10

Community Awareness and Education Initiatives

Introduction

10.1 In Chapter 4, the Committee concluded that the current level of awareness of cyber crime and e-security risks is insufficient to ensure the online safety of end users. This chapter discusses the current initiatives to raise community awareness and educate end users about cyber crime and its prevention. The chapter divides the topic into three sections:

- access to information—where consumers are provided with resources to inform themselves of the nature and prevention of cyber security threats;
- community awareness raising—where publicity campaigns aim to raise the profile of cyber security issues and bring about cultural change in the online behaviours of Australians; and
- skills development—where Australian end users are taught skills to protect themselves and their computer systems from cyber security threats.

10.2 The education of end users about how to better protect themselves from e-security risks is a priority of the Australian Government's *Cyber Security Strategy*.[1] However, the evidence suggested that fragmentation may be undermining the effectiveness of current e-security messages and education efforts. This chapter concludes by discussing a proposal for a

[1] Attorney General's Department (AGD), *Cyber Security Strategy*, Australian Government, 2009, p.vii.

more comprehensive and nationally coordinated strategy for educating the Australian community about cyber crime.

Current educational initiatives and 'cyber safety'

10.3 The Australian Government's approach to cyber crime education involves two main agencies: the Department of Broadband, Communications and the Digital Economy (DBCDE) delivers messages on technical cyber crime issues such as malware[2]; and under its remit to protect consumers from misleading conduct, the Australian Competition and Consumer Commission (ACCC) educates the community about identity fraud and scams.[3]

10.4 In addition to the principal agencies, myriad other Commonwealth, State and Territory departments, as well as industry and community groups, deliver messages on cyber crime to the Australian community. In particular, the Australian Communications and Media Authority (ACMA) educates younger Australians about some aspects of cyber crime through its *Cybersmart* program which, although largely focused on issues such as online bullying, also covers aspects of e-security such as viruses and password protection.[4]

10.5 Since the commencement of this inquiry the online behaviour and safety of younger Australians has become a source of widespread community concern, particularly in relation to online harassment and the use of social networking sites. A number of contributors to this inquiry have made recommendations relating to the teaching of skills in schools to deal with these issues in tandem with other e-security issues, such as malware and identity fraud.[5]

10.6 There is, however, a distinction made between 'e-security' and 'cyber safety' in current government policy. The former is applied to the cyber crime problems of malware, denial of service attacks, hacking and the related technology enabled crimes of identity theft, identity fraud and related financial crimes and online scams. In contrast, DBCDE define

[2] AGD, *Cyber Security Strategy,* Australian Government, p.30.

[3] ACCC, *Submission 46*, p.2.

[4] ACMA, *Cybersmart program*, ACMA, 6 October 2009, viewed 2 March 2010, <http://www.acma.gov.au>.

[5] See for example: Australian Council of State School Organisations, *Submission 42*, p.6; ROAR Film Pty Ltd, *Submission 64*, p.19.

issues relating to the social and personal risks of operating online as 'cyber safety'.[6]

10.7 Consequently, the problems of online harassment, bullying, stalking, child grooming and, for example, unauthorised publication of images and exposure to other online harms fall into the latter framework. In practice, these distinctions are frequently difficult to make because of the interconnectedness of information and communications technologies (ICT).

10.8 On 15 March 2009 the Australian Parliament resolved to establish a Joint Select Committee on Cyber-Safety to examine, among other things, the effectiveness of cyber safety education initiatives in Australia.[7] In-depth consideration of cyber-safety education issues is therefore deferred to the inquiry of the Joint Select Committee on Cyber-Safety. This chapter will examine education initiatives as they relate to e-security.

Access to information

10.9 The relatively fragmented approach to education initiatives is reflected in the wide range of information sources available to Australian end users.

10.10 One of the primary sources of information for end users is the *Stay Smart Online* website, maintained by DBCDE and first launched in 2006. The *Cyber Security Strategy* has designated the *Stay Smart Online* website as 'a single authoritative website for cyber security information for Australian home users and small businesses'.[8] The website provides a range of resources, including quizzes and practical guides, to inform consumers on dealing with system vulnerabilities and safely transacting online. The DBCDE informed the Committee that the website received over 8.4 million hits during 2008-09. The Department also stated that the website is

[6] DBCDE, *Submission 34*, p.5.

[7] Parliament of the Commonwealth of Australia, House of Representatives, *Votes and Proceedings*, No. 152, 11 March 2010, p.1687; Parliament of the Commonwealth of Australia, Senate, *Journals of the Senate*, No. 115, 11 March 2010, p.3296.

[8] AGD, *Cyber Security Strategy,* Australian Government, p.17; DBCDE, *Submission 34*, p.12; Senator the Hon Helen Coonan, *Launch of collaborative online security initiative*, media release, Parliament House, 23 October 2006, viewed 2 February 2009, <http://www.minister.dbcde.gov.au/coonan/media/media_releases/launch_of_collaborative_online_security_initiative>.

reviewed regularly to ensure clarity and effectiveness. No information was received on the actual number of unique visitors to the site.[9]

10.11 The *Stay Smart Online* website also directs users to the free *Stay Smart Online Alert Service* website (delivered by AusCERT) where users can subscribe to simple language email updates on cyber security threats. The DBCDE advised that the *Stay Smart Online Alert Service* website received 34,000 hits during 2008-09. According to an April 2009 review of the service, 89 per cent of respondents rated the services as good and 90 per cent said their awareness of e-security had improved.[10] However, the number of hits does not identify unique visitors and the evidence did not indicate how many people are registered for the *Stay Smart Online Alert Service.*

10.12 Similarly, the ACCC provides the *SCAMwatch* website which advises end users on scams generally, including online scams and phishing schemes. The website provides a range of advice relating to current and emerging scams, including real life examples and downloadable guides, and provides a reporting portal which assists end users in making scam related complaints (See Chapter 5).[11]

10.13 The website received over 100,000 unique visitors in the first quarter of 2009. The *SCAMwatch* website also provides a free online scam alert service, which as of July 2009 had 11,000 subscribers.[12]

10.14 *SCAMwatch* also acts as a portal for State and Territory members of the Australasian Consumer Fraud Taskforce[13] (ACFT). The websites of the New South Wales (NSW) Office of Fair Trading, the Northern Territory (NT) Department of Justice, the Tasmanian Department of Justice, the Western Australian (WA) Department of Commerce and Queensland Office of Fair Trading supplement their information on scams by directing users to the *SCAMwatch* website.[14]

10.15 The ACMA provides the *Cybersmart* website as part of its broader remit to educate younger Australians. The website seeks to engage children of

[9] DBCDE, *Submission 34*, p.12.

[10] DBCDE, *Submission 34*, p.12; Australian Government, *Stay Smart Online Alert Service User Guide*, Australian Government, 2008, p.1.

[11] ACCC, *Submission 46*, p.4.

[12] ACCC, *Submission 46*, p.4; Mr Nigel Ridgway, ACCC, *Transcript of Evidence*, 18 November 2009, p.11.

[13] The ACFT is a partnership of nineteen Australian and New Zealand government regulatory agencies and departments including the ACCC (chair), AGD, ACMA, AFP, DBCDE, ATO and State and Territory fair trading agencies.

[14] See for example: NSW Government, *Submission 49*, p.3.

different ages with a variety of quizzes, interactive online activities and downloadable guides. While the website is largely focused on cyber safety, some cyber security issues are also covered, including advice on protecting passwords and avoiding viruses.[15]

10.16 Additionally, a number of other Australian Government agencies provide limited information on varying aspects of cyber crime through their websites, including the Australian Federal Police (AFP), the Attorney General's Department (AGD), the Australian Taxation Office (ATO) and the Australian Securities and Investment Commission (ASIC).[16]

10.17 Some agencies also provide printed information through publications and media releases.[17] For example:

- in 2009 AGD published the *Dealing with identity theft: Protecting your identity* booklet, a guide for preventing and managing identity theft;[18] and
- the ACCC publishes the *Little Black Book of Scams* which highlights popular scams, including online scams, and provides tips on how to protect and deal with such scams.[19]

10.18 Internet security companies, financial institutions, ICT companies and community organisations, such as the Australian Seniors Computer Clubs Associations (ASCCA), also provide information to consumers through their websites and print media.[20]

[15] Australian Government, *Cyber smart website*, 2010, <http://www.cybersmart.gov.au/>.

[16] See for example: ACCC, *Submission 46*, p.4; AFP, *Technology Enabled Crime*, AFP, 2 September 2009, viewed 4 February 2010, <http://www.afp.gov.au/national/e-crime.html>; AGD, *Identity security*, AGD, updated 2 February 2010, viewed 4 February 2010, <http://www.ag.gov.au/identitysecurity>; NSW Government, *Submission 49*, p.3; ATO, *Submission 59*, pp.9-11; ACCC, 'The Little Black Book of Scams', *Exhibit 16*, p.43; DBCDE, *Submission 34.1*, p.8.

[17] ATO, *Submission 59*, pp.9-11; AFP, *Submission 25*, p.11; NSW Government, *Submission 49*, p.3; NT Government, *Submission 53*, p.3; Tasmanian Government, *Submission 51*, p.3; WA Government, *Submission 48*, p.2; Queensland Government, *Submission 67*, p.4; Mr Bruce Matthews, ACMA, *Transcript of Evidence*, 21 October 2009, p.6.

[18] AGD, *Dealing with Identity theft: protecting your Identity*, Australian Government, 2009.

[19] ACCC, *Little Black Book of Scams*, *Exhibit 16*.

[20] See for example: Mr Bruce Matthews, ACMA, *Transcript of Evidence*, 21 October 2009, p.6; Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.20; McAfee Australia, *Submission 10*, p.6; Symantec Corporation, *Symantec Exposes the Truth about the Internet Black Market and Takes a Stand against Cyber Crime*, media release, Symantec Corporation, 11 September 2009, p.2; APCA, *Submission 50*, p.5; Telstra, *Submission 43.1*, p.3; ASCCA, *Submission 63*, p.12.

10.19 Contributors argued that, while there are myriad sources of information on cyber crime, the provision of information to consumers could be improved. For example, Mr Allen Asher, Chief Executive Officer, Australian Communications Consumers Action Network (ACCAN), told the Committee of the results of a 2009 ACCAN survey:

> … alarmingly, very few people were relying on the information available from … government services. Even though there is a $73 million program that is administered to inform consumers about these things, only two out of five actually got their information from these government services. We found that three out of five were relying on what often might be folk tales from friends and neighbours.[21]

10.20 Additionally, both AusCERT and ASCCA argued that, due to the large number of organisations providing information, consumers may be confused by inconsistent, and sometimes inaccurate, information on cyber crime precautions.[22] For example, Mr Bill Gibson, Chief Information Officer, ATO, stated that, while both the ATO and the banking industry provide information on phishing, they may each express it in a different way, which may in turn confuse end users.[23]

10.21 The ACCAN proposed that to improve the provision of information to consumers, initiatives should be coordinated through a coherent national strategy on online security education.[24] This proposal is discussed in more detail at the end of this chapter.

10.22 More specifically, both ASCCA and the Internet Safety Institute proposed targeted programs to deliver clear and simple cyber security information to consumers at the point of sale of ICT and when online.[25] Mrs Nancy Bosler, President, ASCCA, told the Committee:

> I would say that every computer that is sold needs to have antivirus software and a firewall installed as a normal thing. There needs to be a very good plain-English brochure that goes with that

[21] Mr Allan Asher, ACCAN, *Transcript of Evidence*, 8 October 2009, pp.14-15; ACCAN, *Submission 57.1*, p.2.

[22] See for example: AusCERT, *Submission 30*, p.12; ASCCA, *Submission 63*, p.3.

[23] Mr Bill Gibson, ATO, *Transcript of Evidence*, 16 September 2009, p.8.

[24] ACCAN, *Submission 57.1*, p.5.

[25] See for example: Consumers' Telecommunications Network, *Surfing on thin ice: consumers and malware, adware, spam and phishing*, CTN, November 2009, p.25; Internet Safety Institute, *Submission 37*, p.10.

> computer and spells it out simply. Give them the information, but do not scare them witless.[26]

10.23 The provision of information to consumers the point of sale is further discussed in Chapter 8.

Community awareness raising

10.24 At a national level, there are two awareness raising campaigns conducted annually:

- the DBCDE's *Cyber Security Awareness Week;* and
- the ACFT's *National Consumer Fraud Week.*

10.25 Both of these awareness raising campaigns are conducted in partnership with other areas of government, industry and community groups, and involve advertising campaigns, online activities, public forums and events.[27]

10.26 The DBCDE's *Cyber Security Awareness Week* (running since 2006 as the *National E-security Awareness Week*) focuses on malware and identity theft. The Department said that the 2009 week brought together more than thirty-five partners from the community, State and Territory governments and industry, including Microsoft and Symantec, to hold more than seventy events around Australia. The key messages for the week were:

- get a better, stronger password and change it at least twice a year;
- get security software, and update and patch it regularly;
- stop and think before you click on links or attachments from unknown sources;
- be careful about the information you put online; and
- refer to the *Stay Smart Online* website for further information and to sign up for the email alert service.[28]

[26] Mrs Nancy Bosler, ASCCA, *Transcript of Evidence*, 28 October 2009, p.5.

[27] AGD, *Cyber Security Strategy,* Australian Government, p.17; DBCDE, *Submission 34*, pp.11-12; AFP, *Submission 25*, p.11.

[28] DBCDE, *Submission 34*, pp.11-12; Australian Government, *National E-security Awareness Week 2009 partnerships*, Stay Smart Online, 2009, viewed 5 March 2009, <http://www.staysmartonline.gov.au/news-events/partners>.

10.27 The DBCDE submitted that the week generated a number of media articles that had the potential to reach over four million Australians.[29]

10.28 At a hearing in November 2009, Mr Keith Besgrove, First Assistant Secretary, Digital Economy Services Division, DBCDE, told the Committee that DBCDE are moving to a new approach to community awareness raising:

> … [DBCDE is starting] to move away from the single awareness week each year towards more of a rolling program. We are currently discussing with some of the banks, retailers and other groups having some sort of initiative in the lead-up to Christmas. We are talking to Harvey Norman about a back-to-school initiative in late January. … The idea is to try to have more of a rolling program of initiatives. We would still focus the majority of our efforts during each security awareness week, but we want to try to keep reinforcing the message and also to take advantage of the efforts of others.[30]

10.29 The ACFT's *National Consumer Fraud Week* raises awareness about scams, including online scams. During the 2009 week, ACFT members held a number of public forums, and published several media articles and posters, to advise on protecting from, and dealing with, the latest scams.[31]

10.30 The ACCC (the Chair of the ACFT) also informed the Committee that they are looking to move away from conducting a single awareness week, to conducting a series of events over the next year in order to continually reinforce their messages to consumers.[32]

10.31 Contributors acknowledged that community awareness raising campaigns have some impact, but argued that current campaigns are not sufficiently targeted or protracted, and questioned whether such campaigns are effective in reaching the Australian community.[33]

10.32 Additionally, some contributors argued that such campaigns are not sufficiently coordinated across industry and Government. For example, in relation to DBCDE's *National E-security Awareness Week*, the Internet Society of Australia submitted:

[29] DBCDE, *Submission 34*, p.12.

[30] Mr Keith Besgrove, DBCDE, *Transcript of Evidence,* 25 November 2009, p.5.

[31] ACCC, *Submission 46*, p.5; NSW Government, *Submission 49*, p.4.

[32] Mr Nigel Ridgway, ACCC, *Transcript of Evidence*, 18 November 2009, p.10.

[33] ACCAN, *Submission 57.1*, p.5; Telstra, *Submission 43*, p.4; Microsoft Australia, *Submission 35*, p.16; Internet Safety Institute, *Submission 37*, p.10.

> One government agency that was not … a part of E-Security week was the Privacy Commissioner's Office. Given the implications for an individual's privacy from security threats such as identity theft, and the clear implications for an individual's privacy when they put personal information on social networking sites, they might be involved in initiatives such as e-security week in the future.[34]

10.33 Similarly, the South Australian Police informed the Committee that they were not informed of the ACFT's *National Consumer Fraud Week* and thus missed out on a key opportunity to educate end users.[35]

10.34 There was a widely held view that a highly coordinated and sustained multimedia campaign, similar to public health campaigns such as the *Slip, Slop, Slap* program, is necessary and would be a more effective way of achieving cultural change on e-security. A number of contributors proposed that such a campaign should focus on delivering simple and understandable messages on both computer security (such as updating systems and anti-virus software) and computer behaviours (such as avoiding scams and phishing websites), to bring about cultural change to the way Australian end users operate online.[36]

10.35 It was suggested that such a campaign could utilise a range of media, including print media, television and online media, and could include hard-hitting real life examples to drive home messages to broad sections of the Australian community.[37] Commander Neil Gaughan, AFP, told the Committee:

> I think the key issue is putting forward a public message—a really hard-hitting train crash type scenario—that the message needs to get out there to the consumer, because clearly it is not. It would make all of our jobs a lot easier if it does.[38]

10.36 ACCAN advocated a public awareness campaign but cautioned that such an approach must not alarm consumers. Mr Allen Asher, Chief Executive Officer, ACCAN, stated:

[34] Internet Society of Australia, *Submission 45*, p.5.

[35] South Australia Police (SAP), *Submission 2*, p.2.

[36] See for example: ACCAN, *Submission 57.1*, p.5; Telstra, *Submission 43*, p.4; Mr Peter Coroneos, IIA, *Transcript of Evidence*, 11 September 2009, p.18; Ms Johnson, Australian Information Industry Association, *Transcript of Evidence*, 11 September 2009, p.29; Mr Bill Gibson, ATO, *Transcript of Evidence*, 16 September 2009, p.8; Mr Alastair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.64.

[37] See for example: Mr Bill Gibson, ATO, *Transcript of Evidence*, 16 September 2009, p.8; Mr Alastair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.64.

[38] Commander Neil Gaughan, AFP, *Transcript of Evidence*, 9 September 2009, p.18.

> The concern that I have is that when people are … told, 'We will all be doomed and there is nothing we can do' then people become powerless and fail to act. So it has to operate on a couple of levels. I do not believe that simply telling scare stories is good at all because what that does is drive people away who might otherwise beneficially participate in the digital economy. It drives them away and they just will not participate. We do not want that to happen. At the same time, we do want people to take sensible precautions to ensure that their software is updated and to ensure that they do not respond to obvious phishing.[39]

10.37 In response to the above proposal, DBCDE argued that a public health style eduction campaign is 'not a workable option' in the case of cyber security messaging. The DBCDE submitted that any campaign delivered in a powerful and shocking manner may serve to damage the digital economy by undermining confidence in the online environment.[40] Nevertheless, DBCDE acknowledged that elements of public health style education campaigns, such as sustained programs over a long period of time, could be usefully applied to cyber security messaging.[41]

Skills development

10.38 Skills developmentl is delivered through a variety of government, industry and community organisation programs, largely targeted at children and seniors.

10.39 The DBCDE provides the *Budd:e E-security Education Modules* for students in years 3 and 9. Launched in June 2009, these education modules (developed by ROAR Film Pty Ltd, an Australian online education company), feature e-security tips, games and videos. Schools can access the program free of charge through the *Stay Smart Online* website, or by requesting CDs from DBCDE.[42]

10.40 Mr Keith Besgrove told the Committee of DBCDE's planned rollout of the modules:

> …we believe there are over 9,000 schools in Australia. To date, 1,400 schools have access to our e-security teaching tool online and

[39] Mr Allan Asher, ACCAN, *Transcript of Evidence*, 8 October 2009, p.19.

[40] DBCDE, *Submission 34.1*, p.9.

[41] DBCDE, *Submission 34.1*, p.9.

[42] DBCDE, *Submission 34*, pp.12-13.

> we have also had more than 800 sent the CDs. We have a couple of people who are engaging full time on a continuing basis with schools. I hope this time next year to be able to say that we have at least doubled those numbers. That is certainly our intention. The idea is to reach all of the schools in Australia over the next two years.[43]

10.41 In relation to seniors, in November 2008 the Department of Families, Housing, Community Services and Indigenous Affairs launched the *Broadband for Seniors* program. Under the program, NEC Australia Pty Ltd, in partnership with community and vocational institutions, will establish two thousand free Internet kiosks in community centres and clubs used by seniors throughout Australia to teach online skills, including aspects of Internet safety.[44]

10.42 Industry has also sponsored skills development programs and is working jointly with government agencies. For example, Microsoft, the AFP and ACMA have partnered to roll out the *ThinkUKnow* education program for teachers and parents. The program, which originated in the UK, seeks to educate adults about keeping young people safe online through interactive information sessions. During 2009, the program delivered forty-six pilot presentations to school communities in Victoria, NSW and the Australian Capital Territory. AFP said that the program will be rolled out nationally in 2010.[45] The program largely focuses on cyber safety but also covers some e-security issues such as virus protection.[46]

10.43 Telstra also supports online safety skills initiatives through the Telstra Foundation. In 2008 Telstra committed $6 million over six years to initiatives such as the *SuperClubsPlus Australia* website, a protected website where students can interact and access IT literacy resources, and the *BeNetWise* program, which teaches IT literacy to disadvantaged children.[47]

10.44 Community organisations provide further skills development initiatives. For example, ASCCA teaches online skills, including cyber security, to

[43] Mr Keith Besgrove, DBCDE, *Transcript of Evidence,* 25 November 2009, p.5.

[44] ASCCA, *Submission 63.1*, p.1; Department of Families, Housing, Community Services and Indigenous Affairs, *Broadband for Seniors*, FAHCSIA, 2009, viewed 4 March 2010, <http://fahcsia.gov.au>.

[45] See for example: AFP, *Submission 25*, pp.12-13; Microsoft Australia, *Submission 35*, p.17.

[46] ThinkUKnow Australia, *What is ThinkUKnow?*, 2010, viewed 4 March 2009, <http://www.thinkuknow.org.au>.

[47] Telstra, *Submission 43.1,* p.3.

senior and disabled persons all over Australia via its 142 member clubs, including through a mentoring program.[48]

10.45 While skills development programs exist for the most vulnerable end users, such as children and seniors, evidence indicated that other Australians may also require better access to skills development resources.[49] For example, a March 2009 ACMA survey of 1,637 Australians found that over 68 per cent of respondents were self taught in the use of the Internet, while less than 18 per cent had received formal training.[50]

10.46 ASCCA endorsed this view and argued the need for a more widely available IT literacy program:

> There is a considerable role for governments – particularly the Federal Government – to provide direct funding to community groups outside the vocational area for computer literacy for daily living skills. With government, business and community sectors relying more heavily than ever on ICT for disseminating information via their websites the ability of those who are not computer literate will be severely affected. Their lack of computer literacy will impact on daily living skills, business transactions and social inclusion.[51]

10.47 In relation to skills development programs for Australian children, some submitters argued that, despite current initiatives, skills teaching programs are not sufficiently widespread, nor sufficiently tested or certified.[52]

IT Literacy Drivers Licence

10.48 To overcome these issues, some submitters advocated the development of a national system of certifiable skills standards to raise online security proficiency in all sections of the Australian community including in vocational institutions, workplaces and at home.[53]

[48] Mrs Nancy Bosler, ASCCA, *Transcript of Evidence*, 28 October 2009, p.3; ASCCA, *Submission 63*, p.12.

[49] See for example: ACCAN, *Submission 57.1*, p.5; Queensland Government, *Submission 67*, p.7.

[50] ACMA, *Australia in the Digital Economy: Report 1 – Trust and Confidence*, ACMA, March 2009, p.35.

[51] ASCCA, *Submission 63*, p.3.

[52] Microsoft Australia, *Submission 35*, p.17; Mr Terry Hilsberg, ROAR Film Pty Ltd, *Transcript of Evidence*, 8 October 2009, p.68.

[53] Telstra, *Submission 43*, p.4; Microsoft Australia, *Submission 43*, p.17.

10.49 ROAR Film Pty Ltd, the developer of DBCDE's *Budd:e Education Modules*, proposed the establishment of a national Internet users' licence. Operating largely as an online program, users would be required to gain certification of a prescribed skill level before being permitted to use the Internet in various institutional contexts such as a school or a private organisation. Recreational Internet users, such as home users, could voluntarily obtain such a user's licence.

10.50 ROAR submitted that there is an overlap between e-security, safety and citizenship, and the licence could extend beyond e-security to cyber safety and cyber citizenship issues such as intellectual property and online ethics.[54] ROAR informed the Committee that it has developed e-security modules for a similar initiative in UK schools, where all state schools in London access online teaching resources, including on cyber security, through the London Grid for Learning (a closed broadband network).[55]

10.51 Similar online skills competency programs already exist. The *International Computer Driving Licence* (ICDL) is a basic ICT literacy benchmarking program, originating in Europe, which requires users to complete a range of theoretical and practical tests for IT skills, including aspects of computer security. The ICDL has been obtained by seven million users across 148 countries. Australian users can obtain an ICDL through a number of test centres accredited by ICDL Australia. [56] Up until 2008, the ICDL was run in Australia by the Australian Computer Society (ACS), and since 2008 by EXIN, a global independent IT examination provider. Both ACS and EXIN advocate developing the ICDL, in partnership with government, to provide a national IT literacy standard in Australia.[57]

10.52 Similarly, ACCAN proposed an *Online Competency Skills Test* by which users could asses their own preparedness and level of understanding.[58]

10.53 In response to these proposals, DBCDE submitted that the ICDL does not contain specific cyber security units, and cited DBCDE's current education initiatives (such as the education modules for students in years 3 and 9) as evidence of its commitment to developing IT literacy.[59] However, DBCDE provided no comment on the specific proposal of establishing national

[54] ROAR Film Pty Ltd, *Submission 64*, pp.2-4, 19.

[55] Mr Terry Hilsberg, ROAR Film Pty Ltd, *Transcript of Evidence*, 8 October 2009, p.68.

[56] ACCAN, *Submission 57.1*, p.5.

[57] EXIN South Pacific, *EXIN to take over International Computer Driving Licence (ICDL) in Australia*, media release, July 10 2008, viewed 4 March 2010, <http://www.acs.org.au/icdl/>.

[58] ACCAN, *Submission 57.1*, p.5.

[59] DBCDE, *Submission 34.1*, p.8.

certifiable skills standards for online security that would be accessible to the wider community.

Nationally coordinated education strategy

10.54 As described in the preceding sections, a range of proposals exist to strengthen the different aspects of cyber crime education and community awareness in Australia. However, on a broader level, many submitters criticised the overall strategic direction of education initiatives in Australia. For example, there was wide agreement that education initiatives as a whole are limited by a lack of coordination between different areas of government and industry.[60] Contributors argued that such a lack of coordination not only confuses Australian end users, but also leads to inefficiencies from overlapping initiatives.[61]

10.55 The Committee heard widespread advocacy for a more coherent and strategic approach to cyber crime education and community awareness in Australia.[62]

10.56 As part of its proposal for an Australian Government Office of Internet Security (See Chapter 5), ACCAN argued that the Office should develop and oversee a *National Strategy for E-security Awareness*. ACCAN proposed that an Office of Internet Security could provide high level coordination of a range of educational initiatives, in order to ensure clearly articulated messages reach the public.[63]

10.57 Similarly, the Australian Banking Association (ABA) submitted:

> Our members would like to see a whole-of-Government approach to … education campaigns rather than the fragmented approach adopted to date and the duplication of work and associated unwarranted costs of such duplication. This includes coordination

[60] See for example: ACCAN, *Submission 57.1*, p.5; Mr Bill Gibson, ATO, *Transcript of Evidence*, 16 September 2009, p.7; Mr Tony Burke, ABA, *Transcript of Evidence*, 8 October 2009, pp.50-51; SAP, *Submission 2*, p.2; Mr Darren Kane, Telstra, *Transcript of Evidence*, 11 September 2009, p.34; Internet Safety Institute, *Submission 37*, p.10.

[61] See for example: ROAR Film Pty Ltd, *Submission 64*, p.2; Microsoft Australia, *Submission 35*, p.16; SAP, *Submission 2*, p.2; ABA, *Submission 7*, p.12.

[62] See for example: ASCCA, *Submission 63*, p.3; Mr Bill Gibson, ATO, *Transcript of Evidence*, 16 September 2009, p.7; Microsoft Australia, *Submission 35*, p.16; Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.53.

[63] ACCAN, *Submission 57.1*, p.5; UK Cabinet Office, *Cyber Security Strategy of the United Kingdom,* UK Cabinet Office, June 2009, p.18.

> not just of Federal Government activities in this area, but State Government initiatives as well. The Federal Government should display leadership in this area.[64]

10.58 The Committee heard a number of proposals that could help to shape such an overarching policy. For example, it was argued that all education initiatives should be regularly evaluated against clear and measurable objectives, including through community consultation, to ensure that initiatives are effective and far-reaching.[65] Some advocated the need for industry members (such as ISPs) and community groups to be further engaged in educating Australian end users.[66] Symantec also advocated utilising the high profile of the rollout of the National Broadband Network (NBN) to deliver education initiatives.[67]

10.59 Importantly, submitters argued that any educational initiatives must effectively target all sections of the Australian community, particularly those people most vulnerable to cyber crime such as young people, seniors and new computer users.[68]

Committee View

10.60 The Committee recognises the considerable efforts of a range of stakeholders from Commonwealth, State and Territory governments, industry and community organisations, to educate the Australian community about cyber crime. However, the evidence indicated that cyber security education in Australia remains fragmented, and more consistent and effective messaging is needed to achieve the cultural change necessary.

10.61 The *Cyber Security Strategy* identifies education as the most appropriate strategic response to combating the e-security risks faced by end users (and posed by end users). However, the document lacks a clearly articulated e-security education strategy that could provide the basis for a more comprehensive and coordinated approach.

[64] ABA, *Submission 7*, p.12.

[65] See for example: ACCAN, *Submission 57*, p.3; ASCCA, *Submission 63*, p.4; ACCAN, *Submission 57.1*, pp.5-6; Microsoft Australia, *Submission 35*, p.16; IIA, *Submission 54*, p.6; Mr Alastair MacGibbon, Internet Safety Institute, *Transcript of Evidence*, 11 September 2009, p.64; IIA, *Submission 54*, p.6.

[66] See for example: ACCAN, *Submission 57*, p.3; Telstra, *Submission 43*, p.4.

[67] Mr Craig Scroggie, Symantec Corporation, *Transcript of Evidence*, 9 October 2009, p.53; ROAR Film Pty Ltd, *Submission 64*, pp.2-3,19.

[68] See for example: ACCAN, *Submission 57.1*, p.5; Queensland Government, *Submission 67*, p.7.

10.62 It would be appropriate for the Australian Government to clearly designate DBCDE as the lead department responsible for the development and oversight of an overarching nationally coordinated e-security education strategy. Such a national strategy would give proper recognition to the important role of end user education in the national *Cyber Security Strategy.* The strategy should cover the provision of information, awareness raising and skills development, and deal with all aspects of cyber crime, including malware, identity fraud and scams.

10.63 In developing and implementing such a strategy, DBCDE should:

- utilise education and public relations professionals in the development and delivery of the strategy;
- consult, and continue to engage with, industry and community groups, in the delivery and evaluation of initiatives; and
- identify and utilise opportunities for delivering education initiatives as part of the rollout of the NBN.

10.64 Such a national education strategy should have a specifically identified program output that can be reported on in DBCDE's annual report. Initiatives funded by DBCDE under the strategy should be reviewed to evaluate the effectiveness of initiatives and to ensure value for money. The results of such reviews should also be included in DBCDE's annual report.

Recommendation 31

That the Department of Broadband, Communications and the Digital Economy, in consultation with relevant agencies, industry and relevant community organisations, develop a nationally coordinated strategy for the education of consumers:

- **that the strategy cover all aspects of cyber crime including malware, identity theft, identity fraud and scams; and**
- **includes clear benchmarks against which the effectiveness of education initiatives can be clearly evaluated and publicly reported on to Parliament.**

10.65 The Committee believes that such a national strategy should include a more integrated approach to the provision of information to end users. Current website resources such as the *Stay Smart Online* and *SCAMwatch* websites could form part of a more integrated model linked to a centralised cyber crime reporting centre (See Chapter 5). Additionally, effort should be made to deliver information to consumers at the point of sale of ICT goods and services (See Chapter 8).

Recommendation 32

That the Stay Smart Online and SCAMwatch websites be linked to the national cyber crime reporting centre referred to in recommendation 4.

10.66 The Committee acknowledges that a 'hard hitting' community awareness campaign may alarm end users. However the Committee does not accept the argument that a public health style campaign is not workable in the area of cyber security education. The Committee considers that, through engaging the services of education and public relations professionals, the Government could conduct a far reaching and sustained public awareness raising campaign(s) that appeals to consumers, without undermining confidence in the Internet. Such a campaign should deliver key messages on technical precautions, as well as on appropriate user behaviours.

Recommendation 33

That the Department of Broadband, Communications and the Digital Economy implement a public health style campaign that uses a wide range of media to deliver messages on cyber security issues, technical precautions and appropriate user behaviours.

10.67 Finally, in regards to skills development, the Committee recognises the value of implementing certifiable national skills standards for online security that would apply to all Australian IT users, whether students, employees or home users.

10.68 The Committee did not take detailed evidence on cyber citizenship, cyber safety or cyber security skills training in State and Territory schools and therefore refrains from making any recommendation about IT literacy training in the school context.

10.69 However the Committee considers that there is a case for a nationally consistent approach to certifiable skills standards for IT literacy that is available to all members of the Australian community. In particular the Committee sees value in an 'IT drivers' licence' and notes a model is already well established in the UK and Europe and is available in Australia.

Recommendation 34

That the Department of Broadband, Communications and the Digital Economy support the development of IT literacy training that includes cyber security and is available to the community as a whole.