3

Research and Data Collection

Introduction

3.1 As noted in Chapter 2, cyber crime is highly complex, cross jurisdictional, and continually evolving. These factors make it inherently difficult to gain clear insights into the nature and incidence of cyber crime, and have led to a fragmentation and disparity in data collection and research activities.[1]

3.2 This chapter examines the current sources of data and research on cyber crime in Australia, and canvasses a number of proposals to improve the collation, analysis and reporting of cyber crime information and trends.

Current research and data collection

3.3 A range of submitters to the inquiry argued that a solid evidence base upon which to base policy decisions is lacking[2], and advocated the need for a clearer understanding of cyber crime to formulate a more effective

---

1 See for example: Australian Bureau of Statistics (ABS), *Submission 16*, p.1; Northern Territory Government, *Submission 53*, p.1; AusCERT, *Submission 30*, p.11; Internet Safety Institute, *Submission 37*, p.7.

2 The 2004 Cybercrime inquiry by the Joint Committee on the Australian Crime Commission accepted that there is a lack of independent cyber crime trend information available to the finance industry and law enforcement agencies. The Australian Government's response cited the secondment of specialists to, and information sharing through, the Australian High Tech Crime Commission as new measures. See: Parliamentary Joint Committee on the Australian Crime Commission, *Cybercrime*, March 2004, pp. 40, 49 and 66; Australian Government, Australian Government Response to the Recommendations of the Parliamentary Joint Committee inquiry on Cybercrime, 9 February 2006, pp.5 and 7.

policy response.[3] For example the Australian Communications and Media Authority (ACMA) noted that estimates on losses from fraud in Australia vary from $595 million to more than $2.2 billion, and advocated the need for accurate independent data on such losses.[4] Similarly, the Attorney General's Department (AGD) submitted:

> The capacity of government agencies to develop a targeted response to online identity crime is limited by a lack of detailed information. This means that statistics do not provide meaningful information on the type of identity crime, including whether it was conducted in the digital or real worlds; and makes comparison of data sets from different sources and across jurisdictions difficult.[5]

3.4 Detective Superintendent Brian Hay, Queensland Police Service (QPS), gave a similar opinion in regards to online fraud:

> You cannot do anything unless you have the information. The reality is that there is not one organisation, in my personal belief, in this country that could give you a truly accurate determination of the fraud status. Even the Australian Institute of Criminology would agree that there is much underreporting and that information is siloed in various databases within different types of industries.[6]

3.5 A number of government agencies, industry participants and members of the online community receive or collect data, or conduct research, on various aspects of cyber crime. These activities are largely fragmented and come in a variety of forms:

- data gathering on technical threats to the Australian network, such as malware infections and botnet activity;
- the receipt of complaints from victims of cyber crime, particularly in relation to identity fraud and scams; and
- surveys and other research projects on technical vulnerabilities, user behaviours and the impact of cyber crime.

---

3 See for example: ABS, *Submission 16*, p.1; Australian Institute of Criminology (AIC), *Submission 41*, p.22; Australian Payments Clearing Association (APCA), *Submission 50*, p.7; ACMA, *Submission 56*, p.17; Mr Alastair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, pp.63-64.

4 ACMA, *Submission 56*, p.17.

5 AGD, *Submission 44.1*, p.3.

6 Detective Superintendent Brian Hay, QPS, *Transcript of Evidence*, 17 March 2010, p.7.

3.6 Technical network data on cyber crime is collected by a variety of actors, and is generally focused on providing up-to-date information on specific threats and vulnerabilities on the Australian network, and the Internet as a whole.

3.7 Global information technology (IT) security companies use their vast technical networks and expertise to collect data on malware and fraud, and release their findings publicly via quarterly, half-yearly or annual 'threat reports' and issues papers.[7] For example, Mr Craig Scroggie, Managing Director, Pacific Region, Symantec Corporation, informed the Committee:

> Symantec's perspective is largely derived from research conducted by our global intelligence network, which monitors more than 30 per cent of the entire world's email traffic and gathers intelligence from 240,000 sensors deployed worldwide in more than 200 countries.[8]

3.8 Australian members of the IT security industry also monitor malicious online activity and make data publicly available. For example, AusCERT monitors and provides daily bulletins on technical threats to the Australian network.[9] Additionally, a number of voluntary online technical communities collect technical data on cyber crime. For example, the Shadowserver Foundation, the Australian Honeynet Project and the Spam and Open Relay Blocking System collect and share technical information on botnets and spam.[10]

3.9 The ACMA's Australian Internet Security Initiative (AISI) utilises these sources to identify Australian computers that may be part of a botnet (See Chapter 7). AISI does not currently aggregate data for broader trend analysis and research.[11]

3.10 It was noted that some Australian Government agencies, in partnership with members of industry (including the IT and finance sectors), collect and share intelligence on cyber crime to support national security,

---

7 See for example: McAfee Australia Pty Ltd, *Submission 10*, pp.13-14; RSA, *Submission 2*, p.2; Threatmetrix Pty Ltd, *Submission 19*, p.3; Sophos Pty Ltd, *Submission 66*, p.2.

8 Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.50.

9 AusCERT, *Submission 30*, pp.3, 12.

10 ACMA, *Submission 56.1*, p.2.

11 ACMA, *Submission 56*, pp.3-4.

particularly in relation to protecting critical infrastructure.[12] These activities are discussed in Chapter 5.

3.11 Commonwealth, State and Territory consumer protection and law enforcement agencies obtain some insights into cyber crime when receiving and investigating complaints from victims.[13] These reporting mechanisms are also discussed in Chapter 5. Mechanisms exist to share this data, however they do not aggregate data for broader trend analysis.[14]

3.12 In relation to identity theft and fraud, AGD noted that the majority of offences are reported to financial institutions.[15] Some members of the Australian banking and payments industries collate and publish this information. For example, the Australian Payments Clearing Association publicly releases half yearly reports on fraud losses in Australia, including losses from online fraud.[16]

3.13 Further insights into cyber crime are gained by specific surveys and research projects, as detailed below.

3.14 The Australian Institute of Criminology (AIC) conducts research on cyber crime in its capacity as Australia's national research and knowledge centre on crime and justice. The research of the AIC has led to the publication of a range of academic papers and surveys:

- *Crime in the Digital Age* (1998) examined criminal techniques involving telecommunication systems and the Internet, and protective measures;
- *Electronic Theft* (2001) and *Cyber Criminals on Trial* (2004) examined the commission and prosecution of financially motivated cyber crime; and
- most recently, in 2009 the AIC undertook the *Australian Business Assessment of Computer User Security Survey* (ABACUS) which collected data on the prevalence, nature and impact of computer security incidents experienced by Australia businesses.[17]

---

12 AGD, *Submission 44*, pp.7-9; ASIO, *Submission 47*, pp.4-5; Department of Defence, *Submission 20*, p.1.

13 See for example: Australian Competition and Consumer Commission (ACCC), *Submission 46*, pp.2-3; AFP, *Submission 25*, p.20; Queensland Government, *Submission 67*, p.7.

14 ACCC, *Supplementary Submission 46.1*, p.2; South Australian Police, *Submission 10*, p.4.

15 AGD, *Submission 44.1*, p.3.

16 Mr Anthony Burke, ABA, *Transcript of Evidence*, 8 October 2009, p.54; Mr Christopher Hamilton, APCA, *Transcript of Evidence*, 11 September 2009, p.70; Mr Richard Johnson, *Transcript of Evidence,* 8 October 2009, p.52.

17 AIC, *Submission 41*, p.1.

3.15 The Australian Bureau of Statistics (ABS) gathers some data on cyber security through broader surveys:

- in 2007 the first national *Personal Fraud Survey* reported on online scams;
- the *Business Use of Information Technology Survey*, a repeatable survey running intermittently since 1993, reports on, among other things, the data breaches and online security precautions of Australian businesses.[18]

3.16 Universities and other research institutions, both in Australia and overseas, continue to carry out a plethora of research projects on technical and behavioural cyber crime issues.[19]

3.17 Additionally, the QPS informed the Committee of two operations, *Operation Echo Track* and *Operation Hotel Fortress*, which have gathered information on victims of advance fee fraud, including romance scams. The QPS also cited their *Seniors Online Fraud Project*, carried out in partnership with the Queensland University of Technology, which researches the vulnerabilities of seniors to online fraud and scams.[20]

3.18 A number of government agencies and private organisations have also carried out cyber crime related surveys and assessments:

- in 2006 and 2008, the Department of Broadband, Communications and the Digital Economy (DBCDE) commissioned KPMG to carry out threat and vulnerability assessments for Australian home users and small businesses (these assessments remain confidential);[21]
- between 2002 and 2006 AusCERT, in partnership with Australian law enforcement agencies, carried out the *Australian Computer Crime and Security Survey* on online behaviour and computer security;[22]
- in 2008 AusCERT carried out the *Home User Computer Security Survey* to assess the awareness and security precautions of end users;[23]

---

18 ABS, *Submission 16*, pp.2-3.

19 See for example: AIC, *Submission 41*, p.41.

20 Queensland Government, *Submission 67*, pp.4 and 6; Detective Superintendent Brian Hay, QPS, *Transcript of Evidence*, 17 March 2010, pp.2-3.

21 DBCDE, *Submission 34.1*, p.7.

22 AusCERT, *Australian Computer Crime and Security Surveys,* AusCERT, 22 May 2006, viewed 19 March 2010, <http://www.auscert.org.au/render.html?it=2001>.

23 AusCERT, *Submission 30*, pp.3, 12.

- global IT security companies conduct a range of surveys on user behaviours and security precautions, such as Symantec's 2009 worldwide *Storage and Security in Small and Midsized Businesses Survey* and McAfee's 2007 *Datagate: The Next Inevitable Corporate Disaster* report, both of which surveyed over a thousand businesses worldwide.[24]

Challenges to research and data collection

3.19 A series of challenges to cyber crime research and data collection were identified during the inquiry:

- the compatibility of diverse sources of data;[25]
- the under reporting of cyber crime incidents;[26] and
- a lack of focus on the needs of policy makers.[27]

Compatibility of data

3.20 The Committee heard that varying definitions of cyber crime, and varying practices in the collection of statistics, hamper the development of an accurate evidence base for policy development.[28]

3.21 The ABS submitted that reliable data collection and research is impeded by varying definitions of cyber crime among different institutions.[29] For example, AGD define cyber crime as crimes against computers or computer systems (such as malware intrusions)[30], however other Australian Government agencies, such as the AIC and the Australian Federal Police, extend the definition of cyber crime to include traditional offences that are increasingly committed online (such as scams).[31]

3.22 The ABS explained that:

---

24 Symantec Corporation, *Submission 32*, p.9; McAfee, *Datagate: The Next Inevitable Corporate Disaster*, McAfee, viewed 24 March 2010, <http://www.mcafee.com>.

25 ABS, *Submission 16*, p.1.

26 ABS, *Submission 16*, p.1; Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.2.

27 ABS, *Submission 16*, p.1.

28 ABS, *Submission 16*, p.2.

29 ABS, *Submission 16*, p.1.

30 AGD, *Submission 44*, p.3.

31 AIC, *Submission 41*, pp.3-4; AFP, *Technology Enabled Crime*, AFP, 2 September 2009, viewed 15 March 2010, <http://www.afp.gov.au/national/e-crime.html>.

> 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.).[32]

3.23 Additionally, ABS argued that there exist varying methods for the collection of data among different institutions, thus leading to inconsistent data quality.[33]

3.24 To address these issues the ABS advocated the development of a conceptual framework for the collection of data that defines important concepts and issues, and supports consistent data collection and analysis across different agencies and jurisdictions. The ABS also suggested adjusting the Australian Standard Offence Classification[34] to note traditional offence types that were committed online.[35]

Under reporting

3.25 Contributors argued that data gathered via surveys and consumer complaint mechanisms may lack accuracy due to under reporting. It was argued that this issue stems from: a lack of incentives for businesses to report data breaches; inefficient reporting mechanisms; and the surreptitious nature of cyber crime.[36]

3.26 Businesses may under report cyber crime incidents in order to protect their reputation.[37] Mr Michael Sinkowitsch, Business Development Manager, Fujitsu Australia Ltd, explained:

---

32 ABS, *Submission 16*, p.1.

33 ABS, *Submission 16*, p.1.

34 The Australian Standard Offence Classification is used in ABS statistical collections, and by Australian police, criminal courts and corrective services agencies, to provide uniform classifications of criminal behaviour in crime and justice statistics.

35 ABS, *Submission 16*, p.2.

36 See for example: Mr Michael Sinkowitsch, Fujitsu Australia Ltd, *Transcript of Evidence*, 11 September 2009, p.51; Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, pp.2 and 6; ABS, *Submission 16*, p.2; Detective Superintendent Brian Hay, QPS, *Transcript of Evidence*, 17 March 2010, p.7.

37 Ms Alana Maurushat, Cyberspace Law and Policy Centre, *Transcript of Evidence*, 8 October 2009, p.33.

> ... if a financial institution does not wish to publish attacks on it because it wants to protect its underlying corporate viability and so on, ... government ... does not have all the information to hand that it needs ... to implement the correct strategies in order to meet ... threats, new and emerging, ...[38]

3.27 To address this issue, submitters proposed mandating the reporting of such breaches.[39] This proposal was made primarily to deal with privacy concerns (See Chapter 9), however mandatory reporting would also improve the quality of data on cyber crime.

3.28 In relation to cyber crime reporting, a number of Commonwealth, State and Territory law enforcement and consumer protection agencies receive complaints from victims of cyber crime.[40] Witnesses noted that these reporting mechanisms are not always easily accessible, widely publicised or efficient (See Chapter 5).[41] The difficulty of reporting is likely to deter victims from making a complaint which in turn leads to under reporting.

3.29 The ABS also argued that victims may choose not to disclose incidents due to embarrassment over being deceived by a scam or fraud.[42] Detective Superintendent Brian Hay, QPS, told the Committee that out of the 139 victims of advanced-fee fraud interviewed in a QPS study, including victims of romance scams, 'not a single [person] ever made a complaint to police'.[43]

3.30 Similarly, ACMA commented that while an initial cyber crime incident (such as a malware intrusion) may be noticed by a victim, further crimes that flow on from this initial incident (such as identity theft and fraud) may go unreported.[44]

---

38 Mr Michael Sinkowitsch, Fujitsu Australia Ltd, *Transcript of Evidence*, 11 September 2009, p.51.

39 See for example: Office of the Privacy Commissioner, *Submission 3*, pp.11-12; Symantec Corporation, *Submission 32*, p.11; Fujitsu Australia Ltd, *Submission 13*, p.7; Detective Superintendent Brian Hay, QPS, *Transcript of Evidence*, 17 March 2010, p.7.

40 AFP, *Submission 25*, p.20; Queensland Government, *Submission 67*, p.7; ACCC, *Submission 46*, pp.5-7.

41 Mr Paul Brooks, Internet Society of Australia, *Transcript of Evidence*, 9 October 2009, p.6; Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.2; Mr David Ready, *Submission 6*, p.1; Mr Mike Rothery, AGD, *Transcript of Evidence*, 25 November 2009, p.14.

42 ABS, *Submission 16*, p.1.

43 Detective Superintendent Brian Hay, QPS, *Transcript of Evidence*, 17 March 2010, p.3.

44 ACMA, *Submission 56*, p.18.

Information for policy development

3.31 The ABS submitted that the wide variety of agencies that receive data on cyber crime makes the compilation of data more complicated, and argued that there is a lack of focus on data to support the development of anti-cyber crime policy measures.[45] The Internet Safety Institute submitted that 'there is no single institution in Australia … which has a whole-of-internet national view of e-security victimisation'.[46] Detective Superintendent Brian Hay, QPS, also told the Committee that, in the private sector 'information is siloed in various databases within different industries'.[47]

3.32 Contributors argued that in order to address these issues, a more coordinated and cooperative approach to data collection, information sharing and analysis is required.[48] In particular, the ABS proposed forming official agreements between government agencies for the sharing of information.[49] It was also argued that a centralised reporting portal for victims would assist in more efficient data gathering and information sharing (See Chapter 5).[50]

3.33 Both the AIC and Telstra advocated developing formal links with universities and the international research community to take advantage of other existing cyber crime research and data analysis activities.[51]

3.34 Additionally, the ABS indicated that there are opportunities to measure some aspects of cyber crime, including cyber crime incidence, awareness and precautions, through current ABS activities such as the *Business Longitudinal Database*[52] and other national surveys. The ABS suggested that additional insights could be gained by using other existing information sources, and proposed a national stock take of current data collection mechanisms to identify such sources.[53]

---

45 ABS, *Submission 16*, p.1.

46 Internet Safety Institute, *Submission 37*, p.11.

47 Detective Superintendent Brian Hay, QPS, *Transcript of Evidence*, 17 March 2010, p.7.

48 See for example: AIC, *Submission 41*, pp.16-17; ABS, *Submission 16*, p.2; Australian Computer Society, *Submission 38*, p.9.

49 ABS, *Submission 16*, p.2; Symantec Corporation, *Submission 32.1*, p.9.

50 See for example: Fujitsu Australia Ltd, *Submission 13*, p.7; Mr Alastair MacGibbon, *Cyber security: Threats and responses in the information age*, Australian Strategic Policy Institute, December 2009, pp.11-12; Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.15.

51 AIC, *Submission 41*, p.22; Telstra, *Submission 43*, p.3.

52 The Business Longitudinal Database comprises financial data sourced from the ABS Business Characteristics Survey, the Australian Taxation Office and the Australian Customs Service.

53 ABS, *Submission 16*, pp.2-3.

Committee View

3.35 The Committee acknowledges the proactive approach taken by a number of government agencies, industry members, research institutions and private citizens to collecting data, conducting research and sharing information on cyber crime. However, there was a clear message to the Committee that these activities are fragmented, and that a more coherent approach is needed to collate information, to ensure that government policy is responsive to trends in cyber crime.

3.36 The Australian Government's policy response to cyber crime must be informed by independent and comprehensive information on cyber crime trends. This requires that the data collected by government and industry be accurate, compatible and accessible. To achieve this the Australian Government should nominate an appropriately qualified agency(s), such as the AIC and/or ABS, to:

- conduct a stock take of current data collection and research initiatives, including activities of government agencies, industry, research institutions and voluntary online communities, in order to identify resources that could be better utilised, and to identify gaps in current data collection activities;
- work to develop clear national definitions and procedures to be used in the collection of data on cyber crime; and
- negotiate clear agreements on the sharing and protection of information between government agencies and industry for the purpose of research and policy development.

Recommendation 1

That the Australian Government nominate an appropriate agency(s) to:

- **conduct a stock take of current sources of data and research on cyber crime;**
- **develop clear national definitions and procedures for the collection of data on cyber crime; and**
- **negotiate clear agreements between government agencies and industry on the sharing and protection of information for research purposes.**

3.37 This agency(s) should publish a comprehensive annual or bi-annual report on the status of cyber crime in Australia. In producing the report, the agency(s) should compile and examine data from the wide variety of existing sources including law enforcement agencies, consumer protection agencies, other government initiatives (such as AISI) and industry. The Committee considers that the vast amounts of data collected by global IT companies and the finance industry would be particularly valuable in compiling such reports. The report could also be informed by a comprehensive ABS survey on cyber crime issues.

Recommendation 2

That the Australian Government nominate an appropriate agency(s) to collect and analyse data, and to publish an annual or bi-annual report on cyber crime in Australia.