stolen, and the financial institution, government agency or service provider that has been duped. The cost of online fraud extends beyond the direct financial loss to include loss of consumer confidence, lost time and the emotional impact on victims.

Theoretical Perspectives

Two criminological theories provide the main framework for this analysis. 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). Rational choice theory looks at how offenders in particular situations make these calculations (Vold, Bernard, & Snipes, 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. For example, 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).

According to the second theory, Sykes and Matza’s (1957) techniques of neutralisation, 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). 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) claimed 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. These techniques are: to deny responsibility; to deny injury; to deny the victim; to condemn the condemners; and to appeal to higher loyalties (Sykes & Matza, 1957).

McQuade (2006, p. 141) states that “there has been extremely little empirical testing of established theories to explain in explicit terms why cybercrimes occur”. Some exceptions are Skinner and Fream (1997), who applied applying social learning theory to music piracy and unauthorised computer access by a student population, Rogers (2001), who applied social learning theory and moral disengagement to hackers, and Patchin and Hinduja (2011) who applied general strain theory to cyberbullying. Digital piracy has also been examined using low self control and social learning theory as frameworks (Higgins, 2004), as well as techniques of neutralisation (Higgins, Wolfe, & Marcum, 2008).

Turgeman-Goldschmidt (2009) interviewed Israeli hackers, identifying while doing so their use of techniques of neutralisation. Walkley (2005) discussed

how techniques of neutralisation may explain computer crimes but did not conduct an empirical test of this theory. 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.

Research Questions

Rational choice theory and techniques of neutralisation provide frameworks for thinking about how offenders may go about victim selection, particularly who might be targeted or avoided. For example, 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 metered 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. Techniques of neutralisation may also inform target selection, as the characteristics of some potential victims may be more conducive to neutralisation than others. Therefore, with these theories in mind, the areas explored in this study include:

1. What are offenders' motivations?
2. What people or organisations do offenders target?
3. What people or organisations do offenders avoid?
4. Do offenders rationalise their actions based on victim characteristics?
5. Does physical distance from the victim help alleviate feelings of guilt?

6. Do offenders believe that those who do not secure their systems or information deserve to be taken advantage of?

Method

A qualitative research design was selected for its ability to provide a deep understanding of offending behaviour. This study involved three stages. The first stage was a qualitative analysis of court documents, in particular sentencing remarks and court judgments relating to prosecutions and extraditions involving computer fraud and unauthorised access in Australia, the United Kingdom, the United States of America and New Zealand. A systematic review of legal databases was conducted to identify relevant cases. Only documents available on public databases were identified and retrieved. Although this resulted in a selected sample, it provides an illustration to explore the issues pertinent to this research. Of the 54 cases included in this stage, 12 were female offenders, while the remaining 42 were male. The mean age of the sample, where known (*n*=35), was 32.7 years, ranging from 18 to 50 years. 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.

Stage two consisted of interviews with law enforcement officers within computer crime or fraud specialist units from four policing agencies in Australia, namely the Australian Federal Police, the Queensland Police Service, Western Australia Police and Victoria Police. These interviews focussed on officers' experiences with, and perceptions of, offenders who have been identified by the criminal justice system. The interviews were one-on-one, open-ended and semi structured. The interviews were broadly structured as follows:

- The background of the interviewee, such as how long they had been with the policing agency, and their overall experience with these offence types;

- Offender characteristics, including age, gender, family status, and employment status;
- Offenders' skill, expertise and time dedicated to offending;
- Involvement in other offence types;
- Involvement with other offenders;
- Initiation into, and desistance from, offending;
- Target selection;
- Motivations; and
- Offenders' reactions to law enforcement.

The 15 law enforcement officers interviewed in stage two included 14 males and one female. The interviews ranged from 32 minutes to one hour and 16 minutes in length, with a mean time of 51 minutes.

Stage three consisted of interviewing active and former offenders face-to-face. Participants were recruited within Australia 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 such 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 it 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, meant that they were in control of the amount of personal information that they provided. The interviews were one-on-one, open-ended and semi-structured based on a modified version of McAdams' (2008) *Life Story Interview*. Additional questions enquired about the following topics:

- Relationships with family members, friends, significant others and other offenders;
- Employment and living arrangements;
- Time involved in offending;
- Involvement in other illegal behaviour;
- Experiences with the police and the criminal justice system;
- Age when started offending;
- How came to the decision to start offending;
- How targets were chosen and what was gained;
- Perceptions of getting caught and penalties;
- How felt before, during and after offending;
- People or organisations that would not be targeted;
- The best and worst parts of offending;
- Self perceptions;
- How skills were obtained and improved;
- The extent that offending interferes with participation in other activities;
- When is it ok to offend and when is it not;
- Why stopped offending and at what age (for former offenders);
- 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;
- Friends' involvement in hacking/fraud and other types of crime;
- How serious police officers consider hacking/fraud to be and respect for police; and
- Opinion of school and education level.

Of the seven offenders who participated in stage three, five identified as hackers and two as both hackers and online fraudsters. Five were active offenders and two identified themselves as former offenders. All participants were male, aged between 18 and 49, with a mean age of 29.7 years at the time they were interviewed. The interviews ranged from 45 minutes to two hours and 18 minutes in length, with a mean time of one hour and 39 minutes.

All interviews were transcribed verbatim. Data from the three stages were analysed together to identify the themes that related to victimisation and target selection. Coding of the data was mainly "concept-driven" (Gibbs, 2007, p. 44), in that the codes used primarily arose from the literature relating to the theories being examined. However, "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.

Results

Question 1: What are offenders' motivations?

Many motivations for offenders were identified in the data. 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 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).

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).

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).

> *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 was 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). 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).

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* (Law Enforcement Officer #8).

Parker (1998) claimed that some hackers have extreme political views, including anarchist, Nazi or extreme right wing associations. However, while law enforcement officers advised that there were hackers targeting site for political reasons, they also 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 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. Many offenders obtained 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:

> *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).

Question 2: What people or organisations do offenders target?

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).

Question 3: What people or organisations do offenders avoid?

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).

Question 4: Do offenders rationalise their actions based on victim characteristics?

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 following instance:

> *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…" (Case #28, male hacker, aged 40).

However, one 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).

Question 5: Does physical distance from the victim help alleviate feelings of guilt?

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).

Question 6: Do offenders believe that those who do not secure their systems or information deserve to be taken advantage of?

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).

Discussion

While fraudsters are mainly motivated by financial gain, hackers enjoy 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 sample included in this research may reflect more mainstream offenders, representing the majority rather than a minority of offenders with the appropriate skill, expertise and relevant motives for such attacks.

One component of rational choice theory is that when offenders weigh up the type and amount of benefit likely against the perceived risk of detection and punishment, they take into consideration the skills and equipment needed to successfully commit the offence (Cornish & Clarke, 1987). This analysis identified that types of people or organisations that were deemed to be suitable targets included systems familiar to or accessible by the offender and those that had known vulnerabilities. This indicates that cyber crime offenders are targeting systems that are easily accessible and well known to them. Many offenders also took steps to conceal their activities by removing or changing evidence that they had accessed particular systems. There was some indication that offenders are calculating the risks of detection and punishment when selecting victims. For example, other targets included those who did not have systems in place to detect fraudulent activities, further reducing the likelihood of detection.

The data 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 also 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.

Reliability, validity and reflexivity

This section will address some of the pertinent issues relating to reliability, validity and reflexivity. In relation to reliability, it is possible that the data obtained is 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 to not 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 agrees 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 targets 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.

Another problem with reliability may be "definitional drift" (Gibbs, 2007, p. 98), where the meanings of codes may change over time. Notes were made about all the possible meanings of each code to enable a more reliable and stable coding system.

The validity of the research design was 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 utilised (Neuman, 2006, pp. 150-151).

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 (Gibbs, 2007). 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, Grabosky and Urbas (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 online fraudsters who are not apprehended or prosecuted. Interviewing active and former offenders mitigated this limitation.

However, 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. Nonetheless, 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. Again, this limitation was minimised by including offenders who have been identified by the criminal justice system and those who have not.

Conclusion

Offender techniques are constantly evolving, as are the technologies that present the opportunities to offend. Therefore, it is argued that a strategic approach to crime prevention should be implemented. This can include technical countermeasures, such as firewalls, anti-virus and other target hardening techniques. However, in many instances the vulnerabilities exist at the user level, with offenders using social engineering tactics to gain access to systems. Therefore, educating potential victims about computer security is also essential. However, there is a large pool of susceptible targets and

offenders are constantly changing their methods. Therefore it is important to know more about these types of offences so that alternative deterrence strategies can be developed.

Acknowledgements

I would like to thank those that participated in this study and the assistance provided by the Australian Federal Police, the Queensland Police Service, Western Australia Police and Victoria Police. I also appreciate the support of my supervisors, Dr Hennessey Hayes, Associate Professor Janet Ransley, Professor Simon Bronitt and Professor Peter Grabosky.

References

Akers, R. L., & Sellers, C. S. (2004). *Criminological Theories: Introduction, Evaluation and Application* (4th ed.). Los Angeles: Roxbury Publishing Company.

Australian Institute of Criminology. (2005). Hacking motives. *High Tech Crime Brief, 6*, 1-2.

Barber, R. (2001). Hackers profiled - Who are they and what are their motivations? *Computer Fraud & Security, 2*(1), 14-17.

Berson, T. A., & Denning, D. E. (2011). Cyberwarfare. *Security & Privacy, IEEE, 9*(5), 13-15.

Braithwaite, J. (1993). Review: Crime and the Average American. *Law & Society Review, 27*(1), 215-231.

Brenner, S. W. (2007). Cybercrime: Re-thinking crime control strategies. In Y. Jewkes (Ed.), *Crime Online*. Devon: Willan Publishing.

Chantler, A., & Broadhurst, R. (2006). *Social Engineering and Crime Prevention in Cyberspace - Technical Report*. Brisbane: Queensland University of Technology.

Chantler, A. N. (1995). *Risk: The Profile of the Computer Hacker.* Doctor of Philosophy, Curtin University.

Chu, B., Holt, T. J., & Ahn, G. J. (2010). *Examining the Creation, Distribution and Function of Malware On-Line*: Technical Report for National Institute of Justice. NIJ Grant No. 2007−IJ−CX−0018.

Clarke, R. V. (1997). Introduction. In R. V. Clarke (Ed.), *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Monsey: Criminal Justice Press.

Coleman, J. W. (2006). *The Criminal Elite: Understanding White-Collar Crime* (6th ed.). New York: Worth Publishers.

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology, 25*(4), 933-947.

Finch, E. (2007). The problem of stolen identity and the Internet. In Y. Jewkes (Ed.), *Crime Online*. Devon: Willan Publishing.

Franklin, J., Paxson, V., Perrig, A., & Savage, S. (2007). *An inquiry into the nature and causes of the wealth of internet miscreants*. Paper presented at the ACM Conference on Computer and Communications Security (CCS), 375– 388.

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. London: Pearson Education Limited.

Gibbs, G. (2007). *Analyzing Qualitative Data*. London: SAGE Publications Ltd.

Goode, S., & Cruise, S. (2006). What motivates software crackers? *Journal of Business Ethics, 65*, 173-201.

Higgins, G. E. (2004). Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior, 26*(1), 1-24.

Higgins, G. E., Wolfe, S. E., & Marcum, C. D. (2008). Music piracy and neutralization: A preliminary trajectory analysis from short-term

longitudinal data. *International Journal of Cyber Criminology, 2*(2), 324-336.

Holt, T. J. (2007). Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behavior, 28*(2), 171-198.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies, 23*(1), 33-50.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757-780.

Matza, D. (1990). *Delinquency & Drift*. New Brunswick: Transaction Publishers.

McAdams, D. P. (2008). The Life Story Interview. Retrieved November 12, 2009, from http://www.sesp.northwestern.edu/docs/LifeStoryInterview.pdf

McQuade, S. C. (2006). *Understanding and Managing Cybercrime*. Boston: Pearson Education, Inc.

Meyer, G. R. (1989). *The Social Organization of the Computer Underground.* Master of Arts, Northern Illinois University.

Moschovitis, C. J. P., Poole, H., Schuyler, T., & Senft, T. M. (1999). *History of the Internet: A Chronology, 1843 to the Present*. Santa Barbara: ABC-CLIO, Inc.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). *An analysis of underground forums*. Paper presented at the 2011 ACM SIGCOMM conference on Internet measurement, Berlin, Germany.

Neuman, W. L. (2006). *Social Science Research Methods: Qualitative and Quantitative Approaches* (6th ed.). Boston: Pearson Education, Inc.

Parker, D. B. (1998). *Fighting Computer Crime*. New York: John Wiley & Sons, Inc.

Patchin, J. W., & Hinduja, S. (2011). Traditional and Nontraditional Bullying Among Youth: A Test of General Strain Theory. *Youth & Society, 43*(2), 727-751.

Pontell, H. (2002). 'Pleased to meet you... Won't you guess my name?': Identity fraud, cyber-crime, and white-collar delinquency. *Adelaide Law Review, 23*, 305-328.

Rogers, M. K. (2001). *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behaviour: An Exploratory Study.* Doctor of Philosophy, University of Manitoba.

Shaw, E., Ruby, K. G., & Post, J. M. (1998). The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin, 98*(2), 1-10.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency, 34*(4), 495-518.

Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber Criminals On Trial*. Cambridge: Cambridge University Press.

Smith, R. G., McCusker, R., & Walters, J. (2010). *Trends & Issues in Crime and Criminal Justice No. 394: Financing of terrorism: Risks for Australia*. Canberra: Australian Institute of Criminology.

Standing Committee on Communications. (2010). *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*. Canberra: The Parliament of the Commonwealth of Australia.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664-670.

Taylor, P. A. (1999). *Hackers*. London: Routledge.

Turgeman-Goldschmidt, O. (2009). The rhetoric of hackers' neutralisations. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet*. New Jersey: Pearson Education, Inc.

Vold, G. B., Bernard, T. J., & Snipes, J. B. (2002). *Theoretical Criminology* (5th ed.). New York: Oxford University Press, Inc.

Walkley, S. (2005). *Regulating Cyberspace: An Approach to Studying Criminal Behaviour on the Internet.* Doctor of Philosophy, The Australian National University.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Wright, R., & Bennett, T. (1990). Exploring the offender's perspective: Observing and interviewing criminals. In K. L. Kempf (Ed.), *Measurement Issues in Criminology* (pp. 138-151). New York: Springer-Verlag New York Inc.

Wright, R. T., Decker, S. H., Redfern, A. K., & Smith, D. L. (1992). A snowball's chance in hell: Doing field research with residential burglars. *Journal of Research in Crime and Delinquency, 29*(2), 148-157.