11

Emerging Technical Measures to Combat Cyber Crime

Introduction

11.1 This chapter examines a range of emerging technical measures that may assist in combating cyber crime. It also briefly canvasses ways to encourage the development of new anti-cyber crime measures.

11.2 Cyber crime is continually evolving and adapts to anti-cyber crime measures, thus emerging technical solutions only provide a partial response and are unlikely to offer a complete solution.[1] Nevertheless, technological measures can improve personal security and the resilience of the Internet and information communication technologies (ICTs). Support for technological innovation must therefore remain an important part of the overall national response to cyber crime.

Emerging technical measures

11.3 This section examines the following technical measures:

- smart cards;
- two factor identification;
- an identity metasystem;

1 See for example: Commonwealth Scientific and Industrial Research Organisation (CSIRO), *Submission 26*, p.4; Australian Institute of Criminology (AIC), *Submission 41*, p.17; Australian Security Intelligence Organisation, *Submission 47*, p.4; AusCERT, *Submission 30*, pp.21-22.

- Domain Name System Security Extensions;
- trusted networking infrastructure;
- new encryption techniques;
- privacy enhancing technologies;
- black listing;
- white listing;
- walled gardens;
- 'clean' boot-up disks;
- Trusted Platform Modules;
- black hole and sinkhole routing; and
- program monitoring.

Smart cards

11.4 Smart cards were suggested as a method for combating online identity theft and fraud. Smart cards are pocket-sized cards with an embedded microchip that can store large amounts of data, encrypt data and communicate with other devices. A smart card can take many forms including a credit card or an identity card. In relation to online security, smart cards may be inserted into a reader to authorise and conduct online financial transactions.[2]

11.5 Smart cards combat cyber crime in a number of ways including:

- automatically and randomly encrypting the data transferred in an online transaction to prevent tampering by cyber criminals;[3]
- providing extra sources of verification, such as encrypted card identifiers and unique PINs, to increase the difficulty of committing identity theft and fraud;[4]

2 See for example: AusCERT, *Submission 30*, p.21; Mr Stephen Wilson, Lockstep Technologies Pty Ltd, *Transcript of Evidence*, 9 October 2009, p.45; Smart Card Alliance, *Smart Card Primer*, Smart Card Alliance, 2010, viewed 28 January 2010, <http://www.smartcardalliance.org/pages/smart-cards-intro-primer>.

3 Lockstep Technologies Pty Ltd, *Submission 36*, p.16.

4 See for example: AusCERT, *Submission 30*, p.21; Australian Payments Clearing Association (APCA), *Submission 50*, p.5.

- automatically verifying that a website is legitimate and can be trusted;[5] and
- preventing identity fraud by recognising and blocking transactions being made from an unusual location or in excess of a daily spending limit.[6]

11.6 A number of financial institutions have already implemented smart card technology overseas and are in the process of rolling out smart cards in Australia.[7]

11.7 AusCERT argued that, while smart cards may assist in preventing some aspects of cyber crime, they do not address the threat of identity theft from computers infected with malware.[8] Additionally, the Australian Institute of Criminology (AIC) noted that several studies have demonstrated that technically competent criminals can still circumvent smart card security mechanisms. However the AIC also submitted that properly implemented smart cards are acknowledged as helping to combat identity theft and fraud. The AIC noted that there exists significant support for the continued research and implementation of such technologies.[9]

Two factor authentication

11.8 Two factor authentication is a procedure that combats online identity theft and fraud through adding an extra layer of verification when accessing online services and accounts. It requires the end user to present two factors. The first factor is something the person knows, such as a username or password. The second factor is either something the person has in their possession (such as an ID card), or a physical attribute of the user (such as a fingerprint). Attacks such as phishing or spyware may successfully steal the first factor, however without the second factor the cyber criminal cannot gain access to the account or service.[10]

11.9 A number of Australian businesses, including Australia Post and many financial institutions, use two factor authentication. When a user wishes to conduct a transaction online, not only must they gain access to their

---

5 Mr Stephen Wilson, Lockstep Technologies Pty Ltd, *Transcript of Evidence*, 9 October 2009, p.45

6 Lockstep Technologies Pty Ltd, *Submission 36*, p.16.

7 See for example: AusCERT, *Submission 30*, p.22; APCA, *Submission 50*, p.6.

8 AusCERT, *Submission 30*, p.22.

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

10 See for example: Australia Post, *Submission 27*, p.7; Z Ramzan, *Phsihing and Two-Factor Authentication*, blog entry, Symantec Security Blogs, July 11 2006, viewed 28 January 2009, <http://www.symantec.com/connect/blogs/phishing-and-two-factor-authentication>.

account through entering a password, but must also enter a unique six-digit code sent to their mobile by the business upon their request for the transaction. Thus users must provide two identification factors, each from a different category: a password (something retained in the user's memory) and a unique code proving possession of the correct mobile phone (something in the user's possession). The Commonwealth Bank of Australia informed the Committee that two factor authentication reduced their incidents of fraud by 96 per cent over 2005.[11]

11.10 Smart cards may also be used to provide the second category of two factor authentication (something in the user's possession). Users may be required to scan a smart card in order to conduct a transaction or gain access to a certain system.[12]

11.11 Australia Post submitted that secure two factor authentication services are currently readily available from online security companies, and suggested that two factor authentication could be extended to other online transactions.[13] For example, the Australian Taxation Office suggested that two factor authentication methods could make the lodging of online tax returns more secure.[14]

11.12 Two factor authentication may also require verification of a physical attribute through the use of biometrics. Biometrics are technologies that can identify unique physical attributes including fingerprints, iris prints, handprints, facial structures and voice signatures.[15]

11.13 Some witnesses argued that biometrics may not be sufficiently reliable and may still be circumvented by advanced cyber criminals.[16] The AIC acknowledged that biometrics do have some limitations, such as the expense of implementation, but argued that such technologies are very effective in solving some of the problems of cyber crime relating to passwords and PINs.[17]

---

11 See for example: Australia Post, *Submission 27*, p.6.; Mr John Geurts, Commonwealth Bank of Australia, *Transcript of Evidence*, 8 October 2009, p.59.

12 Lockstep Technologies Pty Ltd, *Submission 36*, pp.13-14.

13 Australia Post, *Submission 27*, p.6.

14 Australian Taxation Office, *Submission 59*, p.15.

15 Biometrics Institute Ltd, *FAQ – Answers*, Biometrics Institute Ltd, 2 July 2009, viewed 28 January 2009, <http://www.biometricsinstitute.org>.

16 See for example: Mr Wilson, Lockstep Technologies Pty Ltd, *Transcript of Evidence*, 9 October 2009, p.42; Ms Caroline Pearce, APCA Ltd., *Transcript of Evidence*, 11 September 2009, p.73.

17 Dr Russell Smith, AIC, *Transcript of Evidence*, 19 August 2009, p.16.

Identity metasystem

11.14 Microsoft advocated the creation of a system where all online authorisation procedures would be conducted through a single, standard program.[18]

11.15 Microsoft observed that in order to gain access to online services, Internet users are required to enter a range of different user names and passwords into many differing and unique online systems, and are often asked to provide a range of personal information.[19]

11.16 Microsoft suggested the risks to users from this process are threefold:

- users increase security risks by employing the same passwords and usernames for a range of different authentication procedures;
- users gain authorisation through a range of non-standard webpages and thus may not be able to recognise a phishing webpage; and
- users are asked to provide an ever increasing number of personal details to third parties, thus raising privacy issues.[20]

11.17 To combat these risks, Microsoft proposed an identity metasystem that would connect, but not replace, all current online authorisation procedures. Every time a user needed to provide authentication they would do so by entering various identifiers into a standard interface, instead of arbitrary details through an interface unique to each online service. In turn, this interface would use the identity metasystem to interact with the appropriate webpage or application to notify if the authentication was successful.[21]

11.18 Microsoft envisages that such a system would allow users to employ verifiable details to complete a range of different authentication procedures through one standard interface. In turn, Microsoft argues that

---

18 Mr Peter Watson, Microsoft Pty Ltd, *Transcript of Evidence*, 9 October 2009, p.17.

19 Microsoft Corporation, *Microsoft's vision for an identity metasystem*, Web services technical articles, Microsoft Corporation, May 2005, viewed 28 January 2009, <http://msdn.microsoft.com/en-us/library/ms996422.aspx>. See also: Microsoft Australia, *Submission 35*, pp.14-15.

20 See for example: Mr Peter Watson, Microsoft Australia, *Transcript of Evidence*, 9 October 2009, p.17; Microsoft Corporation, *Microsoft's vision for an identity metasystem*, Web services technical articles, Microsoft Corporation, May 2005, viewed 28 January 2009, <http://msdn.microsoft.com/en-us/library/ms996422.aspx>.

21 See for example: Mr Peter Watson, Microsoft Australia, *Transcript of Evidence*, 9 October 2009, p.17; Microsoft Corporation, *Microsoft's vision for an identity metasystem*, Web services technical articles, Microsoft Corporation, May 2005, viewed 28 January 2009, <http://msdn.microsoft.com/en-us/library/ms996422.aspx>.

password and username security would be enhanced, susceptibility to phishing schemes would decrease and user privacy would be strengthened.[22]

Domain Name System Security Extensions

11.19 As outlined in Chapter 2, cyber criminals can subvert parts of the Domain Name System (DNS) to divert users to a malware, phishing or scam website.[23]

11.20 Dr Paul Twomey, Senior President of the Internet Corporation for Assigned Names and Numbers (ICANN), advocated the implementation of DNS Security Extensions (DNSSEC) as a means of addressing this risk. DNSSEC is an eleven year old technology which has already been introduced in certain areas of the DNS, but is not yet widespread. It requires each genuine IP address in the DNS to be given a series of unique digital signatures that must match up in order to verify a website's authenticity.[24]

11.21 Several areas of the DNS have already implemented the technology for their country code, including Sweden, Brazil, Bulgaria and the Czech Republic. However, Dr Twomey argued that wider implementation of DNSSEC would reduce the capacity for hackers to subvert the DNS.[25]

Trusted networking infrastructure

11.22 The Commonwealth Scientific and Industrial Research Organisation (CSIRO) also informed the Committee of their work in developing a form of secure network that conceals information from 'outsiders', which prevents theft. CSIRO envisage that sections of the Australian network could be designated to be part of a secure information exchange system. This could be achieved through designating each individual router that

22 See for example: Mr Peter Watson, Microsoft Australia, *Transcript of Evidence*, 9 October 2009, p.17; Microsoft Corporation, *Microsoft's vision for an identity metasystem*, Web services technical articles, Microsoft Corporation, May 2005, viewed 28 January 2009, <http://msdn.microsoft.com/en-us/library/ms996422.aspx>.

23 Educause, *7 things you should know about DNS*, Educause, January 2010, p.1, viewed 1 February 2010, <http://net.educause.edu/ir/library/pdf/EST1001.pdf>.

24 See for example: Dr Paul Twomey, Internet Corporation for Assigned Names and Numbers (ICCAN), *Transcript of Evidence*, 8 October 2009, p.3; Educause, *7 things you should know about DNS*, Educause, January 2010, viewed 1 February 2010, <http://net.educause.edu/ir/library/pdf/EST1001.pdf>.

25 See for example: Dr Paul Twomey, ICCAN, *Transcript of Evidence*, 8 October 2009, p.3; Educause, *7 things you should know about DNS*, Educause, January 2010, viewed 1 February 2010, <http://net.educause.edu/ir/library/pdf/EST1001.pdf>.

would be part of the network, or by designating the ISPs whose customers would be part of the network. Each computer on the trusted network would have its own 'electronic contract' that would determine how its information is used, encrypted and accessed by other computers on the network. Computers outside of this trusted network would not be able to access the information. CSIRO proposed that these electronic contracts could be monitored for compliance to detect misbehaving computers.[26]

New encryption techniques

11.23 The Committee heard that new encryption techniques could also help to combat identity theft and fraud.[27] For example, Dr Peiyuan Zhu advocated his 'Masked Identification System' as a new method for securely encrypting data. Dr Zhu submitted that, through using a randomly generated encryption code that is unique to each data transmission, this new method would render intercepted information useless to cyber criminals.[28]

Privacy enhancing technologies

11.24 The Australian Office of the Privacy Commissioner told the Committee of a range of technologies that may enhance privacy and prevent identity theft, including:

- data separation and anonymising tools which remove personal identifiers from data during transmission and storage;
- privacy metadata which uses an electronic tagging system to control how information can be accessed and used; and
- privacy management systems which permit individuals to easily determine if the privacy policies of organisations meet their own requirements.[29]

Black listing

11.25 Currently, many organisations employ black listing to protect themselves from malicious websites and emails. Black listing involves monitoring all sources attempting to access and exchange data with a particular system.

---

26 CSIRO, *Submission 26*, pp.12-14.

27 See for example: Office of the Privacy Commissioner (OPC), *Submission 3*, p.13; Office of the Victorian Privacy Commissioner, *Submission33*, p.7.

28 Dr Peiyuan Zhu, *Submission 61*, pp.1-4.

29 OPC, *Submission 3*, pp.13-14.

The reputation of each source is assessed, and the data from the source is checked for signs of malicious code or content. Any sources that are then deemed to be malicious are placed on a 'black list' and denied access to the system.[30]

11.26 Technologies for assessing the risk of sources and data are continually emerging. Both Symantec and McAfee advocated products which gather data from a range of sources (including home users, software publishers and online businesses) in order to determine if a website, file or other computer system is a security risk, and thus if the source should be black listed.[31] Alternatively, ThreatMetrix Pty Ltd advocated their 'Device Intelligence' technology for online merchants which, through examining the location and configuration of customer's machines, detects and blocks fraudulent transactions.[32]

11.27 The Government has already taken steps to create an Australia-wide network black list to block malicious website content, albeit without the sole focus of addressing cyber crime. On 15 December 2009 Senator the Hon Stephen Conroy, Minister for Broadband, Communications and the Digital Economy, announced Government plans to legislate for Internet Service Providers (ISPs) in Australia to block all material contained on the Australian Communication and Media Authority's (ACMA's) Refused Classification Content list, including content relating to the detailed instruction in crime.[33] Whilst this content filtering exercise extends to a range of online content, through blocking content relating to the detailed instruction of crime, some cyber crime-related websites may also be blacklisted.

11.28 To carry out blacklisting on a higher network level, above that of ISPs, Web Management Interactive Technologies Pty Ltd, an Australian e-security business, advocated their Australian Protected Network (APN). The APN is essentially a network-wide firewall that is continually updated via a system that anticipates new threats. Under the APN, all Internet traffic entering the Australian network would pass through a central server. This traffic would be tested against a database of threat information, as compiled by members of the Australian Internet

30 Australian Bankers' Association (ABA), *Submission 7.1*, p.2; Sophos Pty Ltd, *Submissi*on 66, p.5.

31 Symantec Corporation, *Symantec delivers groundbreaking reputation-based security technology,* media release, Symantec Corporation, 10 September 2009, p.2; McAfee, *Submission 10*, pp.9-10.

32 Threat Matrix Pty Ltd, *Submission 19*, p.16.

33 Senator the Hon Stephen Conroy (Minister for Broadband, Communications and the Digital Economy), *Measures to improve safety of the internet for families*, Parliament House, 15 December 2009, viewed 29 January 2009, <http://www.minister.dbcde.gov.au/media/media_releases/2009/115>.

community, and traffic originating from known malicious sources would be blocked.[34]

White listing

11.29 White listing was advocated as another method of protecting users from malware and phishing attacks. White listing is a method whereby all sources attempting to access and exchange data with a system are monitored. Known trusted sources are placed on a 'white list' which permits access to the system, while all other sources (even benign but unknown sources) are denied access.[35]

11.30 The Australian Bankers' Association (ABA) submitted that white listing could be applied in a range of ways:

- online security software could white list 'known good' banking websites to deny access to phishing websites;
- ISPs could white list trusted sites to protect their clients from malicious websites; or
- banks could white list access to users from known and trusted locations to prevent identity fraud.[36]

11.31 However, contributors also argued that white listing has its limitations, especially when deployed across large networks with many diverse users. These limitations include: potentially blocking legitimate sources; restricting flexible access to systems (such as remote access); and increasing the complexity of already complex systems. Additionally, many home users may use 'dynamic IP addressing' where the code which identifies their computer or location is continually changing, thus making it difficult to accurately identify and white list users.[37]

Walled gardens

11.32 Walled gardens (as mentioned in Chapter 7) were suggested as means by which to isolate and disinfect computers that are infected with malware. Some ISPs in jurisdictions outside Australia follow a process where, when a customer is found to have a computer infected with malware, their Internet access is restricted in order to isolate them from other Internet

34 Web Management Interactive Technologies, *Submission 68*, p.3.

35 See for example: ABA, *Submission 7.1*, p.2; Sophos Pty Ltd, *Submissi*on 66, p.5; ICANN, *Submission 40.1,* p.3.

36 ABA, *Submission 7.1*, pp.2-3.

37 See for example: ABA, *Submission 7.1*, p.3; ICANN, *Submission 40.1,* p.3.

users. Such limited access is called a 'walled garden'. ISPs then assist the customer to eliminate the malware from the system and, once the user is disinfected, remove the user from the walled garden.[38] Some ISPs already carry out this process in Australia.

'Clean' boot-up disks

11.33 Detective Inspector William van der Graaf, NSW Police, argued that one of the key ways to ensure safe online banking was through the use of a 'clean' boot-up disk. A boot-up disk is a removable storage medium (such as a USB or CD) from which a computer can load and run an operating system. Detective Inspector van der Graaf told the Committee that users can conduct secure transactions by uploading a clean operating system from a boot-up disk each time they wish to transact online, rather than relying on existing operating systems that may be infected with malware.[39]

Trusted Platform Modules

11.34 CSIRO proposed the use of a Trusted Platform Module (TPM) to protect online transactions from malware and phishing. A TPM is a microchip which can verify the safety of another computer prior to conducting a transaction with that computer. When a user wishes to carry out a transaction, the TPM tests three factors against predetermined criteria: the identity of the other user, the identity of the other machine and the configuration of the other computer (including the type of programs installed on the machine). If all three criteria are met, the transaction proceeds. However, if there is any variation from the prescribed criteria (such as unknown programs) the transaction is blocked. In turn, TPM identifies malware on the other computer and reveals phishing websites.[40]

11.35 CSIRO informed the Committee that they have developed a TPM device in the form of a consumer-friendly USB drive, the Trusted Extension Device (TED), which operates on the same principle as the above mentioned clean boot-up disk method. Through the use of a TED, a user can upload a clean operating system to any PC, in order to conduct a transaction. The TED then goes beyond other clean boot up disks by employing a TPM to verify the safety of the other computer prior to a

38 See for example: Mr Bruce Matthews, Australian Communications and Media Authority, *Transcript of Evidence*, 21 October 2009, p.4; AusCERT, *Submission 30.1*, p.3.

39 Detective Inspector William van der Graaf, NSW Police, *Transcript of Evidence*, 8 October 2009, p.79.

40 CSIRO, *Submission 26*, p.10.

transaction. According to CSIRO, not only do users avoid malware on their own machine, but they are also protected from malware and phishing websites hosted on the other machine.[41]

11.36 CSIRO acknowledged that TPM devices currently have limited opportunities for deployment. In order for a transaction to be authorised by a TPM, the other computer must adhere to a rigid and prescribed system configuration. Thus TPM cannot currently be applied in transacting between computers that have diverse and continually updating operating systems or programs. CSIRO submitted that this prevents wide deployment of the TPM, and that they are working to overcome this issue.[42]

Black hole and sinkhole routing

11.37 Black hole and sinkhole routing are two different techniques for diverting and combating malicious web traffic, particularly Distributed Denial of Service (DDoS) attacks.

11.38 Black hole routing is the practice of, when a computer is under attack, redirecting all traffic attempting to access the computer to a null inactive router, a 'black hole'. This Internet traffic, including the malicious elements, then has nowhere to go and drops off. This prevents the attack on the computer, but also blocks any legitimate traffic that may be present.[43]

11.39 Sinkhole routing refers to the practice of, when a computer comes under attack, redirecting all web traffic flowing towards that computer through a router which evaluates the traffic, a 'sinkhole'. This sinkhole router analyses, blocks and traces any malicious traffic while permitting benign web traffic to continue on to its destination. Unlike black hole routing, sinkhole routing permits a computer to continue to receive web traffic during a web attack, but may be less able to effectively handle web attacks involving large amounts of data.[44]

---

41 CSIRO, *Submission 26*, p.11.

42 CSIRO, *Submission 26*, p.10.

43 See for example: Fujitsu Australia Ltd, *Submission 13*, p.8; C Patrikakis, M Masikos and O Zouraraki, 'Distributed Denial of Service Attacks', *Internet Protocol Journal*, Vol.7(4), December 2004, viewed 1 February 2010, <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html>.

44 CPatrikakis, M Masikos and O Zouraraki, 'Distributed Denial of Service Attacks', *Internet Protocol Journal*, Vol.7(4), December 2004, viewed 1 February 2010, <http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html>.

Program monitoring

11.40 Timesavers International Pty Ltd, an Australian e-security developer, informed the Committee of a new approach to preventing malware from infections, as achieved by their new 'CyberForceField' (CFF) software. Modern user-friendly programs (including many anti-virus programs) carry out a number of automatic functions, such as communicating with other programs, downloading updates, scanning hard drives and sending information to the developer. These functions can be subverted to shutdown anti-virus protection, install malware on computers and to intercept information. Timesavers CFF monitors the activity of all programs according to rules and security levels set by the user. CFF then restricts any functions that could expose the system to malware .[45]

11.41 Timesavers submitted that CFF represents a significantly different approach to e-security than the products of established and dominant e-security companies. Timesavers argued that, as a small enterprise, it is hard to gain entry into the wider e-security markets. Timesavers' called upon the Government to support innovative small enterprises to gain access to such markets.[46]

Developing and implementing anti-cyber crime measures

11.42 Contributors to the inquiry argued that the Government could assist in the development of new anti-cyber crime techniques and technologies through the National Broadband Network (NBN) and by creating incentives for the development and uptake of anti-cyber crime measures.

11.43 The Committee heard that the NBN represents an opportunity for the Government to make the online environment more secure for Australian Internet users. A number of methods were suggested, including:

- using the publicity surrounding the NBN to raise awareness and increase the uptake of online security technologies;[47]
- integrating security technologies into the infrastructure of the NBN;[48] and

45 Timesavers International Pty Ltd, *Submission 14*, pp.3-10.

46 Timesavers International Pty Ltd, *Submission 14*, p.11.

47 Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.53.

48 See for example: Sophos, *Submission 66*, p.4; Lockstep Technologies Pty Ltd, *Submission 36*, p.14; Mr Peter Watson, Microsoft Australia, *Transcript of Evidence*, 9 October 2009, p.17.

- utilising the increased speed of the NBN to deliver a 'cloud service' for internet security (where all users may access the internet through a central security mechanism, rather than via individual security mechanisms for each computer).[49]

11.44 It was argued that such initiatives could be furthered through partnering with industry and through allocating a percentage of the NBN's budget to security measures.[50]

11.45 Contributors also canvassed a range of ways to nurture the development and implementation of new security measures:

- engaging with, and harnessing the technical knowledge of, the highly coordinated engineering community that builds and runs the internet, in order to inform policy and to implement new security measures;[51]
- continuing to ensure a healthy, diverse and innovative market place for Internet security companies, which evolves and keeps pace with new cyber security threats;[52]
- encouraging software vendors to promote products that have been developed to international software and hardware security standards;[53] and
- provide financial incentives for Australian home users and small businesses to take up further technical online security measures.[54]

Committee View

11.46 The Committee is of the view that, while no single technology will solve the problem of cyber crime, the continually evolving nature of cyber crime will require innovative and creative responses. Part of this response will be technical devices that strengthen protections for the network. It is important that Australia foster an environment that values research and innovation, and recognises that important technical innovations can arise from a plethora of sources.

---

49 Mr Andrew Littleproud, McAfee Australia Pty Ltd, *Transcript of Evidence*, 9 October 2009, p.70.

50 See for example: ABA, *Submission 7*, p.15; Mr Peter Coroneos, Internet Industry Association, *Transcript of Evidence*, 8 October 2009, p.23.

51 Dr Paul Twomey, ICCAN, *Transcript of Evidence*, 8 October 2009, p.6.

52 Symantec Corporation, *Submission 32*, p.12.

53 Australian Computer Society Inc., *Submission 38*, p.11.

54 Symantec Corporation, *Submission 32*, pp.10-11.

11.47 The global IT corporations bring enormous expertise and capacity to commercialise new products, but breakthrough technologies often result from the inventiveness and creativity of dedicated individuals, small companies, and Australia's world class science and technology researchers.

11.48 The Committee concludes that the Government should consider the value of any current and emerging measures that may combat cyber crime, including the measures outlined in this chapter. The Committee is also of the view that the Government should consider ways to encourage the development and uptake of online security mechanisms, including through the NBN, industry partnerships and market incentives.

Ms Belinda Neal MP

Chair