SUBMISSION NO. 12

Australian Government
Australian Institute of Criminology

Telephone +61 2 6260 9200
Facsimile +61 2 6260 9278
GPO Box 2944
Canberra ACT 2601 Australia
www.aic.gov.au

16 February 2012

Senator Catryna Bilyk
Joint Select Committee on Cyber-Safety
PO Box 6021
Parliament House
CANBERRA ACT 2600
jscc@aph.gov.au

Dear Senator Bilyk

Submission to the Joint Select Committee on Cyber-Safety

The Australian Institute of Criminology (AIC) is pleased to make the attached submission in response to the Joint Select Committee on Cyber-Safety's inquiry into cyber-safety for senior Australians.

Please contact Dr Russell Smith, Principal Criminologist and Manager, Global, Economic and Electronic Crime Program on (03) 9467 6110 or by email Russell.Smith@aic.gov.au if you have any questions.

Yours sincerely

Dr Adam Tomison
Director (Chief Executive)

Australian Government

Australian Institute of Criminology

Telephone +61 2 6260 9200
Facsimile +61 2 6260 9278
GPO Box 2944
Canberra ACT 2601 Australia

www.aic.gov.au

Submission to the Joint Select Committee on Cyber-Safety

Dr Adam Tomison, Director (Chief Executive) of the Australian Institute of Criminology

Dr Russell G Smith, Principal Criminologist and Program Manager

Ms Alice Hutchings, Senior Research Analyst

Background

In November 2011, the Joint Select Committee on Cyber-Safety chaired by Senator Catryna Bilyk launched a new inquiry into cyber-safety for senior Australians. The Australian Institute of Criminology (AIC), Australia's national research and knowledge centre on crime and justice, welcomes the opportunity to contribute to the current inquiry.

The AIC seeks to promote justice and reduce crime by undertaking and communicating evidence-based research to inform policy and practice. The AIC was established in 1973 under the *Criminology Research Act* 1971 (Cth) and since 1 July 2011 has been regulated under the *Financial Management and Accountability Act* 1997 (Cth). The functions of the AIC include conducting criminological research, communicating the results of research, conducting or arranging conferences and seminars and publishing material arising out of the AIC's work. The AIC conducts research on a wide range of crime-related subjects and has undertaken a number of specific research projects on cybercrime during the last 15 years. The material in this document is provided by the AIC in response to the Joint Select Committee on Cyber-Safety's inquiry.

Submission details

Introduction

This submission provides information that is applicable to the inquiry's terms of reference, particularly drawing from relevant research conducted by the AIC.

1. The nature, prevalence and level of cyber-safety risks and threats experienced by senior Australians

There has been much focus on the nature of cyber-safety risks that specifically target young people, such as the distribution of child exploitation material, cyber-grooming and cyber-bullying. However, senior Australians, along with the rest of the population, also face a number of online risks and threats. Although the nature of the offences is the same for older

Australians as the general population, the extent and consequences of victimisation may be different for this age group.

The types of cyber-safety and cyber-security issues that senior Australians may experience or be exposed to include:

- frauds and scams;
- malicious code infection, which may, among other things, capture keystrokes, including account details;
- personal information held on third party databases being accessed without authorisation; and
- cyber-stalking.

Personal information disclosed online, such as one's whereabouts shared on social networking sites, may also allow offenders to identify targets for other offline crimes, including burglary. Seniors may not only be victimised from people unknown to them, but are also at risk of financial abuse from family or other household members with whom they may share computers or online account information (Johnson 2003).

As cybercrimes are currently reported to a diverse range of agencies, if at all, it can be difficult to determine the extent of cybercrime in general, and victimisation of older Australians specifically. In some instances it may be difficult to know when victimisation has occurred, for example, determining if charity solicitations are fraudulent can be problematic. There is some available research in relation to the prevalence of scams and identity fraud that includes analysis in relation to age and rate of online victimisation, however the results are mixed. For example, the Australian Bureau of Statistics (ABS) conducted a *Personal Fraud* survey in 2007 surveying approximately 14,000 people. The results indicated that those aged 55 and over were less likely than other age groups to fall victim to identity fraud (1.8% compared with 3.1% for the general population) or scams (1.6% compared with 2.0% for the general population) in the preceding 12 months (ABS 2008a).

Ross and Smith (2011) surveyed a much smaller sample of Victorian residents who had sent money to Nigeria in the 12 months prior to 31 March 2008. Of the 202 survey responses, 120 (59%) were identified as victims of advance fee fraud, whether that be dating scams, online transactions scams (including job offer and charity scams) or 'other', which included lottery scams and miscellaneous frauds. When the survey responses were analysed in relation to age it was found that respondents aged 65 years or older were more likely to be a victim of scams that were categorised as 'other' types of advance fee frauds than younger respondents.

These studies demonstrate how the age/victimisation relationship is not straightforward, at least in relation to frauds and scams. The ABS (2008a) data indicate that older Australians are less likely to fall victim to personal frauds, while Ross and Smith's (2011) study found that seniors are more likely to fall victim to some types of advance fee frauds, but not others.

This ambiguity may be explained by factors that place seniors at a higher, as well as lower, level of risk than younger Australians. As seniors may be less comfortable with online technologies, perhaps due to the perceived cyber-safety threat, subsequent avoidance from the internet may act as a protective barrier against victimisation. On the other hand, older Australians may:

- have more spare time or feel lonely, thereby turning to social networking or online dating websites, which exposes them to cyber-safety risks;
- seek out investment opportunities, some of which may be fraudulent;
- have lower levels of computer literacy or online experience as the younger generation and thus might be an easier target for criminals; and/or
- be deliberately targeted by scammers.

The Australian population is ageing, with 13 per cent aged 65 years and over in 2007, while the percentage of the population aged over 65 is projected to be between 23 and 25 per cent in the year 2056 and between 25 and 28 per cent in the year 2101 (ABS 2008b). The percentage of Australians aged over 60 years with internet access at home has also substantially increased in recent years, from 29 per cent in 2003 to 54 per cent in 2009 (ABS 2011). As the proportion of senior Australians who have access to the internet rises, there is likely to be an increase in the incidence of offending against this age group in the future.

2. The impact and implications of those risks and threats on access and use of information and communication technologies by senior Australians

Whether or not seniors are more at risk of falling victim to cybercrimes, they may nevertheless be more afraid of victimisation than younger Australians. This may mean that they are less likely to take up new technologies, which may otherwise have offered a number of advantages, such as staying in touch with family and friends, or utilising online services provided by businesses and governments.

If victimisation were to occur, the impact on seniors could be substantial. For example, they may lose all or part of their retirement savings, and having a limited ability to recover financially could impose an additional burden on welfare agencies. In addition to financial implications, victimisation can lead to emotional problems such as loss of trust, fear and anxiety. In Ross and Smith's (2011) study, of the 59% 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 experiencing marital or relationship problems as a result of victimisation. Financial hardship was also reported by 54 per cent of victims (Ross & Smith 2011).

3. The adequacy and effectiveness of current government and industry initiatives to respond to those threats, including education initiatives aimed at senior Australians

Cohen and Felson (1979:589) identified three precursors to the commission of most crimes. These are the presence of a motivated offender, the presence of a suitable target, and the absence of a capable guardian. Although motivations for acting illegally may well have remained fairly constant over time, technological developments have created many new opportunities for offenders. At the same time, the computer security industry has also increased its capacity as 'electronic capable guardians' (Smith & Grabosky 2011).

The traditional response to crime prevention has been to devise a range of situational measures that seek to make the commission of crime less attractive to potential offenders. Such measures aim to increase the levels of effort and skill required to commit offences, to create a greater risk of apprehension of offenders, and to decrease the potential rewards that offenders seek to derive from their illegal activities. Smith, Wolanin and Worthington (2003) have summarised the various crime prevention measures designed to reduce cybercrime employing the categorisation of traditional crime prevention measures developed by Clarke (1995; see also Newman and Clarke 2003). Law enforcement agencies, regulators, legislators, the information technology industry (including carriers, ISPs, and hardware and software manufacturers), businesses, educational bodies, public interest groups including the media, and, most importantly, computer users themselves all play a role in regulating cyberspace.

The criminal justice system is not always effective in controlling crime, and crime prevention requires the contribution of a wide range of stakeholders. Difficulties that law enforcement regularly faces include jurisdictional and evidentiary issues, as well as problems of extradition and the cost and logistics of investigation and prosecution. Offenders have a range of tools and techniques available to them to maintain anonymity and most computer crimes are never reported to the police. Even if suspects are located, further difficulties arise concerning the issue of warrants, security of data trails, disaggregating relevant from irrelevant data, and presenting evidence in court.

Cybercrime often crosses multiple jurisdictions, particularly when there is an organised crime element whereby offenders may reside in different countries and target victims in multiple nations. Timely access to evidence located in one or more foreign jurisdictions may be difficult or impossible, as it would normally require the assistance of authorities that for various reasons may be unwilling or unable to assist. When the suspect is located abroad, these difficulties are compounded. There is a need for effective international coordination in relation to cross-jurisdictional law enforcement and judicial cooperation in the fight against cybercrime.

In relation to cybercrime a variety of crime prevention techniques are actively used by government agencies worldwide to respond to the problem, other than through the use of prosecution and punishment. These strategies may be categorised as creating awareness among potential victims, monitoring and regulation of internet users and control or restriction of internet content. For example, in relation to fraud and scams, proactive steps have aimed at encouraging potential victims to ensure that their computers and personal information are safe, such as the annual campaign run by the ACFT. There are many more prevention programs and initiatives aimed towards young people than there are for the general population, or seniors specifically. While this reflects the extended range of risks young people may be exposed to online, such as cyber-grooming or cyber-bullying, there is scope for seniors to be targeted with crime prevention messages, education and training.

The escalating complexities of technology underline the need for continuing prevention activities. Constant and ongoing training programs are essential in educating the ageing population about the transnational nature of technology-enabled crime. There is, therefore, a need for coordinated action by government agencies to ensure the most effective crime prevention advice is provided to the community. User education through dissemination of media releases by authoritative institutions, such as SCAMwatch, would enable users to maintain current knowledge of the latest scams and the best fraud prevention measures available (Choo, Smith & McCusker 2007).

The AIC recognises the need for research to:

- ensure that prevention activities are suitably targeted to specific age groups, in that they are relevant to the types of technologies they may be using and cyber-safety issues they are likely to be exposed to; and
- rigorously evaluate prevention activities in order to develop best practice, to ensure that resources are used appropriately and to determine if the activities are meeting their intended goals.

4. Best practice safeguards, and any possible changes to Australian law, policy or practice that will strengthen the cyber-safety of senior Australians

Providing victim support, such as networks that provide counselling and raise awareness of measures to reduce future risk, is one area that could receive further attention in relation to cyber-safety issues, particularly for elderly victims. Not only do victims suffer significant impacts due to victimisation, but they may continue to be contacted by scammers if they fall victim to a fraud, and the effects of having their account details compromised or identity stolen can continue for some time.

It is recognised that many instances of cybercrime go unreported. Despite a recommendation by the Australian Law Reform Commission (2008), there is no requirement for mandatory breach reporting for businesses operating in Australia. The reasons for not reporting may vary for different types of victims, such as corporations compared to individuals. The Australian Business Assessment of Computer User Security (ABACUS) survey undertaken by the AIC revealed that in the 2006/07 financial year 77 per cent of respondent businesses 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). Implementing mandatory data breach reporting will allow Australians, including seniors, to take further steps to identify and prevent subsequent victimisation, such as changing passwords on online accounts, checking for abnormal transactions and monitoring their credit records, if their personal information has been accessed without authorisation.

One of the challenges currently facing criminal justice policy makers is a lack of knowledge about the extent of crime that is occurring online. This can be attributed to a low reporting rate, the multitude of state and federal government agencies within Australia that collect this type of data, how the data are recorded, the absence of requirements for mandatory data breach reporting and a lack of resources to enable victimisation surveys to be undertaken. 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) argued, in relation to fraud, that a national reporting centre would allow for the development of an improved response in relation to prevention and intervention. It would also allow for the collation of information domestically, which could then be shared with the international community. Data collected by a national reporting centre could be used to:

- raise awareness of victimisation;
- enable resources to be allocated more 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).

In addition, the AIC believes that funding should be made available for a national cyber security monitoring program. It is suggested that the national monitoring program should incorporate a number of data sources, such as:

- Annual surveys to identify the extent and impact of cyber security incidents on individuals, as well as businesses, organisations of national interest and all tiers of government. The surveys would focus on:
  - measures taken to prevent computer security attacks or compromises;
  - the prevalence of computer security attacks or compromises;
  - the types of computer security attacks or compromised experienced;
  - the effects of victimisation, including financial losses; and
  - responses following computer security attacks or compromises.

  The surveys would collect relevant demographic information, including age of the respondents, therefore allowing for further analysis as to seniors' experiences with cyber-safety issues.
- An annual review of data collected by the anticipated national reporting centre to identify new threats, targets and offender modus operandi.
- Compilation of official statistics on the number, types and outcomes of:
  - cybercrime investigations undertaken by federal and state/territory police;

- cybercrime matters prosecuted by Commonwealth and state/territory offices of public prosecutions;

- sentencing and correctional outcomes relating to cybercrimes prosecuted in the courts; and

- comparative criminal justice administrative data across jurisdictions and selected overseas countries.

The overall objective of such research activities would be to contribute to a more secure online environment, through the identification of problems and effective responses. Improved targeting of cybercrime threats would enhance community confidence in using electronic commerce and e-government resources. Research would also aim to provide statistically sound national data on prevalence and types of cyber security incidents and emerging threats.

The monitoring program results would improve knowledge of the nature and dimensions to the problem, and of suitable risk management strategies, thereby enabling government agencies and the private sector to set priorities and better target scarce resources in fighting cybercrime. As Australia's national research and dissemination centre on crime and justice, the AIC would be interested and qualified to undertake this work.

References

Australian Bureau of Statistics 2008a. *Personal Fraud. Cat. no. 4528.0.* Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/4528.0

Australian Bureau of Statistics 2008b. *Population Projections Australia 2006 to 2101. Cat. no. 3222.0.* Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/3222.02006%20to%202101?OpenDocument

Australian Bureau of Statistics 2011. *Household Use of Information Technology, Australia, 2010-11. Cat. no. 8146.0.* Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8146.02010-11?OpenDocument

Australian Law Reform Commission 2008. *For Your Information: Australian Privacy Law and Practice* (Vol. 2). Barton: Commonwealth of Australia. http://www.alrc.gov.au/publications/report-108

Bronitt S & McSherry B 2001. *Principles of Criminal Law.* Pyrmont: LBC Information Services.

Choo K K R, Smith R G & McCusker R 2007. Future directions in technology-enabled crime: 2007–09. *Research and Public Policy series no. 78.* Canberra: Australian Institute of Criminology.

Clarke R V 1995. Situational crime prevention. In M Tony & D P Farrington (eds), *Building a Safer Society: Strategic Approaches to Crime Prevention* (pp. 91-150). Chicago: University of Chicago Press.

Cohen L E & Felson M 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588-608.

Department of Broadband, Communications and the Digital Economy 2011. *Internet service provider (ISP) filtering.* http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering

Department of the Prime Minister and Cabinet 2011. *Connecting with Confidence: Optimising Australia's Digital Future.* Canberra: Department of the Prime Minister and Cabinet. http://cyberwhitepaper.dpmc.gov.au/white-paper

Johnson, K D 2003. *Financial Crimes Against the Elderly.* Problem Guide No. 20. Office of Community Oriented Policing Services. http://www.popcenter.org/problems/crimes_against_elderly/

Newman, G & Clarke R V 2003. *Superhighway Robbery: Preventing E-commerce Crime.* Cullompton: Willan Publishing.

Richards K 2009. *The Australian Business Assessment of Computer User Security: A national survey. Research and public policy series no. 102.* Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/100-120/rpp102.aspx

Ross S & Smith R G 2011. Risk factors for advance fee fraud victimisation. *Trends & Issues in Crime and Criminal Justice no. 420.* Canberra: Australian Institute of Criminology. http://aic.gov.au/publications/current%20series/tandi/401-420/tandi420.aspx

Shannon J & Thomas N 2005. Human security and cyber-security: Operationalising a policy framework. In Broadhurst & Grabosky (Eds.), *Cyber-Crime: The Challenge in Asia* (pp. 327-346). Aberdeen: Hong Kong University Press.

Smith R G 2008. Coordinating individual and organisational responses to fraud. *Crime, Law and Social Change, 49*(5), 379-396.

Smith R G & Grabosky P N 2011. Cybercrime. In Marmo M, de Lint W & Palmer D (eds.), *Crime and Justice: A Guide to Criminology* (4th ed.). Sydney: Thomson Reuters.

Smith R G, Wolanin N & Worthington G 2003. E-crime solutions and crime displacement. *Trends and Issues in Crime and Criminal Justice no. 243.* Canberra: Australian Institute of Criminology. http://aic.gov.au/publications/tandi/tandi243.html

Wong K C & Wong G 2005. Cyberspace governance and internet regulation in China. In Broadhurst & Grabosky (Eds.), *Cyber-Crime: The Challenge in Asia* (pp. 57-78). Aberdeen: Hong Kong University Press.