SUBMISSION NO. 9

UNCLASSIFIED

AUSTRALIAN CRIME COMMISSION

Submission to the Joint Select Committee on Cyber-Safety

Inquiry into Cybersafety for Senior Australians

ACC
AUSTRALIAN CRIME COMMISSION

Page intentionally blank

Table of contents

Page intentionally blank

Introduction

Australians are targeted by serious and organised criminal networks that exploit the cyber environment to further their criminal activities. The anonymity and international reach of the internet enables criminal networks to target their criminal activities to vulnerable populations.

Older Australians[1], including senior Australians may be particularly vulnerable to, and exploited by such criminal networks, where they have:

- a low level of skill and/or experience using new technologies
- a high level of trust in companies or entities that are presented professionally, but which are in-fact not legitimate
- access to retirement savings and superannuation funds, and
- limited awareness of cyber-safety information that is relevant to their needs.

This paper provides an unclassified overview of the nature of serious and organised criminal exploitation of the cyber environment and the threat and harm that is caused as a result.

[1] See the "Victim Profile" for Serious and Organised Investment Fraud at page 17 of this submission.

Background

Australia's first computer, built in 1949, filled a room the size of a double garage and required enough electricity to power a suburban street.[2] By 2009, there was a computer in nearly four out of five Australian households.[3] Now there are more than 10 million Internet subscribers in Australia and more than nine million Australians connect to the Internet through their mobile phones.[4]

Learning, shopping, working, accessing services, relaxing, socialising—the cyber-world is embedded into daily life in ways that were unimaginable in 1949. The Internet and converging technologies provide increasingly convenient, fast, personalised, interactive services and information.

However, these same technologies also provide unprecedented opportunities for serious and organised crime. The cyber environment allows even a single criminal entity access to millions of potential victims.

Organised criminal networks take advantage of new technologies to expand their reach, commit crimes from a distance, create the appearance of legitimacy and exploit the lack of clear jurisdictional authority.

In this way, cybercrime enables and amplifies serious and organised criminal enterprise. This in turn increases the threat and harm caused to the Australian community, particularly to senior Australians who might be more specifically targeted.

A range of studies have identified that whilst internet usage by senior Australians is lower than that of the mainstream population, there is a growing trend in their usage of new technologies.

[2] CSIRAC: Australia's first computer, CSIRO, accessed 5 November 2011, <http://www.csiro.au/science/CSIRAC.html>

[3] Household Use of Information Technology, 2008–09 (cat. no. 8146.0) Australian Bureau of Statistics, accessed 5 November 2011, <http://abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8146.0Main+Features12008-09>

[4] Internet Activity Australia, June 2011, Australian Bureau of Statistics, accessed 5 November 2011, <http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/>

The Australian Government's commitment to the National Broadband Network will provide a range of opportunities and accessibility not necessarily available to senior Australians previously, especially in respect of improving access to electronic health services in their homes / remote communities and better communication opportunities with family and community.

It is a complex issue that requires a complex and multifaceted national response.

What is cybercrime?

While many definitions have been proposed for cybercrime, none is widely accepted. For the purpose of this submission the Australian Crime Commission (ACC) will refer to the Australian New Zealand Policing Advisory Agency (ANZPAA) definition that includes:

- crime directed at computing and communications technologies themselves, such as unauthorised access to, modification or impairment of electronic communications or data, and
- crime where the use of the internet or information technology is integral to the commission of the offence, (sometimes referred to as technology enabled crime) such as online fraud (including Internet or e-mail scams), online identity theft, online child exploitation and online intellectual property infringement.

Extent of cybercrime

Cybercrime is increasing at an unprecedented rate. The *Norton Cybercrime Report 2011* estimates the global cost of cybercrime topped $388 billion in the past year. This is more than the combined global market for marijuana, cocaine and heroin, and fast approaching the value of all global drugs trafficking. In Australia, 72 per cent of adults who used the Internet have experienced cybercrime in their lifetime, most commonly viruses/malware, online credit card fraud and social network profile hacking.[5]

[5] Norton *Cybercrime report 2011*, accessed 5 November 2011 <http://www.symantec.com/content/en/au/home_homeoffice/html/cybercrimereport/>

Determining the extent of cybercrime accurately is complicated due to underreporting. Some victims never detect the cybercrime of which they have been a victim. Other victims may recognise that they have been the victim of a crime, but overlook or not recognise the link to the cyber environment. In other cases, individuals and businesses may not report cybercrimes due to embarrassment or concern over damage to their reputation.

The Australian Institute of Criminology (AIC) has identified that people over the age of 55 account for four out of 10 victims of cyberfraud scams.[6] The AIC report also identified that older people were more vulnerable to cyberfraud scams, despite their age group being statistically less likely to use the internet.

ACC's role

The ACC is Australia's national criminal intelligence agency with unique investigative capabilities. The ACC supports and complements Australian law enforcement efforts to reduce the threat and impact of serious and organised crime of most harm to the community. This is achieved by working in partnership with other agencies to collect, analyse, fuse and share criminal intelligence about the threats posed by serious and organised crime. The ACC contributes to investigations which identify and disrupt serious and organised criminal activity, and aims to raise awareness and provide advice to help harden the environment against such activity.

Gaining a detailed national and global understanding of serious and organised crime is critical to determining how Australia responds. The ACC contributes to this understanding through its national criminal intelligence data holdings, coercive powers, strategic intelligence products, national legislative and organisational framework that allows information sharing, and specialist skills in sophisticated intelligence gathering and analysis.

[6] Ross, S & Smith, RG (Australian Institute of Criminology (AIC)), *Risk Factors for advance fee fraud victimization*, Trends & issues in crime and criminal justice, No 420, August 2011.

The ACC Board comprises the heads of all state and territory law enforcement agencies, and the heads of:

- the Australian Federal Police
- the Attorney-General's Department
- the Australian Customs and Border Protection Service
- the Australian Securities and Investments Commission
- the Australian Security Intelligence Organisation, and
- the Australian Taxation Office.

The multi-jurisdictional Board sets National Criminal Intelligence Priorities and authorises the use of the ACC's coercive powers under two types of Determinations–Special Operations and Special Investigations.

Serious and organised criminals are increasingly using the cyber environment to facilitate their illegal activities; therefore, the ACC is encountering cybercrime across all of its work priorities. Countering computer-based and technology enabled crime has become a key priority for the Australian, state and territory governments in terms of national security and law enforcement.

Cyber criminals

Organised criminal networks are entrepreneurial and innovative. They are strategic and continually scan for vulnerabilities and opportunities which they exploit for criminal gain and profit. They are attracted to the cyber environment because it is globally connected, borderless, anonymous, fast, low-risk, easily accessible and has vast amounts of rich data including financial, personal, public and private information.

Organised criminal networks take advantage of new technologies, such as the Internet and emerging forms of communication, to commit traditional criminal activities in new ways and at new levels.

Australian-based organised criminal networks are now commonly using information and communications technologies to commit conventional crimes, such as fraud, based on deception, extortion and social engineering.

Organised criminal networks leverage technologies to:

- extend their reach and capacity
- commit crimes from a distance, and
- create the appearance of legitimacy.

These factors converge and contribute to the complexity of detecting and disrupting cybercrime. Criminal networks capitalise on these technologies in targeting Australian victims in serious and organised investment fraud schemes.

Technology extending the reach of criminal activities

Australia's high take-up rate of new technologies creates an ever increasing pool of potential cybercrime victims. Information and communications technology is now linked to almost every facet of our lives. Features of the cyber-world that were cutting edge just years ago are now the norm. Internet banking, social networking, paying bills, online shopping—more and more Australians are online every day for a wide variety of reasons. The number of Internet subscribers in Australia (excluding through mobile phones) increased 4.4 per cent in the six months from December 2010 to June 2011, reaching 10.9 million. This was outstripped by growth in mobile handset subscribers, which increased 18.1 per cent over the same period to reach 9.7 million. In the three months to June 2011, mobile subscribers alone downloaded 3,695 terabytes: enough data to fill 65 million four-door filing cabinets.[7]

In support of the Government's *National Broadband Network,* a commitment of $15 million in the 2008–09 Federal Budget was provided to deliver the *Broadband for Seniors* initiative. This initiative is:

- providing older Australians with access to computers and the internet via free internet kiosks
- supporting seniors to gain confidence and build skills in using new technology

[7] Internet Activity Australia, June 2011, Australian Bureau of Statistics, accessed 24 October 2011, <http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/> note, filing cabinet analogy is from e-crime symposium speech

- addressing the issue of older Australians feeling isolated and ‘left behind’ in the technological age, and
- building community participation and social inclusion amongst older Australians.

People are increasingly becoming more comfortable with sharing their personal information, both on and off-line. This personal information can be very quickly analysed, augmented, used, sold and rented—both legitimately and illegally. The availability of this data, which is often stored and protected by third parties in a different locality, partnered with the communities’ increased comfort in conducting transactions remotely, presents new opportunities for organised criminal networks to extend their reach, through identity theft and targeted fraud.

Programs that encourage senior Australians to use new technologies and participate in the cyber-world not only support the digital economy and address social inclusion, they also increase the risk that senior Australians will be exposed to cyber crime. This is supported by the AIC study which found older people were more vulnerable, despite their age group being statistically less likely to use the internet[8].

[8] AIC 2011, *op cit*

CASE STUDY: Online Romance and Advance Fee Frauds (Also known as Nigerian 419 Frauds)

Online Romance and Advanced Fee scams initially originated from Nigeria (419 being the Nigerian criminal code Fraud offence), but they now can originate anywhere in the world. They target people en masse by letter or e-mail offering the receiver of the email a percentage of a large sum of money, or a large cash prize, subject to the victim sending a "fee" to facilitate the transaction.

Online Romance scams are similar and involve email correspondence from an overseas male or female seeking a partner, which usually ends in the victim being asked to send money to facilitate travel to Australia, or other expenses such as an emergency operation.

The victims of both types of scams are often "groomed" via email over a long period of time by the offenders, to instill a trusting relationship before asking for money. Victims are then solicited for more and more funds over a period of time, to "facilitate" the romance or financial transaction.

Senior Australians are particularly vulnerable to these scams because of their trusting nature, and because of this many victims refuse to believe they are the victim of a scam. Many victims also believe the only way to recover monies already paid to the scammer, is to continue to send funds until the transaction is "successfully" completed.

While the criminals target people en masse, they rely on only a small number of individuals to become victims to profit from this activity. The use of e-mail means that they are able to target millions of people at a time for minimal investment.

CASE STUDY: Trade of personal information

The leads market specialises in on-selling personal data that has, or can be, refined to identify individuals that fall within a target group likely to be able, or to want to, purchase specific products. Often the personal data is obtained legitimately with the full consent of the individuals concerned from sources such as surveys or competitions.

While the leads market is a legitimate industry in its own right, it is also a harvesting ground for organised criminal networks. Using the same methodology as the legitimate market, organised criminal networks purchase information to identify potential victims. In some cases one network may purchase, refine and on-sell the information to another network. In others, they use the information to directly target the victims.

Armed with information such as income, superannuation, mortgage and investment details of individuals, organised criminal networks are able to identify those most susceptible to particular schemes, such as investment fraud.

Just as legitimate businesses use this information to increase sales rates, organised criminal networks are able to increase their illegal profits.

CASE STUDY: Identity crime

Capitalising on the contemporary need for individuals to have multiple forms of electronic personal identity information (PII), such as personal identification numbers (PINs) and computer system passwords, some serious and organised criminal networks specialise in the theft of identity data, and in particular financial data, for the purpose of on-selling to other criminal networks-identity data as an illicit commodity.

Cyber crime brokers are routinely posting advertisements on various online discussion forums promoting their services. Sellers accept payments primarily through money transfer companies and virtual currencies. Their services, at a minimum, include the sale of stolen identities and credit card information.

Prices vary for different countries, with Australia often being the third or fourth least expensive country after the US, UK and sometimes Canada. Average prices for a single Australian credit card range between A$7 and A$35, depending on the amount of credit available on the card. Prices for bank logins vary according to the bank balance. It costs on average A$100 for a login with a balance of A$1,000; A$200 for a login with a balance of A$3,000 and so on.

Credit card magnetic strip coding information and PINs are also available, with prices ranging between A$70 and A$170, depending on the location. Hacked payment clearing company account data is also available for sale. Prices vary depending on the balance. A verified payment clearing company account with a balance of A$1,000 costs on average A$100; a balance of A$5,000 costs A$300, and so on.

Operating at a distance

The cyber environment allows criminals to collaborate and form loose affiliations with like-minded individuals almost anywhere else in the world. They can share ideas and make illicit plans while living thousands of kilometres apart and often never meeting in person. This helps make organised criminal networks more efficient, fast and flexible. It also reduces the risk of exposure and enables criminal syndicates to recruit members in multiple locations around the globe. Law enforcement agencies are constrained by jurisdictional authority and the need to safeguard data and protect privacy.

The global nature of cyberspace supports transnational crimes. Hackers in one continent can steal financial or personal data from people living oceans away. Organisers of fraudulent investment schemes can target victims on the other side of the world. Those selling illegal commodities no longer need physical proximity to buyers as they can ship products to just about any location in response to online orders.

Most organised criminal networks active in Australia operate transnationally, and close to one in five have principals based offshore. A large proportion of e-security attacks that impact on Australia come from Eastern Europe, with Asia and West Africa also becoming emerging regions.[9]

Some cyberspace marketplaces, referred to as black-market web portals (BMWPs), have emerged as major platforms for organised criminal activity worldwide. Similar marketplaces have developed online where illicit commodities may be purchased, as well as capabilities and tools such as malicious software. As this economy has grown in sophistication, mature technical service providers such as payment card verification number generators and illicit data brokers have emerged.

In essence, the very benefits to the community from the cyber environment, such as anonymity, reach to foreign markets and ability to deal directly with the wholesaler, are also a significant benefit to organised criminal networks.

[9] Phair, N 2007, *Cybercrime: The Reality of the Threat*, p. 7, Canberra Australia, E-security publishing http://www.esecurity.net.au/cybercrime.html

CASE STUDY: - Gone Phishing: Fraudulent online banking scams

The ability of criminal networks to manipulate the anonymity and legitimacy of internet websites dates back many years.

In 2003, law enforcement first identified a methodology now known as "Phishing", where online banking customers were redirected to a fake bank website via email, in order to capture their netbanking login and password details. Funds were then withdrawn from the accounts using these details, by the scammers.

This form of online fraud has now reached sophisticated levels. These fake webpages are constructed by IT professionals employed by criminal groups and are located offshore in jurisdictions which are problematic to law enforcement investigations. Phishing and fake websites now target a broad range of online businesses, from paypal to online auction sites.

Senior Australians would be particularly vulnerable to this form of scam, due to the ability of offenders to duplicate the websites of institutions trusted by users, such as banks.

Appearing legitimate

In the past, criminal networks wanting to appear legitimate would need to purchase shop fronts and other investments that were time consuming and expensive to establish and alter, resulting in only a limited number of potential victims. Criminal networks today are becoming more sophisticated–they are using technology and professional expertise, thereby reducing costs and increasing profit and the number of victims.

Criminal networks are moving away from traditional methods of infecting victims computers through spam emails. Instead, they are using what appear to be safe websites and environments that in fact contain embedding malware.

Some criminal networks involved in investment fraud use a complex series of false websites, providing potential victims with a sense that an investment opportunity is legitimate. By drawing upon professional expertise, the websites are not able to be identified as false by viewing alone.

The criminal networks monitor and manipulate the results of search engines by entering data. This enables the negative results and feedback to be moved chronologically down the list of results with these entries often located on the second or third page, which are not viewed by those researching the scam investment. Using Voice over the Internet Protocol (VoIP), they are able to disguise where they are located, with potential victims believing that they are in the country as purported in the fake website. To further perpetuate the deception, the organised criminal networks use Western tourists with English speaking backgrounds in call centres to make contact with victims.

The sophisticated operations circumvent the prevention messaging and on-line feedback that has previously alerted potential victims that they are being scammed. Increasingly victims are educated, computer literate and have undertaken preventative research that provides them with a sense of assurance.

The relatively minimal investment of establishing a credible-looking website allows networks to reinvent themselves or their scams quickly following detection.

Serious and organised investment fraud

A significant and escalating threat, particularly targeting senior Australians, is false offshore investment schemes, also known as 'boiler-room' fraud or 'serious and organised investment fraud' (SOIF). These schemes use sophisticated techniques to solicit investment in non-existent or essentially worthless shares and other securities.

The ACC has developed a preliminary profile of people who are most 'at-risk' of becoming victims of this activity. This profile currently indicates that those over 50 years of age may be at an increased risk.

Victim Profile

Initial analysis has established that victims typically comprise the following characteristics:

- over 50 years of age
- are most likely to be male
- have received a university education or a high school diploma, and
- have a high or medium level of financial knowledge.

Victims were also identified as falling into two categories; *trusting* investors and *entrepreneurial* investors. The *trusting* investors are typically those who have a non-suspicious nature and are generally *empathic*. Fraud operators are able to easily construct relationships with this group, with victims rapidly perceiving operators to be honest and trustworthy. Victims identified as *entrepreneurial investors* are typically self-employed businessmen, who have limited financial knowledge. The *entrepreneurial investors* are categorised as people more willing to take risks on the assumption that high financial dividends will result.

Crime Description

These operations are predominantly based off-shore and are complex. The criminal networks are attracted to the high level of superannuation and retirement savings in Australia and target their scams accordingly, often using information stored online to identify potential victims.

Criminal networks target individuals using leads market personal information. While such scams often start with cold calls or e-mails and high pressure sales tactics, organised criminal networks have been known to spend considerable time grooming their potential victims to persuade them to part with their money. They will then use all of the methodologies described above to provide the appearance of legitimacy and to avoid detection.

If detected, they move to secondary operations, seeking further money to recover the original investment. Often, victims are unaware until advised by law enforcement that they have been scammed. They believe that their money has been invested in a long term scheme that is yet to mature.

Based on initial indications, more than 2,400 Australians have lost in excess of $93 million to these schemes; however, it is believed there is a high level of underreporting and the extent is far greater.

CASE STUDY:

Steve* is a 59 year-old male, living alone. He is University educated, but works as a skilled tradesman. Steve has saved and invested in blue chip shares on the Australian stock market, and has a portfolio valued at approximately $115,000.

Steve was unexpectedly ‘cold-called’ by fraud operators whom he described as "pushy and arrogant". Steve did not ask many questions about the investment, and eventually began to send money ‘on demand’, despite failing to receive receipts for monies already sent. As Steve did not have a close network of peers or friends, he was unable to discuss the investment opportunities being presented, or his financial activities with anyone. Prior to being cold-called, Steve had never invested overseas before, but had always wanted to do so.

Steve was not aware that he had been the victim of a fraud until he was contacted by his state police force. Despite police advice, Steve still remained unconvinced that he was the victim of a fraudulent investment. In total, Steve lost $82,000 of his projected superannuation and is currently unemployed. Steve described the experience as “financially devastating”.

** Name has been changed to protect individual identities.*

CASE STUDY:

David* is 67 years old and works as a self employed builder. He previously worked in the government and with law enforcement. He grew up in the country and completed his education at high school.

Due to unforeseen circumstances, David and his wife have had to take on the full-time care of their adolescent granddaughter.

In June 2011, David received a cold call from a male with an English accent, who told him about a great investment opportunity and subsequently sent him an email referring him to an excellent website. The caller was very chatty and advised that he had lived in Sydney and on the Gold Coast. David had no idea how he came by his name, but said he received similar calls "all the time".

This investment was for indexed trading, trading shares on six overseas share markets. He was told the company was an off-shoot of a British Company. David checked on the ASIC website and saw that the company had a company number but it had been rescinded. He then queried the caller, who said they didn't need a licence as a financial advisor (which they said they were) if you had less than 20 people in the company. David put in $42,000 and then, as that had gone well, put in another $13,000. These extra funds would put David into an 'executive' account, with fewer fees paid to the company.

David realised the company was fraudulent when the website went down and he was no longer able to get through to their phone number. He then *googled* the company and it came up as a fraud, with the details of 56 others who had been victimised in the same way.

The money sent to the criminal syndicate was his wife's superannuation. She had retired but has now had to return to work to help support their granddaughter.

** Name has been changed to protect individual identities.*

Threat and harm

As outlined in the examples provided, cybercrime has the potential to directly and indirectly affect every individual, business or organisation that owns, uses, engages with or stores data on a connected platform.

The wide-ranging impact of cybercrime includes:

- damage to processes and mechanisms ranging from an individual's banking to national infrastructure
- financial losses from online theft, delays in payments, loss of government revenue/data
- loss of online business where consumers lose confidence in digital infrastructure
- tarnished reputations and the credibility of individuals, communities, industries and countries
- lost finances, sometimes life savings, time and effort, plus the emotional damage such as depression, anxiety and broader relationship impacts experienced by victims and their families
- physical and/or mental distress through spam emails, damaged hardware and software and computer networks
- potential for critical infrastructure to be compromised affecting water supply, health services, national communications, energy distribution, financial services and transport
- costs to government agencies and businesses who must help re-establish credit histories, accounts and identities
- costs to businesses to improve e-security measures
- increased investment in time and resources by law enforcement, and
- increased resources to fund other crimes.

Conclusion

As well as creating opportunities for organised criminal networks, technical developments and the convergence of technologies are also creating new technical measures to combat cybercrime such as smart cards, biometrics, two-factor identification and exclusion listing.[10]

The way in which organised criminals are using technology to target and perpetrate their activities may be new and less obvious to senior Australians, no matter their past life experiences and education levels. This, combined with the perception of access to life savings and superannuation, makes them vulnerable to exploitation.

New methodologies have been developed in the ACC and elsewhere to identify criminal targets by mining data sources and near real-time risk assessment of less visible high risk criminal entities and activities. Such methodologies will complement conventional offence-based investigations.

However, there is more to be done. The prolific and increasing incidence of transnational cybercrime has had severe consequences for Australia nationally. The instantaneous, seamless, transnational and networked nature of cyber offences is difficult to police and law enforcement agencies need to move rapidly to adopt innovative approaches to prevention, disruption and deterrence.

In the same way that public health is a complex issue that requires a complex and holistic approach, so too does cybercrime.

Just as vaccination is important in the public health sector, prevention is a critical component of the cybercrime remedial strategy. However, it will not be an effective tool if used in isolation. The sophisticated methodologies that organised criminal networks are using are varied and not easily detected. This is despite victims being educated and technologically savvy.

[10] Australian Parliament, *Emerging technical measures to combat cyber crime*, in Cyber crime report, viewed 12 October 2010http://www.aph.gov.au/house/committee/coms/cybercrime/report/chapter11.pdf.

By the time a cyber-enabled crime comes to the attention of law enforcement, someone has already been affected, in the same way that people visiting their General Practitioner (GP) or hospital already have a health issue they need resolved.

To ensure cybercrime is able to be managed holistically, structures and standards are needed, including early warning systems, preventative measures and response mechanisms.

The overarching solution for attacking cybercrime needs a framework that is similar to that of the public health care system, as it is a complex issue requiring a coordinated multi-dimensional approach.

UNCLASSIFIED

ACC

AUSTRALIAN CRIME COMMISSION