SUBMISSION NO. 16

House of Representatives Standing Committee on Communications: Inquiry into Cyber Crime

Submission from the Australian Bureau of Statistics, June 2009

1 The availability, quality and comparability of data is fundamental to developing an effective understanding of the extent and implications of cyber crime. However, developing an evidence base to provide information about cyber crime poses significant challenges. This submission outlines the key measurement challenges, suggests ways in which they may be tackled, and describes information currently available from the ABS that may help to understand cyber crime.

Key challenges in providing an evidence base around Cyber Crime

2 The main challenges in producing more reliable and complete estimates of cyber crime prevalence that can be used to establish and monitor risk, are:

- a lack of precision in the definition of what constitutes cyber crime;
- a lack of clarity around the information needs required to support policing, policy and community education work in the area of cyber crime;
- the varying sophistication amongst individuals and/or businesses in possessing sufficient knowledge and skills to understand, manage, detect and respond to security issues;
- the wide range of agencies involved in the policing, investigation, detection and monitoring of aspects of cyber crime, which makes the recording and compilation of administrative information about these crimes more complicated;
- the 'hidden' nature of many cyber crime events - i.e. they are not easily detectable;
- that often victims are unaware of breaches of e-security or electronic fraud, restricting the efficacy of data collected via surveys and/or administrative data - i.e. cyber crime is not easily recognisable; and
- understanding what data are available nationally and determining the level of comparability.

Definition of Cyber Crime

3 The most significant measurement issue is the lack of a national definition of cyber crime. The ABS views it as essential to have a common understanding of what constitutes cyber crime or e-crime in Australia, and the relationships between concepts used domestically and internationally, in order to build a relevant evidence base. The definitional issue emerges because cyber crime is not a stand-alone criminal offence, but rather reflects a broad spectrum of criminal offence types and behaviours committed via electronic means. These offences can be either variations of more traditional offences which utilise the electronic mode (such as fraud, child exploitation, theft and blackmail), or can be offences which require opportunities created by the on-line environment (such as hacking, virus development, botnets, etc.). Experts working in the field may have different understandings of various forms of cyber crime compared with those involved in more general law enforcement, and the business and wider community. In addition, legislative definitions of these offences may vary between the Commonwealth, state and territory statutes.

4 Given this starting point, it is not surprising that data exist across a wide spectrum of private and government agencies that have a remit to respond to various cyber crimes such as personal frauds and scams. It can be difficult, however, to understand the prevalence of such incidents in the general community using data from administrative sources, due to the lack of national data and standards across these agencies and the sheer number of organisations involved. Cyber criminals often seek to gain advantage over a victim by means of deception, and consumers may choose not to disclose to authorities that they have been a victim. As a result, low reporting rates to agencies will limit the coverage of such incidents in administrative data.

5 Until there is a clearer articulation of cyber crime and the areas of measurement focus, there will be significant limitations in developing a sound evidence base either through administrative sources or by means of household and business surveys.

Improving the evidence base and data comparability across Australia

6 Defining and explaining the relationship between the various elements of cyber crime is a necessary step towards developing sound estimates of the nature and prevalence of cyber crime and the risks and preventative measures applied in Australia. The ABS has expertise in developing statistical and conceptual frameworks for the crime and justice sector, and a conceptual framework on cyber crime could be developed by the ABS. A conceptual framework is a tool that presents a coherent and comprehensive conceptual map of a field of statistics. It defines important concepts and issues and provides a common language for analysis and discussion of statistics for a particular topic. The tool is also useful in promoting the use of standards and classifications, and supporting consistent data collection and analysis across jurisdictions and over time. Such a framework needs to reflect the evolving nature of cyber crime, and be flexible enough to use into the future.

7 In addition to the development of a conceptual framework, the following would be positive actions to improve the evidence base:

- Identify the key policy and research needs to inform policy development and or evaluation of programs (preferably integrated into the development of a conceptual framework);
- Conduct a national stocktake of data that exist around the topic of cyber crime;
- Develop a set of core indicators that could be used in data collection activity;
- Construct an alternative view of the Australian Standard Offence Classification that articulates cyber crime across traditional offence types;
- Develop of a set of counting rules to assist with standardising administrative data collection across agencies involved in monitoring or policing cyber crime;
- Develop agreements to collect this information from administrative agencies based on agreed standards;
- Form agreements for the sharing of data and information between agencies.

Data available from the ABS

Nature and prevalence of e-security risks including financial fraud and theft of personal information

8 Personal fraud has been recognised as a crime type that is a growing threat to the community, as a result of the rapid expansion and availability of internet technology and the increase in electronic storage, transmission and sharing of data.

9 Although household surveys cannot provide a definitive measure of crime, they can be particularly valuable as they ask people in the community directly about their experiences of crime, and can overcome coverage issues associated with under-reporting in administrative data. Counts of victims who have experienced electronic crimes that are identified through household surveys may not appear in administrative agencies, including police agencies, as the incidents may not be reported by the victim to those agencies.

10 The ABS conducted its first national survey on personal fraud in 2007, providing a national benchmark of the extent of identity fraud (credit/bank card fraud, identity theft) and selected scams (lotteries, pyramid schemes, phishing and related scams, financial advice, chain letters, advance fee fraud), and the level of financial loss as a result of being victimised. The survey also provided a range of demographic characteristics about the victim and characteristics about the most recent incident of fraud. Results can be found in *Personal Fraud, Australia, 2007* (cat. no. 4528.0). The survey was commissioned by the members of the Australasian Consumer Fraud Taskforce.

11 The ABS intends to include some aspects of personal fraud in its 2010-11 National Crime Victimisation survey. However, not all elements of the 2007 survey can be repeated due to a mixture of resource constraints and specific issues associated with the collection of data on personal fraud. ABS also notes that this survey does not capture information about the impact of IT security breaches such as malicious software.

Level of understanding and awareness of e-security risks within the Australian Community

12 There is limited data available on this topic; however, some data measuring Australian children's experiences of internet or mobile phone victimisation is currently being collected by the ABS. The ABS will be

releasing data in late 2009 about children's cyber safety from its Children's Participation in Culture and Leisure Activities Survey. The survey includes information about access and usage of the Internet by children, personal safety and security measures employed in the home, personal safety or security issues encountered by children using the internet or mobile phones, and actions taken to deal with these incidents.

The implications of these risks on the wider economy

13 Cyber crime does have implications for the wider economy as it can impact heavily on businesses. In some cases the cost of fraud experienced by consumers may be borne by businesses (for example financial institutions). Small businesses may be particularly exposed due to lack of awareness of security issues and limited resources for on-line protection.

14 By comparing the performance of businesses impacted by security incidents or breaches with those that have not experienced such incidents, it may be possible to obtain some quantification of impacts. The ABS Business Longitudinal Database could possibly provide a starting point for such an analysis.

Emerging technologies to combat risk

15 The ABS collects limited information relating to cyber crime covering the business sector. The ABS's Business Use of Information Technology Survey in 2005-06 produced information about IT security measures adopted by businesses, whether businesses experienced any IT security incidents or breaches, and what actions were taken as a result of these incidents/breaches. IT security measures included specific technologies such as spam filters, firewalls, etc. Results are in *Business Use of Information Technology, Australia* (cat. no. 8129.0).

16 The ABS's 2007-08 Business Use of Information Technology Survey also captured some of this information, but in less detail, given the Australian Business Assessment of Computer User Security survey conducted by the Australian Institute of Criminology (AIC). Results from this survey examined trends in business victimisation and protection measures and were released by the AIC in June 2009.

Conclusion

17 While some national data exist around elements of cyber crime, the detail and scope of the data is limited and further work could be done to improve Australia's evidence base in this area. The primary opportunities to improve Australia's evidence base on cyber crime lie in appropriately defining the elements of the conceptual field of 'cyber crime', and improving the collation of information from the various agencies that monitor and police elements of cyber crime. A stocktake of available information, against a strong conceptual framework with supporting tools such as appropriate classifications, would facilitate this process. Agreements for the sharing of information between agencies would also need to be considered. Opportunities also exist to measure some aspects of cyber crime from national ABS surveys. These aspects include: the nature of and prevalence of cyber crime (collected from businesses or consumers); the level of understanding and awareness of e-security risks within the Australian community; the community's ability to manage/deal with these risks; and the level of technology adopted by the community to combat these risks.

18 In total, a substantial amount of work is required to significantly improve and sustain an evidence base on cyber crime. Critically, it is important to recognise that the nature of cyber crime will continue to develop and change, and hence its measurement will represent an ongoing challenge. Appropriate resources will need to be provided to those involved in developing the evidence base required to develop an effective understanding of the extent and implications of cyber crime.

19 ABS would welcome the opportunity to discuss these issues further should the Committee be interested.

Australian Bureau of Statistics
June 2009